AML/CFT

Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Laws

Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing

DFL 10/2025 Effective from 14/10/2025 **Status:** In-Force

We, Mohammed bin Zayed Al Nahyan, President of the United Arab Emirates,

- Having reviewed the Constitution;

- Federal Law No. (1) of 1972 Regarding the Competences of the Ministries and the Powers of Ministers, as amended;

- Federal Law No. (39) of 2006 Regarding International Judicial Cooperation in Criminal Matters, as amended;

- Federal Law No. (7) of 2014 Regarding Combating Terrorist Crimes, as amended;

- Federal Decree by Law No. (20) of 2018 Regarding Anti-Money Laundering, the Financing of Terrorism, and the Financing of Illegal Organizations, as amended;

- Federal Decree by Law No. (30) of 2021 Regarding Combating Narcotics and Psychotropic Substances, as amended;

- Federal Decree by Law No. (31) of 2021 Promulgating the Crimes and Penalties Law, as amended;

- Federal Decree by Law No. (34) of 2021 Regarding Countering Rumors and Cybercrimes, as amended;

- Federal Decree by Law No. (38) of 2022 Promulgating the Criminal Procedure Law, as amended; and

- Upon the proposal of the Minister of Finance, and the approval of the Cabinet,

Hereby promulgate the following Decree by Law:

Chapter One: Definitions

Article (1)

For the purposes of implementing the provisions of this Decree by law, the following terms and expressions shall have the meanings assigned to each of them, unless the context requires otherwise:

The State: The United Arab Emirates.

The Ministry: The Ministry of Finance.

The Minister: The Minister of Finance.

The Central Bank:	The Central Bank of the United Arab Emirates.
The Governor:	The Governor of the Central Bank.
The Supreme Committee:	The Supreme Committee for the Supervision of the National Strategy for Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing.
The National Committee:	The National Committee for Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing.
The General Secretariat:	The General Secretariat of the National Committee.
The Unit:	The Financial Intelligence Unit established by virtue of the provisions of this Federal Decree by Law.
The Supervisory Authority:	The federal and local authorities entrusted under the legislation with the supervision of the financial institutions, designated non-financial businesses and professions, virtual asset service providers, and non-profit organizations (NPOs); or the competent authorities responsible for granting approval to engage in an activity or profession, where no specific supervisory authority is designated by the legislation.
Law Enforcement Authorities:	The federal and local authorities entrusted, pursuant to the provisions of this Federal Decree by Law and their applicable legislation, with combating, investigating, detecting, and gathering evidence in respect of the offenses, including Money Laundering, Predicate Offences, the Financing of Terrorism, and the Proliferation Financing.
Concerned Authorities:	The governmental entities concerned with the implementation of any provision of this Decree by Law within the State.
The Executive Office:	The Executive Office for Control and Non-Proliferation, concerned with the implementation of targeted financial sanctions within the State.
Targeted Financial Sanctions:	The freezing of funds and the prohibition of making them available, directly or indirectly, for the benefit of any natural or legal person or organization designated by resolutions issued by the Cabinet regarding Terrorist Lists, or by the United Nations Security Council under Chapter VII of the Charter of the United Nations concerning the prevention and suppression of terrorism and its financing, as well as the prevention, suppression, and halting of proliferation and its financing.
The Crime:	The crime of Money Laundering and the predicate offences related thereto, or the financing of terrorism, or the proliferation financing.
Predicate Offence:	Any act constituting a felony or misdemeanor, including the financing of terrorism, the proliferation financing, and evasion of direct and indirect taxes, in accordance with the applicable legislation of the State, whether committed within or outside the State, provided that such an act is punishable in both countries.
Money Laundering:	Any of the acts defined in Clause (1) of Article (2) of this Decree by Law, including its commission through digital systems, Virtual Assets, or cryptographic technologies.
Terrorist Act:	Any commission, attempt, participation, organization, planning, contribution, or provision of advice in the commission of any of the following acts, or the incitement of others to commit

the same, whether committed by a person or by a group of persons acting for a common purpose:

1. Any act or omission constituting a terrorist crime pursuant to Federal Law No. (7) of 2014 referred to hereinabove or any other law, or pursuant to international treaties and conventions on combating of terrorism to which the State is a party.

2. Any act or omission that is unlawfully intended to cause the death of, or to inflict serious bodily injury upon, a civilian or any other person not taking active part in hostilities in the event of an armed conflict, or to cause substantial damage to property or to the environment, where the purpose of such act, by nature or context, is to instill terror among a group of people, or to influence public authorities in the State, another country, or an international organization to perform or refrain from performing any act, or to obtain any benefit or advantage therefrom.

Terrorist: Any natural person, whether within or outside the State, who intentionally commits any of the following acts:

1. Commits or attempts to commit a Terrorist Act by any means, whether directly or indirectly.

2. Participates as an accomplice in a Terrorist Act.

3. Organizes a Terrorist Act or incites others to commit it.

4. Participates with a group of persons acting with a common intent to commit a Terrorist Act for the purpose of expanding terrorist activity or to commit such act, knowing the group's intention.

Terrorist Organization: A group of two or more persons, whether within or outside the State, that has committed a terrorist act, directly or indirectly, or has threatened to commit it, aims, plans, or seeks to commit it, or promotes or participates in its commission, whether directly or indirectly, regardless of its name, form, place of establishment, location, activity, or the nationality or residence of its members; including any organization recognized as a Terrorist Organization under any other law.

Financing of Terrorism: Any of the acts defined in Clause (1) of Article (3) of this Federal Decree by Law.

Proliferation: The illicit and unauthorized trade, as regulated under the applicable legislation in the State, in materials, systems, equipment, components, programs, or technology contributing to the production or development of Weapons of Mass Destruction, related technology, or their delivery means, including any act stipulated in Clause (3) of Article (3) of this Decree by Law.

Weapons of Mass Destruction: Weapons capable of inflicting harm on a large number of persons and posing a threat to human life and the natural environment through their catastrophic effects, such as nuclear, biological, chemical, or radiological weapons.

Funds: Assets or properties, however acquired, of any type or form, tangible or intangible, movable or immovable, electronic, digital, or cryptographic, including national and foreign currencies, legal documents, and instruments of whatever form, including electronic or digital forms, evidencing the ownership of such assets or properties, or shares or rights therein; as well as economic resources deemed as assets of any kind, including oil and other natural resources and all rights pertaining thereto, whatever their value or means of

acquisition; together with bank credits, cheques, payment orders, shares, securities, bonds, bills of exchange, letters of credit, and any proceeds, profits, or other income derived or resulting therefrom, which may be used to obtain any financing, goods, or services.

Virtual Assets: Digital representation of value that may be digitally traded or transferred and may be used for payment or investment purposes, excluding digital representations of fiat currencies, securities, or other Funds.

Proceeds: Funds derived, directly or indirectly, from the commission of any felony or misdemeanor, including profits, privileges, economic interests, and other benefits derived therefrom, and any equivalent Funds that have been converted, in whole or in part, into other Funds.

Criminal Property: Includes the following:

1. Proceeds derived from the commission of a Money Laundering offence or Predicate Offence.
2. Property used or intended to be used in any manner, in the commission of Money Laundering or a Predicate Offence.
3. Funds constituting the subject matter of Money Laundering.
4. Funds used, intended to be used, or allocated for use in the Financing of Terrorism, Terrorist Acts, Terrorist Organizations, or Proliferation Financing.
5. Proceeds derived from the commission of financing terrorism, Terrorist Acts, Terrorist Organization, or Proliferation Financing.

Suspicious Transactions: Transactions involving funds for which there are reasonable grounds to suspect that they constitute Proceeds of any felony or misdemeanor, or are related to Money Laundering, Financing of Terrorism, or Proliferation Financing, whether such transactions were executed or merely attempted.

Without Prior Notice: The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.

Freezing: The prohibition imposed on the transfer, conversion, disposition, movement, or transportation of Funds or Criminal Property, pursuant to a decision issued by a Competent Authority, while such Funds remain in the possession of their owner, manager, or holder, for the duration of the validity of such decision.

Seizure: The prohibition imposed on the transfer, conversion, disposition, movement, or transportation of Funds or Criminal Property, pursuant to a decision issued by a Competent Authority that assumes actual control and management thereof, for the duration of the validity of such decision.

Confiscation: The permanent deprivation of ownership of private Funds or Criminal Property by virtue of a judgment rendered by a competent court.

Asset Recovery: The process of identifying, tracing, evaluating, seizing, freezing, and confiscating, as well as enforcing the relevant orders for the management of Criminal Property or Funds of

	equivalent value, and their disposal, restitution, delivery, or sharing.
Financial Institutions:	Any person engaged in one or more financial activities or operations determined by the Executive Regulations of this Federal Decree by Law, on behalf of or for the benefit of a Customer.
Designated Non-Financial Businesses and Professions (DNFBPs):	Any person engaged in one or more of the commercial or professional activities or businesses, as specified in the Executive Regulations of this Federal Decree by Law.
Non-Profit Organizations:	Any organized group of a continuing nature for a definite or indefinite duration, consisting of natural or legal persons or a legal arrangement, not aimed at profit, which collects, receives, or disburses funds for charitable, religious, cultural, educational, social, solidarity, or other purposes that fall within the scope of benevolent acts.
Legal Arrangement:	Trusts or other similar arrangements.
Trust:	A legal relationship whereby the Settlor places Funds under the control of a Trustee for the benefit of a Beneficiary or for a specific purpose, and such Funds are deemed separate from the Trustee's own property, while the title thereto remains in the name of the Settlor or another person on behalf of the Settlor.
Settlor:	A natural or legal person who transfers the management of their own Funds to a Trustee pursuant to a Trust Instrument.
Trustee:	A natural or legal person vested with the rights and powers granted thereto by the Settlor or by the Trust, authorized thereby to manage, utilize, and dispose of the Settlor's Funds in accordance with the conditions imposed by either of them.
Customer:	Any natural or legal person, or legal arrangement, who establishes or seeks to establish a business relationship with Financial Institutions, any of the Designated Non-Financial Businesses and Professions, or Virtual Asset Service Providers.
Transaction:	Any disposal or utilization involving Funds or Proceeds, including, inter alia, deposit, withdrawal, transfer, sale, purchase, lending, exchange, mortgage, or donation.
Beneficial Owner:	The natural person who owns or exercises ultimate effective control over the customer, or the natural person on whose behalf the transactions are conducted; including any person who exercises ultimate effective control over a legal person or legal arrangement, whether directly or through a chain of ownership, control, or other indirect means, and who is identified, whether one or more, in accordance with the Executive Regulations of this Decree by Law.
Virtual Asset Service Provider(s):	Any natural or legal person who, as a commercial activity, conducts one or more of the virtual asset activities specified in the Executive Regulations of this Decree by Law or conducts transactions related thereto, on behalf of or for the benefit of another natural or legal person.
Registrar:	The competent authority responsible for supervising the economic or trade register of the various types of establishments registered in the State, as regulated by the legislation in

	force in the State.
Customer Due Diligence (CDD):	The process of identifying and verifying the information of a Customer or Beneficial Owner, whether a natural or legal person or a legal arrangement, as well as identifying the nature of their business, the purpose of the business relationship, and the ownership structure and control thereover, including ongoing monitoring procedures for the purposes of this Decree by Law and its Executive Regulations.
Controlled Delivery:	An approach whereby the competent authorities, under their supervision, allow the entry into, passage through, transit across, or exit from the State of illicit or suspicious funds, or proceeds of crime for the purpose of detecting an offense and identifying its perpetrators.
Undercover Operation:	An investigation and detection approach whereby a Judicial Enforcement Officer operates under an assumed or false identity or performs a covert or deceptive role for the purpose of obtaining evidence or information related to an offense.

Chapter Two: Crimes of Money Laundering, Financing of Terrorism, and Proliferation Financing

Article (2)

1. A person shall be deemed to have committed money laundering if that person knows or there are sufficient indications or evidence to believe that the Funds, in whole or in part, are the Proceeds of a Predicate Offence, and intentionally commits any of the following acts:

    a. Converts, transfers, or carries out any transaction involving the Proceeds for the purpose of concealing or disguising their illicit origin.

    b. Conceals or disguises the true nature of the proceeds, source, location, disposition, movement, ownership, or rights related thereto..

    c. Acquires, possesses, or uses the Proceeds upon receipt thereof.

    d. Assists the perpetrator of the Predicate Offence in evading punishment therefor.

2. Money Laundering shall be deemed an independent crime, and shall be excluded from the application of the provisions on concurrence prescribed under Federal Decree by Law No. (31) of 2021 referred to hereinabove; and the punishment or non-punishment of the perpetrator of the Predicate Offence shall not preclude their punishment for Money Laundering.

3. Conviction of the Predicate Offence shall not be required to establish the illegitimate source of the Proceeds, nor shall it be required to prove knowledge of the specific type or nature of the predicate offence from which the proceeds were derived. Such knowledge, being an element of the Crime, may be inferred from the factual and objective circumstances attendant upon its commission.

Article (3)

1. Whoever intentionally provides, collects, or makes available Funds by any means, directly or indirectly, including through the use of digital systems, Virtual Assets, or cryptographic technologies, with knowledge that such Funds shall be used, in whole or in part, in any of the following cases, shall be deemed to have committed Financing of Terrorism:

    a. The commission of a Terrorist Act or Terrorist Acts;

    b. By a Terrorist or a Terrorist Organization;

    c. Financing the travel of individuals to a State other than that of their residence or nationality for the purpose of committing, preparing, planning, or participating in, or facilitating a Terrorist Act, or providing the necessary Funds for training on Terrorist Acts or for receiving such training.

2. For the purposes of Clause (1) of this Article, Funds used in Financing of Terrorism shall include any Funds used in whole or in part, whether derived from a legitimate or illegitimate source, and regardless of whether such Funds were actually used to commit or attempt to commit a Terrorist Act, or whether they are linked to any specific Terrorist Act. The Financing of Terrorism shall be deemed committed irrespective of whether the accused is located in the same State as the Terrorist or the Terrorist Organization, or in the State in which the Terrorist Act is or will be committed, or in any other State.

3. Except in cases permitted or authorized under the legislation in force in the State, or pursuant to the provisions of treaties and agreements to which the State is a party, whoever intentionally commits any of the following acts shall be deemed to have committed the crime of Proliferation Financing:

    a. Provides, collects, or makes available Funds by any means, directly or indirectly, with knowledge that such Funds shall be used, in whole or in part, for the manufacture, possession, acquisition, development, production, sale, supply, export, transshipment, brokerage, transport, transfer, storage, or use of Weapons of Mass Destruction, their means of delivery, or related materials, including dual-use technologies and goods, when employed for said purposes.

    b. Any other act in accordance with the United Nations Security Council resolutions issued under Chapter VII of the Charter of the United Nations, concerning the prevention, suppression, and cessation of Proliferation and its Financing.

4. Knowledge, as an element of the Crime of Financing of Terrorism and the Crime of Proliferation Financing, may be inferred from the factual and objective circumstances attendant upon their commission.

Article (4)

A Legal Person shall be criminally liable where any of the crimes stipulated in this Decree by Law is intentionally committed in its name or for its account, without prejudice to the personal criminal liability of the perpetrator, and the administrative penalties provided for by law.

Chapter Three: Provisional Measures and Investigation Procedures

Article (5)

1. The Chief of the Unit may, without prior notice, order the cessation or temporary suspension of any Transaction suspected of being related to the Crime, for a period not exceeding ten (10) working days, based upon the Unit's analysis of Suspicious Transaction Reports, or information or requests received from domestic or international sources, including a counterpart Unit or any authority competent to take such measures.

2. The Chief of the Unit may also, without prior notice, order the Freezing of Funds suspected of being related to the Crime and held with Financial Institutions, Designated NonFinancial Businesses and Professions, or Virtual Asset Service Providers, for a period not exceeding thirty (30) days, based upon the Unit's analysis of Suspicious Transaction Reports and other information received thereby. Such order shall be subject to extension by the Attorney General or their delegate.

3. The Unit shall establish a system specifying the controls and procedures governing the cessation or suspension of Suspicious Transactions related to the Crime, and the conditions for lifting such cessation or suspension upon cancellation of the order or expiry of the prescribed term.

4. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall lift the Freezing order upon its cancellation by the Chief of the Unit, or upon the expiry of the period referred to in Clause (2) of this Article, unless the same has been extended.

5. The Executive Regulations of this Decree by Law shall determine the procedures, rules, and controls governing the implementation of the provisions hereof.

Article (6)

1. The Public Prosecution and the Competent Court, as the case may be, may, without prior notice, order the identification, tracing, valuation, Seizure, or Freezing of Funds, Criminal Property, or funds of equivalent value, as well as prohibit their management and impose a travel ban pending the completion of investigation or trial.

2. The Public Prosecution and the Competent Court, as the case may be, may, whenever required, issue decisions prohibiting the disposal or dealing in Funds or Criminal Property, or funds of equivalent value, and take the necessary measures to prevent any act intended to evade Seizure, Freezing, or Confiscation orders, without prejudice to the rights of bona fide third parties.

3. Without prejudice to the rights of bona fide third parties, any contract or act whose parties, or one of them, knew or should have known that its purpose was affect the ability of the competent authorities to effect Seizure, Freezing, Recovery, or Confiscation judgment, shall be deemed null and void by operation of law.

4. Any interested party may file a grievance against the decisions of the Public Prosecution relating to Seizure, Freezing, or those prohibiting dealing or disposing of Funds or Criminal Property, or funds of equivalent value, or against the extension of Freezing ordered by the Attorney General or their delegate pursuant to Clause (2) of Article (5) of this Decree by Law. The grievance shall be adjudicated by the competent Criminal Court within whose jurisdiction the Public Prosecution department issuing the decision is located, or which is competent to hear the criminal case.

5. The grievance shall be filed by way of a written report submitted to the competent Court, whereupon the chief justice of the Court shall fix a session for its consideration and notify the complainant thereof. The Public Prosecution shall submit a memorandum stating its opinion in respect of the grievance, and the Court shall decide thereon within a period not exceeding fourteen (14) working days from the date of submission.

6. The decision rendered in the grievance shall be final and not subject to appeal. Should the grievance be rejected, no new grievance may be submitted until the lapse of three (3) months from the date of rejection,

unless a serious and substantial reason arises prior to such lapse.

7. The Executive Regulations of this Decree by Law shall specify the procedures, rules, and controls for implementing the provisions hereof.

Article (7)

The Public Prosecution and the Competent Court, as the case may be, may assign the Accused, or any person deemed appropriate, to manage the Funds or Criminal Property, or funds of equivalent value, that have been Seized, Frozen, or subjected to Confiscation. The Executive Regulations of this Decree by Law shall set forth the conditions for estimating the remuneration and expenses of such management, the order of their disbursement, and the rules and controls for implementing the provisions hereof.

Article (8)

1. Without prejudice to the provisions of Article (6) of this Decree by Law, the criminal case shall be filed against any person committing Money Laundering, Financing of Terrorism, or Proliferation Financing, as stipulated in Articles (2) and (3) hereof, by the Attorney General or their delegate. It shall be filed in respect of other Crimes under this Decree by Law in accordance with the procedures prescribed by law.

2. The Attorney General or their delegate and the Competent Court, as the case may be, may issue decisions to take the necessary measures for the protection of intelligence information and the methods or means of obtaining the same, or to direct the competent authorities to provide protection to witnesses, confidential sources, Accused persons, or other parties to the proceedings, whenever there exists a serious and substantiated concern for their safety.

Article (9)

1. The Public Prosecution may, either on its own initiative or upon request of Law Enforcement Authorities, where sufficient indications of the commission of the Crime exist, order direct access to accounts, registers, documents, and records in the possession of third parties; it may also order access to the contents of computer systems, means of information technology, correspondence, communications, and parcels; as well as the identification, tracing, and seizure of Funds; monitoring of accounts; and imposition of travel bans, in addition to any other measures that may assist in uncovering the Crime and its perpetrators, without prejudice to the legislation in force within the State.

2. The Public Prosecution may seek the opinion of the Unit regarding the financial aspects of the Crime and their analysis.

3. Law Enforcement Authorities shall receive and follow up on the reports of the Unit, collect the evidence related thereto, and provide the Unit with feedback concerning the procedures taken in respect thereof.

4. Law Enforcement Authorities may obtain such information as they deem necessary for identifying and tracing Funds or Criminal Property, or Funds of corresponding value, as well as any other data necessary for the performance of their duties, in accordance with the manner prescribed by the Executive Regulations of this Decree by Law.

5. Law Enforcement Authorities may conduct Undercover Operations and employ other investigative techniques, as well as undertake Controlled Deliveries, whenever such measures may lead to the detection of the Crime, its

evidence, or the identification of the source and destination of Funds or Criminal Property, or the apprehension of perpetrators, without prejudice to the legislation in force within the State.

6. No criminal liability shall attach to any person assigned by Law Enforcement Authorities to investigate by means of an Undercover Operation or Controlled Delivery, in respect of any act which might otherwise constitute a Crime, unless such person has incited the commission thereof or exceeded the powers granted to them.

Chapter Four: Disclosure

Article (10)

Any person entering into or departing from the State shall be under the obligation to make a disclosure whenever they carry currencies, bearer negotiable instruments, precious metals, or valuable stones, in accordance with the disclosure system issued by the Federal Authority for Identity, Citizenship, Customs and Port Security, in coordination with the Central Bank.

Chapter Five: The Financial Intelligence Unit

Article (11)

An independent "Financial Intelligence Unit" shall be established within the Central Bank and shall act independently. All Suspicious Transaction Reports and information related thereto shall be submitted thereto, exclusively, by all Financial Institutions, Designated Non-Financial Businesses and Professions and Virtual Asset Service Providers. The Unit shall undertake the study and analysis thereof, and shall refer the same to the Concerned Authorities either automatically or upon request, and shall be vested with the following competences:

1. To request from Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and the Concerned Authorities, the provision of any additional information or documents related to the reports and information received, as well as any other information deemed necessary for the performance of its duties, within the timeframe and in the form prescribed by the Unit.

2. To exchange information and cooperate, automatically or upon request, with counterpart units and other competent authorities with respect to the suspension or cessation of operations suspected to be associated with the Crime, regarding such operations, Suspicious Transaction Reports, or any other information which the Unit is empowered to obtain or access, whether directly or indirectly. The Unit shall likewise exchange information with Concerned Authorities within the State to facilitate such cooperation and shall notify the counterpart units of the results of the utilization of the information provided and of the analyses conducted thereon. Such information may only be used for the purposes of combating the Crime and shall not be disclosed to any third party without the approval of the Unit.

3. To conclude Memoranda of Understanding for the purpose of regulating cooperation and the exchange of information with counterpart units and Concerned Authorities.

4. To establish and maintain a database of the information in its possession, and to protect the same by imposing rules governing the security and confidentiality of information, including the implementation of cybersecurity measures and procedures for processing, storing, and transmitting information, and to ensure that access to its facilities, data, and technical systems is restricted.

5. Any other competences in accordance with the provisions of this Decree by Law or as may be prescribed by its Executive Regulations.

Chapter Six: National Coordination and Cooperation

Article (12)

By virtue of the provisions of this Decree by Law, a committee shall be established and shall be known as the "Supreme Committee for the Supervision of the National Strategy for Anti-Money Laundering and Combating the Financing of Terrorism, and Proliferation Financing ", affiliated with the Presidential Court, and its formation and rules of procedure shall be determined by a resolution issued by the Cabinet. The Committee shall exercise the following competences:

1. To study, monitor, and evaluate the effectiveness of the strategies and measures adopted by the National Committee, and to issue recommendations and decisions thereon.

2. To determine the requirements to be followed and fulfilled by the National Committee and the Concerned Authorities in the performance of their duties, to issue the appropriate resolutions in that regard, and to supervise and monitor the implementation thereof.

3. To coordinate with and direct the Concerned Authorities to provide the necessary support to the National Committee in order to facilitate the performance and execution of its duties.

4. To issue decisions concerning the supervision of the Mutual Evaluation Process of the State with respect to combating Money Laundering, Financing of Terrorism, and Proliferation Financing.

5. To propose draft laws relating to its functions and those of the National Committee, and to propose amendments to existing relevant legislation and submit the same to the Cabinet.

6. To propose the required financial allocations for the federal entities concerned for implementing the national strategy for combating the Crime, following coordination with the Ministry, for submission to the Cabinet for approval within the Federal General Budget.

7. Any other competences and tasks determined by the Cabinet.

The Cabinet may delegate the Chairman of the Supreme Committee to issue its rules of procedure.

Article (13)

Pursuant to the provisions of this Decree by Law, a committee shall be established under the chairmanship of the Governor, to be known as the "National Committee for Combating Money Laundering, the Financing of Terrorism, and Proliferation Financing", the formation of which shall be determined by a resolution issued by the Cabinet, upon the proposal of the Minister.

Article (14)

The National Committee shall be competent for the following:

1. To establish and develop a National Strategy for combating the Crime, and to establish related regulations, procedures, and policies in coordination with the Concerned Authorities, and to follow up on their implementation.

2. To identify and assess the risks of the Crime at the national level.

3. To coordinate with the Concerned Authorities and refer to the relevant international information sources to identify high-risk countries and those suffering deficiencies in their regulations for combating Money Laundering, Financing of Terrorism, and Proliferation Financing, and to determine the countermeasures and other appropriate measures commensurate with the degree of risk, and to direct the Supervisory Authorities to verify the compliance of Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and Non-Profit Organizations with the application thereof, without obstructing or delaying their legitimate and charitable activities.

4. To coordinate among the represented entities to enhance the effectiveness of combating the Crime, and to facilitate operational cooperation and the timely exchange of information, whether automatically or upon request.

5. To assess the effectiveness of the national regulations for combating Money Laundering, Financing of Terrorism, and Proliferation Financing by collecting and analyzing statistics and other relevant information from the Concerned Authorities.

6. To monitor the Mutual Evaluation Process of the State to measure the extent of its compliance with the international standards for combating Money Laundering, Financing of Terrorism, and Proliferation Financing, and to submit proposals and recommendations to the Supreme Committee, and to implement the resolutions issued thereunder.

7. To represent the State in international fora related to combating Money Laundering, Financing of Terrorism, and Proliferation Financing.

8. To propose the organizational regulation governing its operations, and to submit the same to the Minister for approval.

9. To consider any matters referred thereto by the Concerned Authorities within the State.

10. Any other competences may be determined by the Executive Regulations of this Decree by Law.

Article (15)

1. The National Committee shall have a General Secretariat, headed by a Secretary-General, and shall include a number of employees.

2. The Secretary-General shall act as Deputy Chairman of the National Committee and as a member of the Supreme Committee and shall be appointed by a resolution of the Cabinet.

3. The organization of the General Secretariat, its organizational structure, determination of its competences, rules of procedure, and its financial and administrative regulations shall be determined by a decision issued by the Chairman of the Supreme Committee, upon the proposal of the Chairman of the National Committee. The Chairman of the Supreme Committee may delegate the Chairman of the National Committee to issue all or part of such decisions. In all cases, the Chairman of the National Committee shall be entitled to amend the

organizational structure of the General Secretariat below the level of departments.

Chapter Seven: Supervisory Authorities and Administrative Penalties

Article (16)

The Supervisory Authorities shall, within their respective areas of competence, undertake the duties of supervision, monitoring, and follow-up to ensure compliance with the provisions set forth in this Decree by Law, its Executive Regulations, and any other decisions issued thereby in connection therewith. In particular, the Supervisory Authorities shall have the following competences:

1. To conduct risk assessments concerning the likelihood of the Crime occurring within Financial Institutions, Designated Non-Financial Businesses and Professions, activities of Virtual Asset Service Providers, and Non-Profit Organizations.

2. To perform supervisory and inspection operations, whether desk-based or field-based, over Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and Non-Profit Organizations.

3. To maintain statistics on the measures undertaken and the penalties imposed.

4. Any other competences as provided under the provisions of this Decree by Law or as may be determined by its Executive Regulations.

Article (17)

1. Without prejudice to any more severe administrative sanction prescribed under any other legislation, the Supervisory Authority may impose the following administrative penalties upon Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and Non-Profit Organizations under its supervision, in the event of their violation of any provision of this Decree by Law, its Executive Regulations, or any other decisions issued thereby in connection therewith:

    a. Warning.

    b. An administrative fine of not less than ten thousand dirhams (AED 10,000) and not exceeding five million dirhams (AED 5,000,000) for each violation.

    c. Prohibiting the violator from engaging in the sector relevant to the violation for a period to be determined by the Supervisory Authority.

    d. Restricting the powers of board members, executive, supervisory, or managerial personnel, or owners proven responsible for the violation, including the appointment of a temporary supervisor.

    e. Suspending directors, board members, or executive or supervisory personnel proven responsible for the violation for a period to be determined by the Supervisory Authority or requesting their replacement.

    f. Suspending or restricting the activity or profession for a period to be determined by the Supervisory Authority.

g. Revocation of the license.

2. Notwithstanding Paragraph (G) of Clause (1) of this Article, the Supervisory Authority may, upon imposing administrative penalties, issue an order requiring the submission of periodic reports on the measures undertaken to remedy the violation.

3. The Supervisory Authority may impose an incremental administrative fine in the event of recurrence of the same violation within a period not exceeding one year from the date of the prior administrative fine imposed therefor.

4. In all cases, the Supervisory Authority may publish the administrative penalties imposed by it through various media outlets.

5. The mechanism for sharing the administrative fines imposed by local Supervisory Authorities shall be determined by a resolution of the Cabinet upon the recommendation of the Minister.

Chapter Eight: Preventive Measures, Transparency, and Beneficial Owners

Article (18)

1. Where Financial Institutions, Designated Non-Financial Businesses and Professions, or Virtual Asset Service Providers suspect, or have reasonable grounds to suspect, that a Transaction or Funds, in whole or in part, represent Proceeds or are related to or intended to be used in the Crime, regardless of their value, they shall notify the Unit without delay and directly, by providing a detailed report containing all available data and information concerning such Transaction and the relevant parties, through the electronic system designated by the Unit or by any other approved means, and shall furnish any additional information requested by the Unit, without invoking confidentiality provisions.

2. The provision of Clause (1) of this Article shall not apply to lawyers, notaries, other legal professionals, or independent legal auditors, where the information relating to such Transactions was obtained under circumstances subjecting them to professional secrecy.

3. The Executive Regulations of this Decree by Law shall determine the rules, controls, and cases requiring the reporting of Suspicious Transactions.

Article (19)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall comply with the following:

   a. Identify, understand, manage, assess, document, and continuously update the risks of the Crime within their business scope, taking into consideration the risk-based approach and the multiple aspects of risks as defined by the Executive Regulations of this Decree by Law, while retaining the risk assessment study and related information, and providing the same to the Supervisory Authority upon request.

   b. Implement Customer Due Diligence (CDD) Measures and continuous monitoring procedures, determining their scope based on the multiple risk dimensions and with due regard to the outcomes of the national risk assessment, while retaining the information obtained from implementing such measures. The

Executive Regulations shall specify the cases in which such measures apply, the types of measures, and the conditions for deferring the completion of Customer or Beneficial Owner identification.

c. Refrain from opening or maintaining accounts, or conducting any financial or commercial transactions, under anonymous, fictitious, alias, or numbered names, or providing any services thereto.

d. Establish internal policies, controls, and procedures, approved by senior management, enabling them to manage and mitigate identified risks, and to review and update the same on a continuous basis, ensuring their application to all branches and subsidiary companies in which they own a majority share. The Executive Regulations shall specify the minimum requirements of such policies, controls, and procedures.

e. Implement forthwith the instructions issued by the Executive Office or any other Competent Authorities concerning Targeted Financial Sanctions.

f. Retain all records, documents, and data relating to Transactions, whether domestic or international, ensuring their immediate availability to Competent Authorities upon request, pursuant to the provisions of the Executive Regulations of this Decree by Law.

g. Any other obligations stipulated in the Executive Regulations of this Decree by Law.

2. For the purposes of this Decree by Law, the Executive Regulations shall regulate the following:

a. The obligations of Non-Profit Organizations.

b. The obligations of the Registrar and Competent Authorities regulating Legal Arrangements.

c. The obligations of companies, nominee directors, and nominee shareholders.

d. The obligations pertaining to the Legal Arrangement, the Trustee, and any person occupying an equivalent position.

3. The Cabinet shall issue a resolution regulating the procedures of identifying the Beneficial Owner.

Article (20)

No natural or legal person shall engage in any Financial Activities, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, or Virtual Asset Service Provider activities without obtaining a license, registration, or enrolment from the Competent Authority or from the relevant Supervisory Authority, as the case may be.

Chapter Nine: International Cooperation and Asset Recovery

Article (21)

Without prejudice to the legislation in force within the State and to the provisions of the treaties or conventions to which the State is a party, or under the condition of reciprocity, the following shall apply:

1. None of the following shall constitute a ground for refusal of a request for international cooperation:

    a. That the request involves matters of a financial, customs, or direct or indirect tax nature.

    b. The mandatory confidentiality provisions applicable to Financial Institutions, DNFBPs, and Virtual Asset Service Providers, unless the relevant information has been obtained under circumstances wherein legal professional privilege or professional secrecy applies.

    c. Any other cases specified in the Executive Regulations hereof.

2. Any judgment or judicial order issued by a competent court or judicial authority in another State providing for provisional measures or for Confiscation in any of its forms of Criminal Property or of Funds equivalent in value thereto, relating to a Predicate Offence or Money Laundering, may be executed without the need for national investigations.

3. The Concerned Authorities shall accord priority to all requests for international cooperation, particularly those related to the Crime, and shall execute such requests expeditiously; they shall exchange information with competent foreign authorities, both counterpart and non-counterpart, automatically and upon request, and shall take effective measures to preserve the confidentiality of the information received and to use the same solely for the purpose for which it was requested or provided.

4. The competent judicial authorities, upon request from a judicial authority in another State, shall provide mutual legal assistance in investigations, prosecutions, or proceedings related to the Crime, and may order the following:

    a. The identification, tracing, evaluation, Seizure, Freezing, or Confiscation of Funds, Criminal Property, or funds of equivalent in value, or any other measures applicable in accordance with the legislation in force within the State, including the provision of records held by Financial Institutions, DNFBPs, Virtual Asset Service Providers, or NonProfit Organizations; the search of persons and premises; the taking of witness statements; the obtaining of evidence; and the use of investigative techniques such as Undercover Operations, interception of communications, electronic data and information gathering, and Controlled Delivery.

    b. The surrender and recovery of persons and Criminal Property.

5. The Concerned Authorities shall exchange, to the maximum extent possible, information related to the Crime with competent foreign authorities, obtain on their behalf any other required information, and execute the requests received therefrom.

6. The Executive Regulations of this Decree by Law shall determine the rules, controls, and procedures governing international cooperation.

Article (22)

1. The Cabinet shall, based upon a proposal from the Minister and after coordination with the Concerned Authorities, issue a resolution regarding the determination and regulation of the procedures for the recovery and management of assets that are Seized, Frozen, or subject to Confiscation, provided that such resolution specifies the entities responsible for Asset Recovery and management and the circumstances of their disposal.

2. Subject to the procedures of sharing Criminal Property or Funds equivalent in value thereto, the proceeds of their sale, upon the issuance of a final judgment of Confiscation, shall remain charged, within their value, with any rights lawfully vested in any bona fide party.

3. The Concerned Authorities shall cooperate, coordinate, and exchange information among themselves in order to enhance the effectiveness of Asset Recovery.

Chapter Ten: Statistics

Article (23)

1. The Concerned Authorities shall maintain comprehensive statistics on Suspicious Transactions reports, investigations, judgments related to the Crime, Funds Frozen, Seized, and Confiscated, requests for international cooperation, and any statistics pertaining to the effectiveness and adequacy of the measures combating the Crime.

2. The General Secretariat shall, in coordination and cooperation with the Concerned Authorities, maintain a centralized national statistical database regarding the combating of Money Laundering, Financing of Terrorism, and Proliferation Financing, ensuring the quality, consistency, and regular updating of the data.

Chapter Eleven: Confidentiality of Information

Article (24)

Information obtained in relation to Suspicious Transactions or to any of the Crimes stipulated in this Decree by Law shall be deemed confidential, and may only be disclosed to the extent necessary for its use in investigations or proceedings related to violations of the provisions of this Decree by Law, or in other cases permitted by law.

Chapter Twelve: Penalties

Article (25)

The penalties prescribed in this Decree by Law shall be imposed without prejudice to any more severe penalty provided for in any other law.

Article (26)

1. Whoever commits the Crime of Money Laundering shall be punished with imprisonment for a term not less than one (1) year and not exceeding ten (10) years, together with a fine of not less than one hundred thousand dirhams (AED 100,000) and not exceeding five million dirhams (AED 5,000,000), or an amount equivalent to the value of the relevant Criminal Property; whichever is greater.

2. The penalty shall be temporary imprisonment and a fine of not less than one million dirhams (AED 1,000,000) and not exceeding ten million dirhams (AED 10,000,000), or an amount equivalent to twice the value of the relevant Criminal Property; whichever is greater, if the perpetrator commits the Crime of Money Laundering in any of the following circumstances:

a. Where they exploit their influence or authority conferred upon them by virtue of their position or professional activity;

b. Where the act is committed through a Non-Profit Organization;

c. Where the act is committed through an organized criminal group;

d. Where the Predicate Offence is one of the crimes set forth in Chapter Seven of Part One or Chapter One of Part Two of Book Two of Federal Decree by Law No. (31) of 2021 referred to hereinabove, or in Federal Decree by Law No. (30) of 2021 referred to hereinabove;

e. In case of recidivism.

3. Whoever commits the Crime of Financing of Terrorism shall be punished with life imprisonment or temporary imprisonment for a term not less than ten (10) years, and a fine of not less than one million dirhams (AED 1,000,000) and not exceeding ten million dirhams (AED 10,000,000), or an amount equivalent to twice the value of the relevant Criminal Property; whichever is greater.

4. Whoever commits the Crime of Proliferation Financing shall be punished with temporary imprisonment and by a fine of not less than one million dirhams (AED 1,000,000) and not exceeding ten million dirhams (AED 10,000,000), or an amount equivalent to twice the value of the relevant Criminal Property; whichever is greater.

5. The attempt to commit the crimes of Money Laundering, Financing of Terrorism, and Proliferation Financing shall be punishable with the same penalty prescribed for the consummated crime.

6. The Court may, upon the request of the Attorney General or their delegate, or sua sponte, mitigate or exempt from the penalty prescribed in this Article any offender who voluntarily provides the judicial or administrative authorities with information concerning any of the crimes punishable under this Article, if such information leads to their disclosure, the identification or apprehension of their perpetrators, the establishment of proof against them, or the seizure of the Criminal Property.

Article (27)

1. Without prejudice to any more severe penalty prescribed by another law, every legal person whose representatives, directors, or agents have, on its behalf or in its name, committed the Crimes of Money Laundering, Financing of Terrorism, or Proliferation Financing, shall be punished with a fine of not less than five million dirhams (AED 5,000,000) and not exceeding one hundred million dirhams (AED 100,000,000), or an amount equivalent to the value of the Criminal Property involved; whichever is greater.

2. Every legal person whose representatives, directors, or agents have, on its behalf or in its name, committed any of the offences punishable under Articles (28), (29), (30), (32), (33), (34), or (35) hereof, shall be punished with a fine of not less than two hundred thousand dirhams (AED 200,000) and not exceeding ten million dirhams (AED 10,000,000).

3. In case of conviction of the legal person for the Financing of Terrorism or the Proliferation Financing, the Court shall order its dissolution and the closure of the premises wherein its activity is conducted.

4. The Court may, in case of conviction of the legal person for the Crime of Money Laundering, or in the event of violation of Article (10) of this Decree by Law, order its dissolution and the closure of its premises.

5. In the cases where any of the Crimes referred to in Clauses (1) and (2) of this Article are committed, the person responsible for the actual management of the legal person shall be punished by imprisonment and a fine, or by either of the two penalties, if it is proven that they were aware thereof and that the commission of such Crime was due to their breach of the duties of their position.

6. The Court, upon pronouncing a conviction, may order the publication of a summary of the judgment by appropriate means, at the expense of the convicted person.

Article (28)

Whoever deliberately or through gross negligence violates the provisions of Article (18) hereof shall be punished by imprisonment and a fine of not less than one hundred thousand dirhams (AED 100,000) and not exceeding one million dirhams (AED 1,000,000), or by either of these two penalties.

Article (29)

1. Any person who notifies or warns another person, or discloses any information related to Transactions under review concerning Suspicious Transactions, or reveals that the Competent Authorities are conducting inquiries or investigations in respect thereof, in contravention of Article (24) hereof, shall be punished by imprisonment and a fine of not less than fifty thousand dirhams (AED 50,000), or by either of these two penalties.

2. Any person who deliberately or through gross negligence breaches the duties of managing the Funds entrusted to them, or violates any order issued by a competent authority regarding Seizure, Freezing, or other precautionary measures, shall be punished by imprisonment and a fine of not less than fifty thousand dirhams (AED 50,000), or by either of these two penalties.

3. The punishment shall be imprisonment for a period of not less than one year and a fine equal to the value of the Proceeds, provided that such fine shall not be less than one hundred thousand dirhams (AED 100,000), in the event that any of the acts mentioned in Clauses (1) and (2) of this Article result in the inability to seize the Proceeds, or in their destruction or loss of value.

Article (30)

1. Any person who possesses, conceals, or conducts any Transaction in Funds where there are sufficient indications or evidence suggesting the illegitimacy of their source, or the concealment of the Beneficial Owner thereof, shall be punished by imprisonment for a period not less than three (3) months and a fine of not less than fifty thousand dirhams (AED 50,000), or by either of these two penalties.

2. Any person who promotes, offers for sale, provides services, or deals in Virtual Assets characterized by total anonymity, or that prevent or obstruct the ability of the Competent Authorities to trace the Transaction or its parties, or any unlicensed accounts or technologies allowing such concealment, shall be punished by imprisonment for a period not less than three (3) months and a fine of not less than fifty thousand dirhams (AED 50,000), or by either of these two penalties.

3. Upon conviction, the Court shall order Confiscation in accordance with the provisions of Article (31) hereof.

Article (31)

1. Where the Crime is proven, the Court shall order the Confiscation of the following:

    a. The Criminal Property;

    b. Any Funds owned by the offender equivalent to the value of the Criminal Property, in cases where such property has been mingled with legitimate Funds, cannot be seized, or is subject to the rights of bona fide third parties.

2. Confiscation shall be enforced irrespective of whether the Criminal Property is in the possession or ownership of the offender or of another party, without prejudice to the rights of bona fide third parties.

3. If it is impossible to order Confiscation of the Criminal Property or of Funds equal in value thereto, due to their unavailability or the existence of bona fide third-party rights, the Court shall impose a fine equivalent to their value at the time of the commission of the Crime.

4. The anonymity of the perpetrator, the absence of their criminal liability, or the lapse of the criminal case in relation to a punishable Crime pursuant to the provisions of this Decree by Law shall not preclude the Court, sua sponte or upon the request of the Public Prosecution, as the case may be, from ordering Confiscation of the seized Criminal Property if its connection to the Crime is established.

Article (32)

Any person who violates the provisions of Article (20) of this Decree by Law shall be punished by imprisonment and a fine of not less than two hundred thousand dirhams (AED 200,000) and not exceeding ten million dirhams (AED 10,000,000), or by either of these two penalties.

Article (33)

Any person who violates the instructions issued by the Executive Office or any other Competent Authority related to Targeted Financial Sanctions shall be punished with imprisonment and a fine of not less than twenty thousand dirhams (AED 20,000), or by either of these two penalties.

Article (34)

Any person who violates the provisions of Article (10) of this Decree by Law, or refrains from providing additional information where requested, or deliberately conceals information required to be disclosed, or knowingly provides false information, shall be punished by imprisonment and a fine, or by either of these two penalties. The Court may, upon conviction, order the Confiscation of the seized Funds, without prejudice to the rights of bona fide third parties.

Article (35)

1. Any person who intentionally provides false or misleading information concerning the Beneficial Owner to any Competent Authority requesting such information, or to Financial Institutions, DNFBPs, or Virtual Asset Service Providers, shall be punished by imprisonment and a fine of not less than twenty thousand dirhams (AED 20,000), or by either of these two penalties.

2. Any person who unlawfully enables another person to benefit from their account with a Financial Institution or a Virtual Asset Service Provider, while knowing, or having sufficient grounds to believe, that such use is intended for the misuse of the account, shall be punished by imprisonment and a fine, or by either of these two penalties.

3. Any person who violates the provisions of Clause (1) and paragraphs (A), (C), and (D) of Clause (2) of Article (19) of this Decree by Law shall be punished by imprisonment and a fine of not less than ten thousand dirhams (AED 10,000), or by either of these two penalties.

Article (36)

1. Where a foreigner is punished with a custodial sentence due to the commission of the Crime of Money Laundering or any of the felonies stipulated in this Decree by Law, the judgment must include an order for their deportation from the State.

2. Without prejudice to the provision of Clause (1) of this Article, where a foreigner is convicted, in relation to other misdemeanors stipulated in this Decree by Law and sentenced to a custodial penalty, the court may order their deportation from the State, or impose deportation in lieu of the custodial penalty.

Article (37)

1. No criminal, civil, or administrative liability shall be incurred by the Supervisory Authorities, the Unit, the Law Enforcement Authorities, the Financial Institutions, the DNFBPs, the Virtual Asset Service Providers, or by the members of their Boards of Directors, employees, and legally authorized representatives, as a result of furnishing any of the required information or breaching any statutory, contractual, or administrative restriction imposed to ensure the confidentiality of information, even if they were not fully aware of the nature or actual occurrence of the Crime, unless it is proven that the reporting was made mala fide with the intent to harm others.

2. The criminal proceedings shall not lapse by prescription in relation to the crimes of Money Laundering, Financing of Terrorism, or Proliferation Financing, nor shall the imposed penalties extinguish by lapse of time; likewise, the civil actions arising therefrom or connected therewith shall not lapse by prescription.

3. The provisions of this Decree by Law shall not prejudice the provisions of Federal Law No. (7) of 2014 referred to herein above.

4. The Crime punishable under Article (33) of this Decree by Law, where it jeopardizes the security or interests of the State, as well as the crimes of Financing of Terrorism and Proliferation Financing, shall be deemed offences affecting the internal and external security of the State.

Chapter Thirteen: Final Provisions

Article (38) Judicial Enforcement

By virtue of a resolution issued by the Minister of Justice or the Head of the competent local judicial authority, in coordination with the competent minister or authority, certain employees may be vested with the capacity of Judicial Officers to detect the acts committed in contravention of the provisions of this Decree by Law, its Executive Regulations, or the regulations, resolutions, and circulars issued pursuant thereto.

Article (39) Violations and Administrative Penalties

The Cabinet shall, upon the proposal of the Minister and after coordination with the Supervisory Authority, issue a resolution prescribing the violations and administrative penalties applicable to acts committed in contravention of the provisions of this Decree by Law and its Executive Regulations, specifying the entities responsible for imposing

such sanctions, the mechanism for grievance thereagainst, and the entity entrusted with the collection of administrative fines.

Article (40) Executive Regulations

The Cabinet shall, upon the proposal of the Minister, issue the Executive Regulations of this Decree by Law.

Article (41) Repeals

1. Federal Decree by Law No. (20) of 2018, referred to herein above, shall hereby be repealed.

2. Any provision that contradicts or conflicts with the provisions of this Decree by Law shall hereby be repealed.

3. The Executive Regulations, resolutions, and circulars issued pursuant to Federal Decree by Law No. (20) of 2018 and are in force as of the date of issuance of this Decree by Law shall remain effective insofar as they do not conflict with the provisions hereof, until the regulations, resolutions, and circulars that supersede the same are issued.

Article (42) Publication and Entry into Force

This Decree by Law shall be published in the Official Gazette and shall enter into force (2) two weeks after the date of its publication.

Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing

CAB RES 134/2025 Effective from 14/12/2025 **Status:** In-Force

The Cabinet:

– Having reviewed the Constitution;

– Federal Law No. (1) of 1972 Regarding the Competences of the Ministries and the Powers of Ministers, as amended;

– Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing;

– Cabinet Resolution No. (10) of 2019 Regarding the Executive Regulations of Federal Decree by Law No. (20) of 2018 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Illegal Organizations, as amended;

– Upon the proposal of the Minister of Finance, and the approval of the Cabinet; Hereby resolves as follows:

Hereby resolves as follows:

Chapter One: Definitions

Article (1)

The definitions set forth in Federal Decree by Law No. (10) of 2025, referred to hereinabove, shall apply to this Resolution. In addition, the following terms and expressions shall have the meanings assigned to each of them, unless the context requires otherwise:

Companies:	Companies, regardless of their type or activity, that are subject to the provisions of the legislation in force in the State.
Senior Management:	The person or persons vested with authority to take strategic and executive decisions materially affecting risk management, compliance policies, and operational governance, including chief executive officers, general managers, members of the board of directors, or any person occupying a position that enables them to directly influence the conduct of business and internal policies, including compliance policies.
Intermediary Financial Institution:	A Financial Institution that, in the payment chain, receives and transmits a funds transfer between the originating Financial Institution and the Beneficiary Financial Institution, or another Intermediary Financial Institution.
Beneficiary Financial Institution:	The Financial Institution that receives the transfer from the originating Financial Institution, either directly or through an Intermediary Financial Institution, for the benefit of the Beneficiary, and which constitutes the end point in the payment chain.
Financial Institutions:	Any person engaging in one or more financial activities or operations for the benefit of, or on behalf of, a Customer, as stipulated in Article (2) of this Resolution.
Designated Non-Financial Businesses and Professions (DNFBPs):	Any person engaging in one or more commercial or professional activities or businesses for the benefit of, or on behalf of, a Customer, as stipulated in Article (3) of this Resolution.
Commercial Gaming:	Any game of chance, or any form of chance-based or skill based practice, involving the placement of a monetary stake for the purpose of winning money or any other item of value, including agreements whereby the loser must compensate the winner with money or any other agreed consideration. This includes, without limitation, lottery operations, Commercial Gaming halls, internet gaming, sports wagering, and any other licensed games of chance or opportunity regulated by the General Commercial Gaming Regulatory Authority, whether conducted within gaming premises or elsewhere.
Commercial Gaming Operators:	Any person who carries out the operation of Commercial Gaming halls, internet Commercial Gaming, sports betting, or lottery gaming.
Virtual Asset Service Providers:	Any person who, as a commercial activity, conducts one or more Virtual Asset activities or related operations for the benefit of, or on behalf of, another natural or legal person, as stipulated in Article (4) of this Resolution.
Trust Protector:	A natural or legal person appointed pursuant to a Trust deed and granted powers and authorities for the purpose of protecting the Trust, ensuring its proper administration, and achieving its objectives, without such powers prejudicing its legal independence or resulting in the transfer of assets to the benefit of the settlor, or the settlor's effective control over them.
Nominator:	One or more natural or legal persons who issue instructions, directly or indirectly, to a nominee acting on their behalf as a Nominee Director or Nominee Shareholder of a legal person.

Nominee Shareholder:	A natural or legal person who exercises voting rights in accordance with the instructions of the Nominator, or receives dividends on their behalf, and shall not be deemed the Beneficial Owner of a legal person by virtue of holding shares in a nominee capacity.
Nominee Director:	A natural or legal person who customarily performs management functions in a company on behalf of the Nominator and in accordance with their instructions, and shall not be deemed the Beneficial Owner of a legal person.
Beneficial Owner:	The natural person who owns or exercises ultimate effective control over the Customer, or the natural person on whose behalf Transactions are conducted, including any natural person exercising ultimate effective control over a legal person or Legal Arrangement, whether directly or through a chain of ownership or control or by any other indirect means, and who is identified, whether one or more persons, in accordance with Article (10) of this Resolution.
Reasonable Measures:	Measures taken within the framework of Customer Due Diligence and Beneficial Owner identification procedures, proportionate to the risks of Money Laundering, Financing of Terrorism, or Proliferation Financing.
Business Relationship:	Any ongoing commercial or financial relationship established between Financial Institutions, DNFBPs, or Virtual Asset Service Providers and their Customer, in connection with the activities or services they provide to the Customer.
Correspondent Banking Relationship:	A relationship between a correspondent Financial Institution and a respondent institution through a current account, or any other type of account or related service, including correspondent relationships established for securities transactions or funds transfers.
Payable-Through Accounts:	Correspondent accounts used directly by third parties to conduct transactions on their behalf.
Financial Group:	A group of Financial Institutions consisting of a holding company or another Legal Person that exercises control over the rest of the group, and coordinates functions for the purpose of applying supervision at the group level, across its branches and subsidiaries, in accordance with International Core Principles for Financial Supervision and the anti-money laundering and combating terrorism financing policies and procedures.
International Core Principles for Financial Supervision:	The Basel Committee's Core Principles for Effective Banking Supervision (Principles 1–3, 5–9, 11–15, 26, and 29); The International Association of Insurance Supervisors Core Principles (Principles 1, 3–10, 18, 21–23, and 25); The International Organization of Securities Commissions Principles (Principles 24, 28, 29, and 31) and Responsibilities (A, B, C, and D).
Wire Transfer:	Any operation for the electronic funds transfer conducted by a Financial Institution or a Virtual Asset Service Provider on behalf of an originator, whereby funds are transmitted to a specified Beneficiary at another Financial Institution, Virtual Asset Service Provider, or virtual wallet, whether the originator and beneficiary are the same person or different persons.
Shell Bank:	A bank incorporated or licensed in a jurisdiction in which it has no physical presence, and is not affiliated with a regulated Financial Group.
Population Register:	The State Population Register, which includes individual data and civil events, as regulated by Federal Law No. (9) of 2006 Regarding the Population Register and Identity Card System, as amended.

High-Risk Customers: Customers who present heightened risk due to their personal profile, activities, the nature of the Business Relationship, or geographic location, including customers from high-risk countries, non-residents not holding a State issued identity card, customers with complex ownership structures, customers conducting complex or economically or legally unjustified Transactions, customers engaging in large cash Transactions, Transactions with unknown third parties, or any other high-risk Transactions as determined by Financial Institutions, DNFBPs, Virtual Asset Service Providers, or the Supervisory Authority.

Politically Exposed Persons (PEPs): Natural persons entrusted with, or have been previously entrusted with, prominent public functions in the State or in any other country, such as Heads of State or Government, senior politicians, senior government officials including judicial or military officials, senior executive managers of state-owned enterprises, senior political party officials, and persons entrusted with, or have previously been entrusted with, the management of international organizations or any prominent function therein, including members of Senior Management such as directors, deputy directors, members of the board of directors, or persons of equivalent positions. This definition includes:

1. Immediate family members of the politically exposed person, such as spouses, children and their spouses, and parents;

2. Persons known to be close associates of the politically exposed person, including:

    a. Persons having joint beneficial ownership of a legal person or Legal Arrangement, or any other close professional or social relationships with a PEP;

    b. Persons having sole beneficial ownership of a legal person or Legal Arrangement that has been established for the benefit of a PEP.

Adequate Information: In the context of legal persons; information that is available or can be obtained to identify the Beneficial Owner and the means by which ownership or control is exercised, including full name, nationality, date and place of birth, residential address, identity number and type, tax registration number, if any, and any other information required for this purpose. In the context of Legal Arrangements; information used to identify the natural persons who are the Beneficial Owners thereof and their roles, including information on the Trustee, Settlor, Protector, if any, Beneficiary, or, as the case may be, class of Beneficiaries and the authorities and powers granted thereto, and any other person exercising ultimate effective control over the Legal Arrangement or occupying a similar or equivalent position.

Accurate Information: Information that has been verified for accuracy. In the context of legal persons; information that has been verified to confirm its accuracy through the verification of the identity and status of the Beneficial Owner using original documents, data, or information obtained from a reliable and independent source. The extent of the verification measures may vary according to the identified level of risk. Where there is a discrepancy in the information, necessary supplementary measures shall be taken to confirm the accuracy of the Beneficial Owner's information. In the context of Legal Arrangements, information that has been verified to confirm its accuracy through the verification of the identity and status of the Beneficial Owner, using reliable documents, data, or information. The extent of verification measures may vary according to the identified level of risk. Where there is a discrepancy in the information, necessary supplementary measures shall be taken to confirm the accuracy of the Beneficial Owner's information.

Up-to-Date Information:	In the context of legal persons, information that is as current as possible and updated within a reasonable, specified timeframe following any change. In the context of Legal Arrangements, information that is as current as possible and updated within a reasonable timeframe. However, where Beneficiaries are designated by characteristics or class, Trustees or persons in equivalent or similar positions are not required to obtain complete Adequate and Accurate Information until a Beneficiary becomes entitled at the time of payment or seeks to exercise vested rights, in accordance with the risk-based approach.
Decree by Law:	Federal Decree by Law No. (10) of 2025 Regarding Anti Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

Chapter Two: Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, and Non-Profit Organizations

Part One: Financial Institutions and Designated Non-Financial Businesses and Professions

Division One: Nature of Financial Institutions and Designated Non-Financial Businesses and Professions

Article (2)

Financial Institutions shall include any person who, as a commercial activity, carries out one or more of the following financial activities or operations for the benefit of, or on behalf of, a Customer:

1. Acceptance of deposits and other repayable funds from the public.
2. Lending, including consumer loans and mortgage loans, with or without recourse, and the financing of commercial transactions, including the purchase of export documents and the purchase of debts, whether with or without recourse.
3. Financial leasing, excluding financial leasing related to consumer products.
4. Money or value transfer services, excluding any natural or legal person who solely provides Financial Institutions with messaging or other support systems for the transfer of funds.
5. Issuance and management of means of payment, including debit cards, credit cards, cheques, payment orders, banker drafts, and electronic money.
6. Guarantees and financial commitments.
7. Trading in financial market instruments such as cheques, bills of exchange, certificates of deposit, derivatives, and others; or foreign exchange, currency exchange instruments, interest rates, indices, other financial derivatives, or tradable financial instruments; and trading in commodity futures contracts.

8. Participation in the issuance of securities and the provision of financial services related to such issuances.

9. Management of funds and portfolios of all types.

10. Safekeeping and administration of cash or liquid securities on behalf of others.

11. Other operations for investing, managing, or operating funds or monies on behalf of others.

12. Subscription to, or savings in, life insurance policies and other types of investment-related insurance, including those provided by insurance agents and brokers.

13. Money or currency exchange.

14. Any other financial activities or operations as may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Article (3)

Designated Non-Financial Businesses and Professions (DNFBPs) shall include any person who carries out one or more of the following commercial or professional activities or businesses:

1. Commercial Gaming Operators, including Commercial Gaming conducted on board vessels or marine craft, when conducting a single financial transaction or several transactions that appear to be linked and whose value equals or exceeds eleven thousand dirhams (AED 11,000).

   A financial transaction shall not include a transaction that solely involves gaming chips or gaming instruments.

2. Real estate brokers and agents, when concluding transactions or settlements on behalf of their customers in relation to the purchase or sale of real estate.

3. Dealers in valuable metals and precious stones, when carrying out any single cash transaction or several transactions that appear to be linked and whose value equals or exceeds fifty-five thousand dirhams (AED 55,000).

4. Lawyers, notaries, other independent legal professionals, and independent accountants, whether practicing individually, as partners, or as professionals within a firm practicing such profession, when they prepare, conduct, or execute financial transactions on behalf of their customers in relation to the following activities:

   a. Buying and selling real estate;

   b. Managing funds owned by the customer ;

   c. Managing bank accounts, savings accounts, or securities accounts;

   d. Organizing contributions for the establishment, operation, or management of Companies;

   e. Establishing, operating, managing legal persons or Legal Arrangements, or selling, or purchasing commercial entities.

5. Company and Trust Service Providers, when carrying out or executing any transaction for the benefit of, or on behalf of, their customers in relation to the following activities:

a. Acting as an agent in the incorporation or establishment of Legal Persons;

b. Acting, or arranging for another person to act, as a director or secretary of a company, or as a partner or in a similar position in another Legal Person;

c. Providing a registered office, business address, place of residence, correspondence address, or administrative address for a company, any legal person, or a Legal Arrangement;

d. Acting, or arranging for another person to act, as a Trustee of an express Trust or performing an equivalent function for another form of Legal Arrangement;

e. Acting, or arranging for another person to act, as a Nominee Shareholder for another person.

6. Any other businesses or professions may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Article (4)

Virtual Asset Activities shall include the following activities or operations:

1. Exchange between Virtual Assets and fiat currencies.

2. Exchange between one or more types of Virtual Assets.

3. Transfer of Virtual Assets.

4. Safekeeping or administration of Virtual Assets or instruments enabling control over Virtual Assets.

5. Provision of financial services or activities related to an issuer's offer or sale of Virtual Assets, or participation therein.

6. Any other activities or operations as may be determined by a resolution issued by the Supervisory Authority, in coordination with the National Committee.

Division Two: Risk Identification and Risk Mitigation

Article (5)

1. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall identify, understand, manage, and assess their crime risks in a manner proportionate to the nature and size of their business, taking into account the risk-based approach and the results of the National Risk Assessment, and shall comply with the following:

    a. Consider all relevant risk factors, such as Customer risks, countries and geographic risk, product, service, transaction, and delivery channel risks, prior to determining the overall level of risk and the appropriate level of risk mitigation measures to be applied.

    b. Document the processes for identifying and assessing risks and the information related thereto, retain the relevant study, update it on an ongoing basis, and provide it to the concerned authorities upon

request.

2. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall mitigate the crime risks identified pursuant to Clause (1) of this Article, taking into account the risk-based approach, the results of the National Risk Assessment, and sectoral assessments, and shall comply with the following:

   a. Establish internal policies, controls, and procedures approved by Senior Management, enabling them to manage and mitigate the identified risks, and review and update them on an ongoing basis.

   b. Ensure that such internal policies, controls, and procedures are proportionate to the nature and size of their business, and monitor their implementation, assess their effectiveness, and enhance them where necessary, in accordance with Article (21) of this Resolution.

   c. Apply Enhanced Due Diligence measures for the management and mitigation of identified risks, including, by way of example:

      1) Obtaining and verifying additional information, such as information on the Customer's identity and occupation, the Beneficial Owner, the amount of funds, and information available through public databases and open sources;

      2) Obtaining additional information on the purpose of the Business Relationship or the reasons for expected Transactions or Transactions that have actually been carried out;

      3) Updating Customer Due Diligence information on the Customer and the Beneficial Owner more regularly;

      4) Taking Reasonable Measures to identify the source of funds and wealth of the Customer and the Beneficial Owner;

      5) Increasing the degree and level of ongoing monitoring of the Business Relationship to determine whether it appears unusual or suspicious, and selecting Transaction patterns requiring further scrutiny and review;

      6) Carrying out the first payment through an account in the Customer's name held with a Financial Institution subject to equivalent Due Diligence standards;

      7) Obtaining approval from Senior Management to commence or continue the Business Relationship with the Customer.

3. Financial Institutions, DNFBPs, and Virtual Asset Service Providers may, upon fulfilling the requirements set out in Clauses (1) and (2) of this Article, and in coordination with the Supervisory Authority, apply Simplified Due Diligence measures to manage crime risks where low risks are identified, unless there is a suspicion that a crime has been committed.

   Such Simplified Due Diligence measures shall be proportionate to the elements of low risk and shall ensure full implementation of the instructions issued by the Executive Office or other Competent Authorities in relation to Targeted Financial Sanctions, and may include, by way of example, the following:

   a. Verifying the identity of the Customer and the Beneficial Owner after the commencement of the Business Relationship;

b. Updating Customer data at longer intervals;

c. Reducing the frequency of ongoing monitoring and Transaction scrutiny;

d. Inferring the purpose and nature of the Business Relationship from the type of Transaction or the Business Relationship established, without the need to collect information or undertake specific procedures.

4. Where high risks related to Proliferation Financing are identified, Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall take proportionate measures to manage and mitigate such risks. This includes, by way of example, the following:

a. Adopting enhanced internal controls aimed at detecting and preventing potential violations of, non-implementation of, or circumvention of instructions of the Executive Office or other relevant Competent Authorities relating to Targeted Financial Sanctions, and conducting ongoing enhanced scrutiny of the Business Relationship to ensure full compliance;

b. Maintaining documented records of the measures taken and making them available to the competent authorities upon request;

c. Conducting periodic reviews of internal controls in line with changes in the level of risk.

Division Three: Customer Due Diligence and Beneficial Owner Identification Procedures

Article (6)

1. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall verify the identity of the Customer and the Beneficial Owner before or during the establishment of a Business Relationship or the opening of an account, or prior to carrying out a Transaction for a Customer with whom no such relationship exists.

2. In cases of low crime risk, Financial Institutions, DNFBPs, and Virtual Asset Service Providers may defer the completion of Customer identity verification until after the establishment of the Business Relationship, subject to the following conditions:

a. Verification shall be completed as soon as possible after the commencement of the Business Relationship or execution of the Transaction;

b. The deferral shall be necessary so as not to disrupt the normal course of business;

c. Appropriate and effective measures shall be applied to control the risks of the Crime.

3. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall take measures to manage risks in circumstances where the Customer is able to benefit from the Business Relationship prior to the completion of the verification process.

Article (7)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers, as applicable, shall apply Customer Due Diligence measures in the following cases:

    a. Upon the commencement of a Business Relationship;

    b. Where there is suspicion of a Crime;

    c. Where there are doubts as to the accuracy or adequacy of Customer identification data previously obtained.

2. Financial Institutions shall apply Customer Due Diligence measures in the following cases:

    a. When conducting occasional Transactions for a Customer amounting to or exceeding fifty-five thousand dirhams (AED 55,000), whether carried out as a single Transaction or several Transactions that appear to be linked;

    b. When conducting occasional Transactions in the form of Wire Transfers amounting to or exceeding three thousand five hundred dirhams (AED 3,500).

3. Virtual Asset Service Providers shall apply Customer Due Diligence measures when conducting occasional Transactions amounting to or exceeding three thousand five hundred dirhams (AED 3,500), whether carried out as a single Transaction or several Transactions that appear to be linked.

Article (8)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Customer Due Diligence measures and conduct ongoing monitoring in respect of the Business Relationship, which shall include the following:

1. Scrutinizing Transactions carried out throughout the duration of the Business Relationship to ensure that such Transactions are consistent with the information available thereto regarding the Customer, the nature of their activities, and the risks they represent, including, where necessary, the source of funds.

2. Ensuring that documents, data, or information obtained as part of Customer Due Diligence measures are up to date and relevant, through reviewing records, with particular emphasis on records relating to categories of High-Risk Customers.

Article (9)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall identify the Customer, whether permanent or occasional, and determine whether the Customer is a natural person, Legal Person, or Legal Arrangement, and shall verify such identity using original documents, data, or information obtained from a reliable and independent source, as follows:

    a. In respect of Customers who are natural person, obtaining the name as stated in the identity card or travel document, nationality, address, date and place of birth, and, where applicable, the name and address of the employer, together with a true copy of a valid identity card or travel document;

    b. In respect of Customers who are Legal Persons or Legal Arrangements, obtaining the following basic information:

1) Name, legal form, memorandum of association, tax registration number of the Legal Persons subject to corporate tax, and the unique reference number, if any;

2) Address of the registered office or principal place of business, and where the Person is foreign, the name and address of its legal representative in the State, if any, together with supporting evidence;

3) Articles of association or any other equivalent approved documents;

4) Names of relevant persons holding Senior Management positions within the Legal Person or Legal Arrangement.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall verify that any person acting on behalf of the Customer is duly authorized to do so, and shall identify such person in accordance with Clause (1) of this Article.

3. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall understand the purpose and the intended nature of the Business Relationship and obtain information relating thereto where necessary.

4. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall understand the nature of the Customer's business and the ownership and control structure thereof.

Article (10)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall take into account the risks of the Crime arising from the Customer and the Business Relationship, identify the Beneficial Owner of Legal Persons and Legal Arrangements, and take Reasonable Measures to verify such identity using documents, data, or information obtained from a reliable and independent source, in a manner that enables them to be satisfied that the Beneficial Owner's identity has been determined, as follows:

1. Customers that are Legal Person:

    a. Obtaining the identity of the natural person who ultimately owns, whether individually or jointly with another person, an actual controlling ownership interest or shares in the Legal Person of 25% (twenty-five percent) or more;

    b. Where there is doubt as to the identification of the natural person under paragraph (a) of this Clause, or doubt that the natural person who owns an ownership interest or controlling shares is the Beneficial Owner, or where no natural person exercises control through ownership interest, the identity of the natural person who exercises legal or actual control over the Legal Person , or through any other means, whether directly or indirectly, shall be identified;

    c. Where no natural person is identified pursuant to paragraphs (a) and (b) of this Clause, identifying the relevant natural person holding a Senior Management position shall be identified, whether one or more persons.

2. Customers that are Legal Arrangement:

    a. Identifying the identity of the Trustee, Settlor, Trust Protector, Beneficiaries, or classes of Beneficiaries, and the powers and authorities granted thereto where no Beneficiaries are identifiable at the time of

establishment of the Trust;

b. Identifying the identity of any other natural person exercising ultimate effective control, including through a chain of ownership or control over the trust, whether directly or indirectly;

c. Obtaining adequate information regarding the Beneficial Owner to enable the identification thereof at the time of payment or when the Beneficial Owner intends to exercise legally acquired rights;

d. Identifying the natural persons holding equivalent or similar positions in other Legal Arrangements;

e. Identifying the Beneficial Owner of a Legal Person where such Legal Person is a party to the Legal Arrangement, in accordance with the provisions of this Article.

Article (11)

Where the Customer, or the controlling owner, is a company listed on a securities market that is subject to disclosure requirements ensuring sufficient transparency with respect to the identification of the Beneficial Owner, or a subsidiary thereof holding a controlling interest, it shall be permissible not to identify or verify the identity of any shareholder or Beneficial Owner of such Companies. In such cases, identity information may be obtained from publicly available registers, from the Customer, or from any other reliable sources.

Article (12)

1. In addition to the Due Diligence measures required in respect of the Customer and the Beneficial Owner, Financial Institutions shall apply Due Diligence and ongoing monitoring measures with respect to the beneficiary of life insurance policies and other types of investment-related insurance classes, as soon as the beneficiary is identified or designated, as follows:

    a. Where the beneficiary is designated by name, name of the person shall be obtained, whether the person is a natural person, a Legal Person, or a Legal Arrangement.

    b. Where the beneficiary is designated by category or description, such as by family relationship (including spouse or children) or by other means such as a will or estate, sufficient information about the beneficiary shall be obtained to ensure that the Financial Institution will be able to identify the beneficiary at the time of payment of compensation or entitlements.

    c. In all cases, the identity of the beneficiary shall be verified at the time of payment of compensation or entitlements, or upon the exercise of any rights related to such policies.

2. In all cases, Financial Institutions shall consider the beneficiary of life insurance policies as a risk factor when determining the applicability of Enhanced Customer Due Diligence measures. Where it is determined that such beneficiary is a Legal Person or Legal Arrangement that presents high risk, Financial Institutions shall apply Enhanced Customer Due Diligence measures, which shall include reasonable procedures to identify and verify the Beneficial Owner of the beneficiary of the insurance policy at the time of payment of compensation or entitlements, or upon the exercise of any rights related to such policies.

Article (13)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Customer Due Diligence measures to Customers and existing Business Relationships at the time this

Resolution enters into force, at such times as they deem appropriate based on materiality and risk, and shall ensure the adequacy of data previously obtained where Due Diligence measures were applied prior to the entry into force of this Resolution.

Article (14)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall be prohibited from establishing or continuing a Business Relationship or executing a Transaction where they are unable to apply Customer Due Diligence measures, and shall consider submitting a Suspicious Transaction Report to the Unit whenever necessary.

2. Where Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers suspect the commission of a Crime, they may refrain from applying Customer Due Diligence measures if they have reasonable grounds to believe that such measures may result in alerting the Customer, and shall submit a Suspicious Transaction Report to the Unit, stating the reasons for not applying such measures.

Article (15)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall comply with the following:

1. Refraining from dealing with Shell Banks in any manner whatsoever, including opening bank accounts therefor or accepting funds or deposits therefrom.

2. Refraining from opening or maintaining anonymous accounts or accounts held under obviously fictitious names.

Division Four: Politically Exposed Persons

Article (16)

1. In addition to applying Customer Due Diligence measures, Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall comply with the following:

    a. In respect of foreign Politically Exposed Persons:

        1) Establishing appropriate risk management systems to determine whether the Customer or the Beneficial Owner is a Politically Exposed Person;

        2) Obtaining approval from Senior Management prior to establishing or continuing a Business Relationship with existing Customers who are Politically Exposed Persons.

        3) Taking Reasonable Measures to identify the source of funds and wealth of Customers and Beneficial Owners identified as Politically Exposed Persons.

        4) Conducting enhanced ongoing monitoring of the Business Relationship.

    b. In respect of domestic Politically Exposed Persons and persons entrusted with a prominent function in an international organization:

1) Taking adequate measures to determine whether the Customer or the Beneficial Owner falls within these categories.

2) Applying the measures set out in subparagraphs (2), (3), and (4) of paragraph (a) of this Clause where a high-risk Business Relationship exists with such persons.

2. Subject to Clause (1) of this Article, Financial Institutions concerned with life insurance policies shall take Reasonable Measures to determine whether the beneficiary or the Beneficial Owner thereof is a Politically Exposed Person prior to the payment of compensation or entitlements or the exercise of any related rights. Where higher risks are identified, they shall inform Senior Management prior to the payment of compensation or entitlements or the exercise of any related rights, conduct enhanced scrutiny of the entire Business Relationship, and consider submitting a Suspicious Transaction Report to the Unit whenever necessary.

Division Five: Suspicious Transaction Reports

Article (17)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall establish indicators through which they are able to identify suspicion of a Crime for the purpose of submitting Suspicious Transaction Reports, and shall update such indicators on an ongoing basis in line with the development and diversification of methods used in the commission of a Crime, in compliance with instructions issued by the Supervisory Authority in this regard.

Article (18)

1. Where Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers suspect, or have reasonable grounds to suspect, that a Transaction or attempted Transaction, or funds, in whole or in part, constitute proceeds, are related to the Crime, or are intended to be used therein, regardless of their value, they shall, without invoking banking secrecy, professional secrecy, or contractual liability, comply with the following:

    a. Immediately and without delay notify the Unit by submitting Suspicious Transaction Reports, containing all available data and information relating to such Transaction or funds, and related parties, through the Unit's electronic system or any other means approved thereby.

    b. Promptly respond to any request from the Unit for additional information.

2. Lawyers, notaries, other independent legal professionals, and independent statutory auditors shall be exempt from the provisions of Clause (1) of this Article where the information relating to such transactions was obtained in the course of assessing a Customer's legal position, defending, or representing the Customer before courts, or in arbitration or mediation proceedings, or providing a legal opinion relating to judicial proceedings, including providing advice on initiating or avoiding such proceedings, whether the information was obtained before, during, or after such proceedings, or in other circumstances subject to professional secrecy.

Article (19)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers, as well as their directors, officers, and employees shall be prohibited from disclosing, whether directly or indirectly, to the Customer or any other person that they have submitted or are about to submit a Suspicious Transaction Report, or any information or data related thereto, or that an investigation is being conducted in respect thereof, without prejudice to information sharing with branches and subsidiaries at the level of the Financial Group, in accordance with the provisions of Article (32) of this Resolution.

2. Attempts by lawyers, notaries, other independent legal professionals, or independent statutory auditors to dissuade a Customer from committing an unlawful act shall not constitute disclosure.

Division Six: Reliance on a Third Party

Article (20)

1. Taking into account the countries identified by the National Committee as high-risk and countries with deficiencies in their anti-money laundering, combating terrorist financing, and proliferation financing systems, and to the maximum extent possible the available information on country risks, Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers may rely on a third party to apply Customer Due Diligence measures for the purposes of identifying the Customer and Beneficial Owner and understanding the nature of the Customer's business or for the purposes of a Business Relationship, provided that they remain responsible for the accuracy of such measures and comply with the following:

    a. Ensuring that the third party is regulated and supervised and complies with Customer Due Diligence and record-keeping requirements pursuant to this Resolution.

    b. Immediately obtaining from the third party the necessary identification data and information collected during Customer Due Diligence measures, and taking the necessary steps to ensure the ability to obtain copies of the necessary documents without delay upon request.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers that rely on a third party that forms part of the same Financial Group, shall ensure the following:

    a. That the Group applies Due Diligence requirements in respect of customers and Politically Exposed Persons, maintains records, and implements anti-crime programs in accordance with Divisions Three, Four, and Eleven of Part One of this Chapter and Article (32) of this Resolution, and that the group is subject, in this regard, to supervision by the competent authority.

    b. That any high risks related to countries are adequately mitigated through the Group's anti-crime policies and controls.

3. Reliance on a third party shall not include the use by Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers of external sources, such as outsourcing or agency services to perform Customer Due Diligence measures on their behalf, where such services are carried out in accordance with their internal policies and procedures, and the external sources are subject to their supervision and control in the effective implementation of those policies and procedures, and apply fitness and propriety standards and effective audit procedures to their staff.

Division Seven: Internal Supervision and Foreign Branches and Subsidiaries

Article (21)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall have internal anti-crime policies, controls, and procedures approved by Senior Management, proportionate to the identified Crime risks and to the nature and size of their activities, and the mitigation thereof. Such policies, controls, and procedures shall be reviewed and updated thereby on an ongoing basis, and shall include the following:

1. Customer Due Diligence measures as required pursuant to this Resolution, including risk management procedures for Business Relationships prior to the completion of the verification process.

2. Procedures for reporting Suspicious Transactions.

3. Appropriate anti-crime compliance management arrangements, including the appointment of a Compliance Officer at management level.

4. Screening procedures to ensure the application of high standards of fitness and propriety in the appointment of employees;

5. Preparation of anti-crime periodic programs and workshops to build the capacities and qualify those assuming the compliance function and other relevant employees.

6. An independent audit function to test the effectiveness and adequacy of internal anti crime policies, controls, and procedures.

Division Eight: Duties of the Compliance Officer

Article (22)

Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall appoint a Compliance Officer at management level and under their responsibility, who shall have independence in decision-making and possess appropriate competence and experience, and who shall undertake the following duties:

1. Monitoring Transactions related to the Crime.

2. Reviewing records and receiving, examining, and assessing Suspicious Transaction data, and deciding whether to notify the Unit or to retain the matter stating the reasons therefor, in full confidentiality.

3. Reviewing Anti-Money Laundering, and combating Financing of Terrorism, and Proliferation Financing internal systems and procedures, assessing their consistency with the provisions of the Decree by Law and this Resolution, evaluating the establishment's level of compliance with their implementation, proposing what is necessary to update and develop them; and preparing periodic reports thereon to be submitted directly to Senior Management, and sending a copy thereof to the concerned Supervisory Authority upon its request,

including Senior Management observations and decisions.

4. Developing, implementing, and documenting ongoing programs and training plans for employees of the establishment regarding all matters related to the Crime and methods of combating it.

5. Cooperating with the Supervisory Authority and the Unit, providing them with any data they may request, and enabling their assigned personnel to access the records and documents necessary for the exercise of their competencies.

Division Nine: High-Risk Countries

Article (23)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply Enhanced Customer Due Diligence measures proportionate to the level of risk arising from a Business Relationship or Transactions with a natural or legal person from countries identified by the National Committee as high-risk, or from countries with deficiencies in Anti-Money Laundering, and combating Financing of Terrorism, and Proliferation Financing systems.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall apply countermeasures and any other measures required by the Supervisory Authority, whether on its own initiative or as determined by the National Committee, in relation to high-risk countries and countries with deficiencies in Anti Money Laundering, combating the Financing of Terrorism, Proliferation Financing systems.

Division Ten: Requirements Relating to New Technologies

Article (24)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall identify and assess the risks of Money Laundering, Financing of Terrorism, and Proliferation Financing that may arise from the development of new products and new business practices, including new service delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall assess such risks prior to the launch or use of products, practices, or technologies, and shall take appropriate measures to manage and mitigate those risks.

Division Eleven: Record-Keeping

Article (25)

1. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall retain all records, documents, instruments, and data relating to all domestic and international financial and cash Transactions and commercial dealings, for a period of not less than five (5) years from the date of completion of the Transaction or the termination of the Business Relationship with the Customer. Such

records shall be made available to the concerned authorities promptly upon request.

2. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall retain all records and documents obtained through Customer Due Diligence measures, ongoing monitoring, account files, business correspondence, copies of personal identification documents, including Suspicious Transaction Reports, results of any analysis conducted, closed-circuit television (CCTV) and the related automated teller machines (ATMs) recordings, and any other recordings, for a period of not less than five (5) years from the date of termination of the Business Relationship, or from the date of account closure for Customers holding accounts therewith, or after the completion of an occasional Transaction, or from the date of completion of inspection by the Supervisory Authority, or from the date of completion of an investigation, or from the date of issuance of a final court judgment, with the retention period calculated by reference to the most recent of such procedures.

3. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall organize retained records, documents, and instruments in a manner sufficient to permit the reconstruction of individual Transactions, data analysis, and the tracing of financial transactions, so as to be capable, where necessary, of providing evidence for prosecution of criminal activity.

4. Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers shall make all Customer information, including information relating to Customer Due Diligence, ongoing monitoring, and the results thereof, as well as records, files, documents, correspondence, and related forms, available to the concerned authorities promptly upon request.

Part Two: Obligations Specific to Financial Institutions

Division One: Correspondent Banking Relationship

Article (26)

1. Prior to entering into a Correspondent Banking Relationship or any other similar relationship, Financial Institutions shall take the following measures:

    a. Refraining from entering into or continuing a Correspondent Banking Relationship with Shell Banks, or with any institution that permits its accounts to be used by Shell Banks.

    b. Collecting sufficient information on any respondent Correspondent Institution for the purpose of identifying it and reaching a full understanding of the nature of its business, and, through publicly available information, determining its reputation and the level of supervision to which it is subject, including whether it has been subject to an investigation relating to the Crime or to a supervisory action.

    c. Assessing the anti-crime controls applied by the respondent institution.

    d. Obtaining approval from Senior Management prior to establishing a new Correspondent Banking Relationship.

    e. Understanding the anti-crime responsibilities of each institution.

2. With respect to Payable-Through Accounts, the Financial Institution shall ensure that the respondent institution has applied Due Diligence measures in respect of Customers who have direct access to such accounts, and that it is able to provide relevant Customer Due Diligence information upon request by the correspondent

institution.

Division Two: Money or Value Transfer Services (MVTS)

Article (27)

1. Money or Value Transfer Service Providers shall be licensed by or registered with, the concerned Supervisory Authority. The Supervisory Authority shall take the necessary measures to penalize any person providing such services without the license or registration, in accordance with its applicable legislation, and shall ensure that licensed or registered providers comply with anti-crime controls.

2. Money or Value Transfer Service Providers shall maintain an updated list of their agents and make it available to the concerned authorities within the State in which the Money or Value Transfer Service Providers and their agents operate. They shall also include such agents in the anti-crime programs, and monitor their compliance with such programs.

Division Three: Wire Transfers

Article (28)

1. Financial Institutions shall verify the accuracy of originator information in all international Wire Transfers equal to or exceeding the amount of three thousand five hundred dirhams (AED 3,500), and shall ensure that such transfers are always accompanied by the following data:

    a. The full name of the originator and the beneficiary.

    b. The account number of the originator and the beneficiary, or, where no account number exists, the transfer shall include a unique transaction reference number that enables the Financial Institutions to trace it.

    c. The address of the originator, or the originator's identity number or travel document number, or the date and place of birth, or the customer identification number held by the originating Financial Institution, which shall refer to a record containing such data.

2. Where multiple international Wire Transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the transfer file shall include accurate originator data and complete beneficiary information, which is fully traceable in the beneficiary country, and the Financial Institution shall be required to include the originator's account number or a unique transaction reference number.

3. Financial Institutions shall ensure that all international Wire Transfers below the amount of three thousand five hundred dirhams (AED 3,500) are accompanied by the data referred to in Clause (1) of this Article, without the need to verify the accuracy of such data, unless there are suspicions of the commission of the Crime.

4. Financial Institutions originating domestic Wire Transfers shall ensure that the information accompanying such transfers includes the same originator data specified in Clause (1) of this Article, unless such data is otherwise available to the Beneficiary Financial Institutions and the concerned authorities through other means.

5. Where the information accompanying a domestic Wire Transfer is available to the Beneficiary Financial Institutions and the concerned authorities through other means, the originating Financial Institution shall be

required to include only the account number or the unique transaction reference number, provided that such number permits tracing of the transaction to the originator or the beneficiary. The originating Financial Institution shall provide such data within three (3) Working Days from the date of receipt of a request from the Beneficiary Financial Institution or the concerned authorities.

6. Financial Institutions shall be prohibited from executing Wire Transfers where they fail to comply with the conditions set out in this Article.

7. Originating Financial Institutions shall retain all information collected regarding the originator and the beneficiary in accordance with the provisions of Article (25) of this Resolution.

8. Financial Institutions shall, when processing Wire Transfers, apply freezing measures and transaction prohibition measures in accordance with instructions issued by the Executive Office or other competent authorities relating to Targeted Financial Sanctions.

Article (29)

1. Intermediary Financial Institutions shall ensure that all originator and beneficiary information accompanies international Wire Transfers.

2. Where technical limitations prevent the originator and beneficiary information from remaining with an international Wire Transfer when such transfer is converted into a domestic Wire Transfer, the Intermediary Financial Institution receiving the international transfer shall retain a record containing all information received from the originating Financial Institution or from a foreign intermediary institution, in accordance with the provisions of Article (25) of this Resolution.

3. Intermediary Financial Institutions shall take reasonable and immediate measures to identify international Wire Transfers lacking required originator or beneficiary information, and shall establish risk-based policies and procedures to determine whether to execute, suspend, or reject such transfers, as well as the appropriate follow-up actions in respect thereof.

Article (30)

1. Beneficiary Financial Institutions shall take Reasonable Measures to identify international Wire Transfers lacking required originator or beneficiary information, such as monitoring them during execution, where feasible, or after execution.

2. Beneficiary Financial Institutions shall verify the identity of the beneficiary of international Wire Transfers equal to or exceeding three thousand five hundred dirhams (AED 3,500), where such identity has not been previously verified.

3. Beneficiary Financial Institutions shall establish risk-based policies and procedures to determine when to execute, reject, or suspend Wire Transfers lacking the required originator or beneficiary information, and to determine the appropriate follow-up actions.

4. Beneficiary Financial Institutions shall retain all information collected in respect of the originator and the beneficiary in accordance with the provisions of Article (25) of this Resolution.

Article (31)

1. Money or Value Transfer Service Providers shall comply with all relevant requirements set out in Articles (28), (29), and (30) of this Resolution, whether they conduct their activities directly or through their agents.

2. Where a Money or Value Transfer Service Provider acts as both the originator from the State and the recipient in another State, it shall:

    a. Collect all information relating to the originator and the beneficiary for the purpose of determining whether to submit a Suspicious Transaction Report;

    b. Where it is decided to submit a Suspicious Transaction Report in relation to the Transaction, it shall be submitted to the Financial Intelligence Unit of the concerned State, together with all relevant information.

Division Four: Financial Groups

Article (32)

Financial Groups shall implement group-wide programs for combating Crime, which shall be applicable to all branches and subsidiaries in which the group holds a majority ownership. Such programs shall, in addition to what is stipulated in Article (21) of this Resolution, include the following:

1. Policies and procedures for the exchange of information required for Customer Due Diligence and crime risk management purposes;

2. Provision of information relating to customers, accounts, and transactions from branches and subsidiaries to compliance, audit, and Anti-Money Laundering, combating Terrorism Financing officers at the financial group level where necessary for the purposes of combating Crime, including information resulting from the analysis of Transaction, or activities that appear unusual or suspicious, Suspicious Transaction Reports, or information indicating that such a report has been submitted. In all cases, such information shall be made available to branches and subsidiaries where appropriate and where consistent and proportionate with risk management;

3. The provision of adequate safeguards relating to confidentiality, non-tipping-off or notification, and the use of exchanged information.

Article (33)

1. Financial Institutions shall ensure that their foreign branches and subsidiaries, in which they hold a majority interest, apply combating Crime measures in a manner consistent with the requirements of the Decree by Law and this Resolution, where the minimum requirements for combating Crime in the other country are less stringent than those applied in the State, to the extent permitted by the laws and regulations of the other State.

2. Where the other State does not permit the appropriate implementation of combating Crime measures consistent with the requirements of the Decree by Law and this Resolution, Financial Institutions shall take additional measures to manage and mitigate the risks of Money Laundering, Financing of Terrorism, and Proliferation Financing associated with their foreign operations, shall notify the Supervisory Authority in the State thereof, and shall comply with the instructions issued thereby in this regard.

Part Three: Obligations Specific to Non-Profit Organizations

Article (34)

1. Non-Profit Organizations shall, in coordination with the concerned Supervisory Authority, undertake the following:

    a. Apply focused, proportionate, and risk-based measures approved by the concerned Supervisory Authority;

    b. Apply best practices approved by the concerned Supervisory Authority to address vulnerabilities, in a manner that enables them to protect themselves against misuse for the Financing of Terrorism;

    c. Establish clear policies to enhance accountability, transparency, integrity, and public confidence in their activities and management;

    d. Conduct Transactions through regulated financial channels whenever possible, taking into account differences in financial sector capacities in various countries and the risks associated with the use of cash, in accordance with applicable legislation in the State.

2. The obligations set out in Clause (1) of this Article shall apply to persons acting on behalf of, or for the benefit of, Non-Profit Organizations.

Part Four: Obligations Specific to the Supervisory Authority of Virtual Asset Service Providers

Article (35)

1. The Supervisory Authority responsible for Virtual Asset Service Providers may issue decisions, circulars, and procedures necessary for the adequate regulation thereof, and for determining the scope, limits, and form of Virtual Asset Transfers, verification obligations taking into account the level of risks, record-keeping requirements, and necessary technical standards, in a manner that ensures compliance with the provisions of the Decree by Law and this Resolution.

2. The Supervisory Authority of Virtual Asset Service Providers shall, on its own initiative or in coordination with the concerned authorities, take the necessary measures to identify any person conducting Virtual Asset Service Provider activities without a license, registration, or listing, and to apply appropriate sanctions against them. Such measures may include:

    a. Reviewing public databases and open sources to identify relevant online advertisements or potential business solicitations made by any person who is not licensed, listed, or registered;

    b. Establishing feedback channels with the concerned authorities or communication channels to receive public feedback in this regard;

    c. Coordinating with the Unit to obtain relevant information available thereto;

    d. Reviewing non-public information, such as information relating to the refusal, suspension, restriction, or revocation of licenses, listing, or registrations, and any other relevant information held by law enforcement authorities.

Part Five: Obligations Specific to Virtual Asset Service Providers and the Scope of Their Application to Financial Institutions

Article (36)

1. Any natural or legal person conducting any Virtual Asset Service Provider activity, offering related products or services, or performing its transactions from within the State shall be licensed, registered, or listed, as applicable, by the competent Supervisory Authority.

2. Virtual Asset Service Providers shall comply with the provisions of Articles (26) to (33) of this Resolution in a manner proportionate to the nature of their activities and in accordance with Supervisory Authority instructions, subject to the following:

    a. The originating Virtual Asset Service Provider shall obtain and retain accurate originator and beneficiary information of the transfer and shall transmit such information immediately and securely to the beneficiary Virtual Asset Service Provider or Beneficiary Financial Institution, if any, and shall make such information available to concerned authorities upon request, including such information as determined by the Supervisory Authority and, at a minimum, the following:

        1) With respect to the originator: name, account number, or Virtual Asset wallet address, and residential or business address;

        2) With respect to the beneficiary: name and account number or Virtual Asset wallet address.

    b. The beneficiary Virtual Asset Service Provider shall obtain and retain accurate information on the originator and the beneficiary of the transfer and make it available to concerned authorities upon request.

3. Virtual Asset Service Providers shall comply with all obligations applicable to Financial Institutions set out in the legislation in force in the State relating to Targeted Financial Sanctions.

4. All requirements set out in Clauses (1) and (2) of this Article shall apply to Financial Institutions where they send or receive Virtual Asset Transfers on behalf of a Customer.

Chapter Three: Transparency and Beneficial Ownership

Part One: Obligations of the Registrar, Companies, Nominee Directors, and Nominee Shareholders

Article (37)

1. The Registrar shall be responsible for registering all Companies and for providing information relating thereto and making such information publicly available, as follows:

    a. A description of their various types or forms and their basic characteristics;

    b. Procedures for their establishment;

c. Procedures for registration and for obtaining their Basic Information as referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution;

d. Procedures for registration and for obtaining Beneficial Owner information.

2. The Registrar shall obtain and retain the Up-To-Date Basic Information referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution, together with the Up- to-Date Information of the Nominee Director or Nominee Shareholder referred to in Article (39) of this Resolution, verify the accuracy thereof, make it publicly available, and establish the necessary mechanisms for that purpose.

3. Upon registering Companies, the Registrar shall obtain the company's Beneficial Owner information in accordance with Clause (1) of Article (10) of this Resolution and shall, upon obtaining such information and in all cases, ensure that such information is adequate, accurate, and Up-To-Date, make it available to the concerned authorities, and establish the necessary mechanisms for that purpose.

4. To ensure access to accurate and Up-To-Date Information identifying the Beneficial Owner, the Registrar shall take supplementary measures, such as coordination with competent authorities that retain such information or have access thereto. The Registrar may notify the Supervisory Authority to impose the prescribed administrative sanctions on Companies, or take any other measures it deems appropriate, where it is unable to obtain Beneficial Owner information or where it has doubts as to its accuracy.

5. The Registrar shall coordinate with the Supervisory Authority and the National Committee to identify and assess Crime risks relating to all Legal Persons in the State, take appropriate measures to manage and mitigate such risks, and determine the measures required to ensure that the concerned authorities obtain adequate, accurate, and Up-To-Date Beneficial Owner Information.

Article (38)

1. Companies shall be required to obtain and retain the following:

a. The Basic Information referred to in Paragraph (b) of Clause (1) of Article (9) of this Resolution, together with the Up-To-Date information of the Nominee Director or Nominee Shareholder referred to in Article (39) of this Resolution, and shall update such information within fifteen (15) Working Days from the occurrence of any amendment or change thereto, verify their accuracy on an ongoing basis, and assist the Registrar in documenting such information where necessary;

b. The data of the partners' or shareholders' register, including the number of shares or ownership interests held by each, and the classes of shares, if any, including the nature of the voting rights attached thereto, provided that such data is retained within the State at the company's office, registered place of business, or another location notified to the Registrar;

c. The shareholders' register shall be exempt from being retained within the State where the company retains Beneficial Owner information within the State at its office, registered place of business, or at any other location notified to the Registrar, provided that the company shall comply with providing such information to the Registrar upon request and without delay;

d. The Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution, and shall update such information within fifteen (15) Working Days from the occurrence of any amendment or change thereto and verify its accuracy on an ongoing basis.

2. Companies shall cooperate with Financial Institutions, Designated Non-Financial Businesses and Professions, and Virtual Asset Service Providers in providing adequate, accurate, and Up-To-Date Beneficial Owner Information.

3. Companies shall cooperate to the maximum extent possible, with the concerned authorities in identifying and making available adequate, accurate, and Up-To-Date Beneficial Owner Information without delay.

4. No company established and registered in the State may issue bearer shares, bearer share warrants, or any similar instruments that cannot be traced. Bearer shares or bearer share warrants issued prior to the entry into force of this Resolution shall be converted into registered shares in accordance with the legislation in force in the State within thirty (30) Working Days from the date of publication of this Resolution. The holder of bearer shares, bearer share warrants, or similar instruments shall notify the company of their capacity and status, and the company shall register the holder's identity prior to the exercise of any rights attached thereto during the conversion period.

Article (39)

Subject to the legislation in force in the State, and for the purposes of preventing and mitigating Crime risks, a Nominee Director or Nominee Shareholder shall notify the company of their capacity, disclose thereto the information relating to their status and the identity of the person they represent or the Nominator, and notify the company of any change thereto within a period not exceeding fifteen (15) Working Days from the date of such change.

Article (40)

The Registrar, Companies, persons responsible for their management or liquidation, and any other persons concerned with the dissolution of a company, shall retain the records and all information referred to in Articles (37), (38), and (39) of this Resolution for a period of not less than five (5) years from the date of the company's dissolution or cessation of its existence, or from the date on which the company ceases to be a customer of a Financial Institution or professional intermediary.

Part Two: Obligations Relating to Legal Arrangements

Article (41)

1. The competent authorities responsible for regulating Legal Arrangements shall have mechanisms available to:

    a. Identify the various types, forms, and essential characteristics of Legal Arrangements;

    b. Determine and describe procedures for establishing Legal Arrangements and for obtaining basic information and Beneficial Owner information in accordance with Paragraph (b) of Clause (1) of Article (9) and Clause (2) of Article (10) of this Resolution;

    c. Make the information referred to in Paragraphs (a) and (b) of this Clause accessible to all, without delay and in an effective manner;

    d. Access the Beneficial Owner information relating to Legal Arrangements, Trustees, and their Funds;

e. Ensure that information relating to Legal Arrangements, including that referred to in Clause (2) of this Article, is Adequate, Accurate, and Up-to-Date.

2. Subject to the risk-based approach, Trustees of Trusts and persons holding a similar or equivalent position in any other Legal Arrangement established or managed in the State, shall:

   a. Obtain and retain Adequate, Accurate, and Up-to-Date Information on the Beneficial Owner in accordance with Clause (2) of Article (10) of this Resolution;

   b. Where the parties to the Legal Arrangement are legal persons or other Legal Arrangements, obtain adequate, accurate, and up-to-date basic information and Beneficial Owner information in accordance with Paragraph (b) of Clause (1) of Article (9) and Article (10) of this Resolution;

   c. Retain basic information relating to supervised intermediaries and service providers, including investment advisers, managers, accountants, and tax advisers.

3. Trustees in Legal Arrangements and persons holding a similar or equivalent position shall maintain the information referred to in Clause (2) of this Article accurately, update it within fifteen (15) Working Days of any amendment or change, and retain such information for a period of not less than five (5) years from the date their dealings with the Legal Arrangement end.

4. Trustees in Legal Arrangements and persons holding a similar or equivalent position shall:

   a. Disclose their status to Financial Institutions, DNFBPs, and Virtual Asset Service Providers when establishing a Business Relationship or carrying out an Occasional Transaction exceeding the prescribed threshold under this Resolution;

   b. Cooperate to the fullest extent possible with Concerned Authorities by providing necessary information relating to Legal Arrangements upon request and without delay;

   c. Provide Financial Institutions, DNFBPs, and Virtual Asset Service Providers, upon request, with information relating to the Beneficial Owner of the Legal Arrangement and the Funds held or managed under the terms of the Business Relationship.

5. Except for Trustees and persons holding a similar or equivalent position, and based on risk, context, and materiality, the Concerned Authorities may obtain, without delay, adequate, accurate, and up-to-date basic information and Beneficial Owner information relating to Legal Arrangements, their Funds, and Trustees, from any of the following sources:

   a. Competent authorities responsible for regulating Legal Arrangements, or those required under applicable legislation in the State to retain or collect such information, or to establish access mechanisms thereto;

   b. Financial Institutions, DNFBPs, and Virtual Asset Service Providers;

   c. Supervised intermediaries and service providers, including investment advisers and managers, accountants, and tax advisers;

   d. Any other source retaining such information.

6. The Concerned Authorities, in particular Law Enforcement Authorities and the Unit, may request and obtain, without delay, information from Trustees, persons holding a similar or equivalent position, Financial Institutions,

DNFBPs, Virtual Asset Service Providers, and any other entity, concerning:

a. Basic information and Beneficial Owner information of Legal Arrangements;

b. The residence of the Trustee or persons holding a similar or equivalent position;

c. Funds held or managed by Financial Institutions, DNFBPs, or Virtual Asset Service Providers in relation to Trustees or authorized persons holding a similar or equivalent position with whom they have a Business Relationship or for whom they conduct an Occasional Transaction.

7. The provisions of this Resolution shall apply to all Legal Arrangements established in the State and to foreign Legal Arrangements, regardless of their designation, such as Trusts, fiduciary arrangements, trust contracts or arrangements, endowments, or custodial arrangements, where such foreign Legal Arrangements are connected to or conduct business in the State, or where the Trustees or persons holding a similar or equivalent position reside in the State.

Part Three: Prohibition of Invoking Bank or Professional Secrecy, or Contractual Liability

Article (42)

Banking secrecy, professional secrecy, or contractual liability may not be invoked to prevent the application of the provisions of the Decree by Law and this Resolution in the following cases:

1. Exchange of information between Financial Institutions, where such exchange relates to reliance on third parties, correspondent banking relationships, or Wire Transfers regulated under Articles (20), (26), and (28) to (31) of this Resolution;

2. Exchange of information between Concerned Authorities at the national or international level relating to anti-crime matters.

Part Four: Access to Information

Article (43)

1. The Concerned Authorities, in particular the Public Prosecution, Law Enforcement Authorities, and the Unit, shall obtain, as swiftly and effectively as possible, the basic information referred to in Paragraph (b) of Clause (1) of Article (9) and the Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution, as held by competent authorities, Financial Institutions, DNFBPs, and Virtual Asset Service Providers.

2. The Concerned Authorities shall, in the context of public procurement, have timely access to the basic information referred to in Paragraph (b) of Clause (1) of Article (9) and the Beneficial Owner information referred to in Clause (1) of Article (10) of this Resolution.

3. The Concerned Authorities shall establish appropriate mechanisms to exchange, or facilitate timely access to, adequate, accurate, and up-to-date Beneficial Owner Information referred to in Clause (1) of Article (10) of this Resolution, in relation to all types of Companies, including foreign Companies and other entities that pose Crime related risks and whose activities are connected to the State, such as permanent establishments, branches, or agencies, or that maintain substantial commercial activities or ongoing Business Relationships

with Financial Institutions or DNFBPs, or that hold significant real estate or other investments in the State, or are registered for tax purposes therein.

Chapter Four: The Financial Intelligence Unit and the National Committee

Part One: Independence of the Unit

Article (44)

1. The Unit shall operate as the national center for receiving Suspicious Transaction reports and other information relating to the Crime, analyzing such information, and disseminating the results of such analysis to Law Enforcement Authorities.

2. The Unit shall enjoy operational independence, including the authority to decide on the analysis, request, re-dissemination, and referral of information, and shall operate independently with Concerned Authorities and counterpart units in order to perform its functions effectively. No staff member of the Unit may be summoned in relation to their duties without the approval of the Chief of the Unit.

3. The headquarters of the Unit shall be located in the capital of the State, and it may establish sub-branches within or outside the branches of the Central Bank.

4. The Chief of the Unit shall be appointed and removed from office by a decision of the Board of Directors of the Central Bank.

5. For the purpose of performing its duties and competences under the Decree by Law and this Resolution, the Unit shall appoint such qualified and experienced personnel as it deems appropriate and shall determine their duties. The Central Bank shall provide the Unit with the human, financial, and technical resources necessary to enable it to perform its functions effectively.

Part Two: Competences of the Unit

Article (45)

The Unit shall have the following competences:

1. Establishing its organizational structure and internal regulations, which shall include procedures to ensure the efficiency and integrity of its staff, to define their responsibilities in handling sensitive and confidential information, and to prevent access or disclosure of information, except by authorized persons;

2. Establishing a database or special register for the information available thereto, and protecting such information through information security and confidentiality controls, including cybersecurity measures and procedures for processing, storing, and disseminating information, as well as procedures to ensure restricted access to its premises, information, and technological systems;

3. Ensuring that its staff obtain the necessary security clearances and are aware of their responsibilities in handling and disseminating sensitive and confidential information;

4. Providing training courses and programs for the training and qualification of its staff and any other entity, whether within or outside the State;

5. Preparing studies, research, and statistics relating to the Crime, and following up on any national or international studies, research, or statistics prepared in this regard;

6. Preparing annual reports on its anti-crime activities, including, in particular, a general analysis of notifications and Suspicious Transaction reports received by the Unit, Crime activities and trends, and preparing a summary of such reports for publication purposes.

Article (46)

In carrying out its functions in relation to Suspicious Transaction reports, the Unit shall have the following competences:

1. Receive reports from Financial Institutions, DNFBPs, and Virtual Asset Service Providers in accordance with the forms approved by the Unit, examine, analyze, and retain such reports in its database;

2. Request Financial Institutions, DNFBPs, Virtual Asset Service Providers, and Concerned Authorities to provide any additional information or documents relating to the reports and information received by the Unit, as well as any other information it deems necessary for the performance of its functions, including information relating to disclosure systems, customs information, tax information, Population Register information, and the information referred to in Paragraph (b) of Clause (1) of Article (9) and Article (10) of this Resolution, within the timeframes and in the manner determined by the Unit;

3. Analyze reports and available information as follows:

    a. Operational analysis, using available and obtainable information to identify specific targets such as persons, funds, or criminal networks, trace the course of specific activities or Transactions, and identify links between such targets, activities, or Transactions and potential criminal property;

    b. Strategic analysis using available and obtainable information, including data provided by the Concerned Authorities, to identify Crime trends and patterns;

4. Provide Financial Institutions, DNFBPs, and Virtual Asset Service Providers with feedback on reports received by the Unit to enhance the effectiveness of Crime combating measures and the detection and reporting of Suspicious Transactions;

5. Cooperate and coordinate with the Supervisory Authority by referring the results of its analyses relating to the quality of reports received, in order to ensure compliance by Financial Institutions, DNFBPs, and Virtual Asset Service Providers with Crime combating procedures;

6. Use dedicated, secure, and protected channels to disseminate report-related data, analysis results, and other relevant information to Law Enforcement Authorities, where sufficient grounds exist to suspect a link to the Crime, for the purpose of taking the necessary actions in this regard;

7. Use dedicated, secure, and protected channels to provide the Public Prosecution and Law Enforcement Authorities with information relating to Crime, including information obtained from Financial Intelligence Units in other countries, whether spontaneously or upon request.

Article (47)

For the purpose of performing its functions at the international level, the Unit shall have the following competences:

1. Exchanging information, both spontaneously and upon request, with counterpart units, regardless of differences in their nature, and with other foreign competent authorities responsible for the suspension or cessation of Transactions suspected of being related to Crime; cooperating in relation to such Transactions, Suspicious Transaction reports, or any other information that the Unit is authorized to obtain or access, directly or indirectly; and exchanging information with Concerned Authorities in the State to facilitate such cooperation.

2. Concluding Memoranda of Understanding to regulate cooperation and the exchange of information with counterpart units and Concerned Authorities, in accordance with the legislation in force in the State.

3. Notifying counterpart units of the results of the use of the information provided and of the analyses conducted on the basis thereof. Such information, including the information referred to in Clause (1) of this Article, shall be used solely for the purposes of combating Crime, and shall not be disclosed to any third party without the consent of the Unit.

4. Following up on developments relating to Crime through relevant regional and international organizations and bodies, and participating in meetings related thereto.

5. Following the requirements of the Egmont Group and attending and participating in its meetings as a member thereof.

Part Three: Competences of the National Committee

Article (48)

The competences of the National Committee shall be expanded to include the following:

1. Identifying, assessing, and understanding Crime risks at the national level, including risks arising from the development of new products or new business practices, such as the use of new or emerging technologies or services or products delivery methods.

2. Updating the National Risk Assessment and the National Anti-Crime Strategy at least once every three (3) years, or whenever necessary.

3. Disseminating information relating to the National Risk Assessment, in accordance with the mechanism it deems appropriate, to Concerned Authorities, Financial Institutions, DNFBPs, Virtual Asset Service Providers, and Non-Profit Organizations.

4. Coordinating with the Concerned Authorities in the application of the risk-based approach, the allocation of resources, and the implementation of Crime combating or mitigation measures.

5. Coordinating with the Registrar and the Supervisory Authority in identifying and assessing Crime risks relating to all legal persons, including foreign-established Companies and others that pose Crime risks and whose activities or investments are connected to the State, taking appropriate measures to manage and mitigate the identified risks, and determining the measures required to ensure that the Concerned Authorities have access to adequate, accurate, and Up-To-Date Beneficial Owner Information.

6. Identifying and assessing Crime risks relating to Legal Arrangements and taking appropriate measures to manage and mitigate the identified risks, including requiring the submission of Beneficial Owner information to be retained by the competent authorities regulating foreign Legal Arrangements or any other authority responsible for retaining such information, in the following cases:

    a. Legal Arrangements registered or licensed under the legislation of the State, or administered therein;

    b. Legal Arrangements administered in the State or whose Trustees reside therein;

    c. Foreign Legal Arrangements whose activities are connected to the State, including those having substantial and ongoing commercial activities or relationships with Financial Institutions or DNFBPs, significant real estate or other domestic investments, or tax registration in the State.

7. Coordinating with the Concerned authorities to ensure that the application of the provisions of the Decree by Law complies with personal data protection and privacy requirements under the personal data protection and privacy legislation in force in the State.

8. Developing and coordinating capacity-building and training programs for personnel working in the field of Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing.

Chapter Five: Supervisory Authority

Part One: Supervisory Authority over Financial Institutions, DNFBPs, and Virtual Asset Service Providers

Article (49)

The competences of Supervisory Authorities shall be expanded to include the following:

1. Identifying and assessing Money Laundering, Terrorist Financing, and Proliferation Financing risks that may arise from the development of new products and new professional practices, including new service delivery methods and the use of new or emerging technologies for both new and existing products.

2. Applying a risk-based approach to ensure that Money Laundering, Terrorist Financing, and Proliferation Financing prevention or mitigation measures are proportionate to the identified risks.

3. Implementing identified risk-based and proportionate measures and allocating resources efficiently to mitigate Proliferation Financing risks.

4. Issuing instructions, regulations, and forms relating to Crime combating applicable to entities subject to their supervision, where necessary.

5. Establishing policies, procedures, and controls necessary to verify the compliance of supervised entities with the provisions of the Decree by Law, this Resolution, and any other Crime combating legislation in the State, and requesting information relating to the implementation thereof.

6. Establishing systems, rules, and standards of merit and eligibility, and taking all necessary legal or regulatory measures on an ongoing basis at the time of licensing, registration, renewal, or amendment, to prevent criminals or their associates from holding or being the Beneficial Owners of significant or controlling interests in Financial Institutions, DNFBPs, or Virtual Asset Service Providers, or from controlling or participating in their

management or operation, directly or indirectly.

7. Coordinating with the Unit in identifying indicators of suspected Crime through which Financial Institutions, DNFBPs, and Virtual Asset Service Providers submit Suspicious Transaction reports to the Unit.

8. Coordinating with the Unit regarding the quality of reports and information received by the Unit from Financial Institutions, DNFBPs, and Virtual Asset Service Providers, and taking the necessary supervisory measures in this regard.

9. Conducting off-site and on-site supervision and inspections of Financial Institutions, DNFBPs, and Virtual Asset Service Providers on a risk-based basis, and for that purpose, requesting and obtaining any information deemed necessary for the performance of supervisory functions.

10. Determining the frequency of supervisory and inspection activities over Financial Institutions, DNFBPs, and Virtual Asset Service Providers based on:

    a. The National Risk Assessment;

    b. The characteristics of Financial Institutions, Financial Groups, DNFBPs, and Virtual Asset Service Providers, including their diversity, size, and degree of discretion permitted under the risk-based approach;

    c. Crime risks, the level of understanding thereof, and the internal policies, controls, and procedures applied by Financial Institutions, Financial Groups, DNFBPs, and Virtual Asset Service Providers, as determined in the Supervisory Authority's assessment of the risk structure specific to each of them.

11. Taking all measures necessary to ensure the full and immediate compliance of Financial Institutions, DNFBPs, and Virtual Asset Service Providers with instructions issued by the Executive Office or other competent authorities regarding Targeted Financial Sanctions, through on-site visits and continuous follow-up, and imposing effective, proportionate, and dissuasive administrative penalties in cases of violation or failure to comply.

12. Verifying that supervised institutions adopt and implement the prescribed controls, procedures, and measures under the Decree by Law and this Resolution, and apply them to their foreign branches and majority-owned subsidiaries to the extent permitted by the laws of the host country.

13. Ensuring that Financial Groups apply appropriate additional measures to manage Money Laundering and Terrorist Financing risks where the laws of the host country do not permit proper implementation of the prescribed controls, procedures, and measures. Where such additional measures are insufficient, the Supervisory Authority shall take supervisory measures, including imposing further controls on the Financial Group or requiring the closure of its operations in that country.

14. Ensuring that Financial Institutions subject to International Core Principles for Financial Supervision are regulated and supervised in accordance with those principles, including the application of consolidated supervision at the Financial Group level for AML/CFT purposes, and ensuring that other Financial Institutions are subject to regulation, supervision, or monitoring commensurate with their Money Laundering or Terrorist Financing risk.

15. Reviewing the institution's and the Financial Group's Crime risk structure assessment, including compliance risks, periodically or upon material developments in the management or operation thereof.

16. Establishing adequate controls and procedures to ensure that Financial Institutions, DNFBPs, and Virtual Asset Service Providers are notified of and comply with National Committee decisions relating to:

    a. Enhanced Due Diligence measures and countermeasures determined by the National Committee;

    b. Any concerns relating to deficiencies in AML/CFT/CPF systems in other countries;

    c. Any other decisions issued by the National Committee.

17. Providing supervised entities with instructions, guidance, and feedback to assist in implementing national Crime combating measures, particularly in detecting and reporting Suspicious Transactions and applying Simplified Due Diligence measures where low risks are identified, to enhance the effectiveness of Crime combating implementation.

18. Maintaining an updated list of Compliance Officers of supervised entities, notifying the Unit thereof, and requiring such entities to obtain its prior approval before appointing their Compliance Officers.

19. Organizing awareness programs and campaigns relating to Crime combating.

Part Two: Supervisory Authority over Non-Profit Organizations

Article (50)

The Supervisory Authority for Non-Profit Organizations shall have the following competences:

1. Obtaining available information from all competent authorities regarding the activities of Non-Profit Organizations from reliable sources in a timely manner, for the purpose of determining their size, characteristics, and types, assessing risks to identify the nature of Terrorist Financing risks to which they are exposed, identifying the sub-sector thereof most exposed to such risks, and establishing focused, proportionate, and risk-based measures to address them, in a manner consistent with the risk-based approach, and periodically reviewing such measures to ensure their adequacy.

2. Supervising and monitoring Non-Profit Organizations using focused, proportionate, and risk-based measures to prevent their misuse in supporting or financing Terrorism, requiring the implementation of such measures and other obligations, and monitoring compliance therewith.

3. Reviewing the adequacy and sufficiency of legislation relating to Non-Profit Organizations to prevent their misuse in supporting or financing Terrorism, and working to improve such legislation whenever necessary.

4. Periodically assessing Non-Profit Organizations by reviewing Up-to-Date Information on potential vulnerabilities that may render them susceptible to exploitation in supporting or financing Terrorism.

5. Cooperating and coordinating with Non-Profit Organizations to develop best practices for addressing vulnerabilities that enable them to protect themselves from misuse in Terrorism Financing.

6. Encouraging and implementing awareness and education programs to raise awareness among Non-Profit Organizations and donors regarding their potential vulnerabilities, which expose them to the risk of misuse in the field of supporting and financing Terrorism, and of measures that can be taken to protect themselves from such risks.

7. Cooperating, coordinating, and exchanging information at the national level with all Concerned Authorities that retain relevant information relating to Non-Profit Organizations.

8. Establishing adequate controls and procedures to ensure that Non-Profit Organizations are notified of, and implement, the relevant decisions of the National Committee.

9. Possessing detection expertise and the capacity to examine Non-Profit Organizations suspected of being exploited by terrorist activities or organizations, or of supporting them.

10. Obtaining full access, during detection and examination processes, to information relating to the management and organization of any Non-Profit Organization, including financial information and information relating to its programs.

11. Conducting off-site and on-site inspections of Non-Profit Organizations without obstructing or delaying their legitimate charitable activities.

12. Establishing mechanisms to ensure the immediate exchange of information with Concerned Authorities for the purpose of taking preventive or investigative measures where there are suspicion or reasonable grounds to suspect that a Non-Profit Organization:

    a. Is a front for fundraising by a terrorist organization, or is being misused to finance Terrorism.

    b. Is being exploited as a conduit for Terrorism Financing, for evading funds-freezing measures, or for any other form of terrorist support.

    c. Conceals or obscures the trail of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organizations.

13. Identifying appropriate points of contact and the necessary procedures for responding to international requests for information relating to Non-Profit Organizations suspected of engaging in, or being exploited for, Terrorism Financing or the support thereof.

Chapter Six: Provisional Measures and Investigation Procedures

Part One: Provisional Measures

Article (51)

1. The Chief of the Unit may order the suspension or cessation of a Transaction suspected of being related to the Crime, immediately and without prior notice, for a period not exceeding ten (10) working days, based on the Unit's analysis of Suspicious Transaction reports, information, or requests received from domestic or international sources, including counterpart Units regardless of their nature, or any authorities competent to take such measures.

2. The Unit shall establish a system governing the controls and procedures for the suspension or cessation of suspicious Transactions related to the Crime and the circumstances under which such suspension or cessation is lifted upon revocation of the order or expiry of the prescribed period.

3. The Chief of the Unit may order the freezing of funds suspected of being linked to a Crime held by Financial Institutions, DNFBPs, or Virtual Asset Service Providers, without prior notice, for a period of thirty (30) days,

based on the Unit's analysis of Suspicious Transaction reports and other information received thereby.

4. Where the decision referred to in Clause (3) of this Article is taken, the Unit shall:

   a. Notify the relevant Financial Institutions, DNFBPs, or Virtual Asset Service Providers to implement the freezing order, without prior notice;

   b. Notify the Attorney General or their delegate of the freezing decision and the grounds for suspicion, who may amend or revoke the decision or issue any directions deemed appropriate.

5. A freezing order may be extended by the Attorney General or their delegate for such period they determine upon the Unit's request, stating the justifications therefor.

6. The Chief of the Unit shall submit a proposal to the Attorney General to cancel the extension of the freezing order where the grounds therefore cease to exist, for such action as they deem appropriate.

7. Financial Institutions, DNFBPs, and Virtual Asset Service Providers holding frozen funds shall notify the owner of the frozen funds of the freezing order and its issuing authority, request them to provide the documents necessary to prove the integrity of the Transaction and the legitimacy of the source of funds, and refer the same to the Unit to take the appropriate actions.

8. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall lift the freezing order where it is revoked by the Chief of the Unit, or where the period specified in Clause (3) of this Article expires without extension.

Article (52)

1. The Public Prosecution and the competent court, as the case may be, may order, without prior notice, the identification, tracing, valuation, seizure, or freezing of Criminal Funds or Property, or Funds of equivalent value, the prohibition of their management, and the imposition of travel bans until the conclusion of the investigation or trial.

2. Where necessary, the Public Prosecution and the competent court, as the case may be, may order travel bans and take decisions preventing dealings in or disposition of Criminal Funds or property or funds of equivalent value, and take the necessary measures to prevent any disposition intended to evade seizure, freezing, or confiscation orders, without prejudice to the rights of bona fide third parties.

3. Without prejudice to the rights of bona fide third parties, any contract or disposition entered into with the accused shall be null and void by operation of law where the parties thereto, or any of them, knew, or ought to have known, that its purpose was to affect the ability of competent authorities to seize, freeze, recover, or confiscate, or to enforce such measures.

4. For the purposes of Clause (3) of this Article, knowledge of the contracting parties with the accused shall be inferred from the factual and objective circumstances surrounding the conclusion of the contract or disposition.

Article (53)

1. The Public Prosecution and the competent court, as the case may be, may:

a. Assign the accused, the owner, holder, or manager of Funds, or any other person deemed appropriate, to estimate and manage Criminal Funds or Property, or funds of equivalent value, that have been seized, frozen, subject to confiscation, or subject to Asset Recovery pursuant to an international judicial cooperation request, determine the scope of management and disposal powers in accordance with the legislation in force in the State, provided that the person assigned to manage and dispose shall demonstrate competence, integrity, and absence of conflicts of interest, and submit periodic reports on the managed Funds, including their status, expenses, and returns, if any, and if necessary, the mechanism for their disposition. The assignee may be removed where mismanagement or breach of the limits of their powers is established;

b. Authorize the disposal or sale of Criminal Funds or Property, or any funds of equivalent value, even prior to the issuance of a judgment, where necessary, such as where there is a risk of deterioration or loss of economic value over time, or where management or safeguarding costs exceed their value upon sale, or where they are subject to total or partial deterioration. The proceeds from such sale shall accrue to the public treasury upon issuance of a final confiscation judgment.

2. Criminal Funds or Property, or funds of equivalent value, shall remain encumbered, within the limits of their value, by any compensation, rights, or obligations lawfully determined in favor of the victim or any bona fide third parties.

3. Subject to the legislation in force in the State, the General Attorney shall form a committee to assess management fees and expenses of Funds, determine its rules of procedures, composition, and conditions for exercising its competences in determining such fees and expenses, when the management is assigned to a third party. The Committee shall also determine the method of payment, either as a lump sum or a percentage not exceeding (10%) ten percent of the value of the managed Funds. For the purposes of exercising its competences, the Committee may seek assistance from experts as it deems appropriate from governmental or non-governmental entities, taking into account the type, value, and complexity of the Funds under management, any return generated, and the efforts exerted in management. The fees and expenses shall be deducted from the managed Funds pursuant to a decision approved by the Attorney General.

Article (54)

1. Orders to freeze Funds held by Financial Institutions, DNFBPs, or Virtual Asset Service Providers shall be executed solely by the competent Supervisory Authority or the Unit, as the case may be.

2. Financial Institutions and Virtual Asset Service Providers shall transfer frozen Funds to interest-bearing or profit-generating deposit accounts at prevailing market rates where such freezing is pursuant to decisions issued by competent authorities.

3. Interest and profits accruing from frozen Funds shall be deemed an integral part of the Criminal Property where a confiscation judgment is issued.

4. Frozen Funds, together with accrued interest and profits, shall be returned where the freezing order is lifted by competent authorities.

5. Financial Institutions, DNFBPs, and Virtual Asset Service Providers shall not dispose of seized or frozen Funds under any circumstances, including for the settlement of prior obligations, unless coordination is effected with the competent Supervisory Authority to obtain authorization from the Public Prosecution or the competent court, as the case may be.

6. Without prejudice to the legislation in force in the State, seizure or freezing orders issued by the competent authorities shall not prevent the enforcement of administrative fines imposed by the Supervisory Authority prior to the issuance of the order. This shall be carried out by requesting the release of an amount equivalent to the value of the imposed administrative fines from the scope of the order, at the discretion of the competent authorities.

Part Two: Investigation Procedures

Article (55)

1. The Public Prosecution, on its own initiative or at the request of Law Enforcement Authorities, where sufficient indications of a Crime exist, may order the search of persons and premises, prohibit suspects from travel, obtain evidence, identify, trace, and seize Funds, monitor accounts, intercept communications, directly access accounts, registers, instruments, and documents held by third parties, access computer systems and information technology means, examine correspondence, communications, and parcels, conduct controlled deliveries, and take any other measures that assist in the detection of the Crime and its perpetrators, without prejudice to the legislation in force in the State.

2. The Public Prosecution may seek the opinion of the Unit on the financial aspects of the Crime and their analysis, and request all information available thereto.

3. Law Enforcement Authorities shall receive and follow up on the Unit's reports, collect intelligence and information relating thereto, and provide feedback to the Unit regarding actions taken in connection therewith.

4. The Public Prosecution and Law Enforcement Authorities may access, in a timely manner, without delay and without prior notice, any information deemed necessary for the prompt identification and tracing of Criminal Funds or Property, or Funds of equivalent value, or any other information as they deem necessary, even if such information is subject to banking or professional secrecy, where required for the performance of their duties for the detection of the Crime or its perpetrators. Where necessary, they shall conduct parallel financial investigations, by undertaking the following:

    a. Taking into account the extent of linkage of the financial aspects of the Crime, in order to determine its temporal and geographic scope, the value of Criminal Property and the manner of its acquisition, to identify, trace, and seize such property or Funds of equivalent value, that may be subject to confiscation, identify the person to whom the Criminal Property has been transferred and their relationship with the accused, their disposal thereof, and their knowledge of its source; to strengthen the evidence proving the commission of the Crime and attributing it to its perpetrator; to demonstrate their financial capacity before and after the criminal activity and the extent of its proportionality to their legitimate sources of income, and take all precautionary measures in preparation for legal confiscation;

    b. Coordinating with Concerned Authorities, each within its competence, to obtain timely access to any information and documents relating to the Crime, including disclosure systems, customs, tax, Population Register, property registers, and bank account records and those managing them, and other information deemed necessary for the performance of their duties;

    c. In all cases, Law Enforcement Authorities shall, immediately upon becoming aware of the Crime, promptly identify, trace, and seize the Criminal Funds or Property, or Funds of equivalent value, potentially subject to confiscation.

5. Law Enforcement Authorities may collect witness statements, conduct undercover operations and other intelligence-gathering activities, use various detection methods, and carry out controlled deliveries where such

measures would lead to the detection of the Crime and its evidence, identification of the source and destination of Criminal Property, or arrest of perpetrators, without prejudice to the legislation in force in the State.

Chapter Seven: National Cooperation and Coordination

Article (56)

1. Concerned Authorities shall cooperate and exchange expertise and information among themselves, including tax information, to enhance efforts for Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing, particularly with respect to asset recovery and identification of Criminal Property.

2. Concerned authorities may enhance and develop partnerships with the private sector to exchange expertise and facilitate access to information in the field of Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing.

Chapter Eight: International Cooperation and Asset Recovery

Part One: General Provisions on International Cooperation

Article (57)

In applying the provisions of this Chapter, due regard shall be given to the legislation in force in the State and the provisions of treaties or agreements to which the State is a party, or the principle of reciprocity.

Article (58)

For the purpose of requesting and executing international cooperation requests relating to the Crime, the Concerned Authorities shall:

1. Provide the widest possible range of international cooperation promptly, constructively, and effectively, and exchange information spontaneously and upon request.

2. Establish clear procedures for prioritizing and executing incoming international cooperation requests in a timely manner.

3. Cooperate, coordinate, and exchange information among themselves to enhance the effectiveness of Asset Recovery at the international level.

4. Conclude, negotiate, and sign agreements and other mechanisms with competent foreign authorities in a timely manner.

5. Participate in multilateral networks to facilitate prompt and constructive international cooperation in the field of Asset Recovery.

6. Consider applying for membership in inter-agency or inter-authority networks supporting international cooperation in the field of Asset Recovery.

7. Take the necessary measures to enable informal cooperation with other countries for Asset Recovery purposes, including facilitating assistance prior to the submission of formal requests, updating requesting countries on the status of their requests, and providing assistance based on initial requests without the need for supplementary requests, where appropriate.

8. Request additional information from competent foreign authorities where necessary to execute or facilitate the execution of international cooperation requests.

9. Request information on behalf of foreign counterpart authorities, obtain any other required information on their behalf, and exchange all obtainable information as if the request had been made at the national level.

Article (59)

The Concerned Authorities shall give priority to all international cooperation requests, particularly those relating to the Crime, and shall execute them urgently and without undue delay through clear and secure procedures, mechanisms, and channels to enhance information protection, and shall in all cases:

1. Use information obtained through international cooperation solely for the purpose for which it was requested, unless consent is granted by the competent foreign authorities for another purpose.

2. Provide feedback to the competent foreign authorities on the use and benefit of the information obtained, where requested.

3. Maintain the confidentiality of international cooperation requests and the exchange of information with competent foreign authorities in a manner consistent with each party's obligations regarding privacy and data protection, and in accordance with the legislation in force in the State, in order to protect the integrity of the investigation and the request for information relating thereto. Where confidentiality of received information cannot be maintained, the requesting authority shall be notified accordingly.

4. Ensure, where exchanging information with competent foreign authorities, their ability to guarantee the confidentiality of the exchanged information; and Concerned Authorities shall protect the information obtained pursuant to clear procedures and in the same manner in which they protect similar information from domestic sources. The Concerned Authorities may refuse to provide or exchange any information where the competent foreign authorities are unable to protect such information effectively.

Article (60)

1. International cooperation requests shall not be refused or subjected to unreasonable or unjustified conditions that restrict their execution. In all cases, such requests shall not be refused on the grounds of any of the following:

    a. That the request involves financial, customs, or tax matters, whether direct or indirect;

    b. Confidentiality requirements applicable to Financial Institutions, DNFBPs, or Virtual Asset Service Providers, except where the information was obtained under circumstances covered by legal professional privilege or professional secrecy;

    c. That the request is related to a Crime under ongoing detection or judicial prosecution in the State, if the request would impede such proceedings, response may be deferred until completion thereof;

d. Differences in the nature or status of the requesting competent foreign authority as compared with the nature or status of the Concerned Authorities in the State.

2. Where execution of an international cooperation request is refused or deferred, Concerned Authorities shall notify the requesting authority of the reasons therefor.

3. Dual criminality shall not be a condition for executing international cooperation requests that do not involve coercive compulsory measures.

4. Where an international cooperation request involves coercive compulsory measures, dual criminality shall be required and deemed satisfied where the act constituting the Crime is punishable under the legislation in force in both the State and the requesting country, regardless of the type, description, or category of the Crime. Where dual criminality is not satisfied, the requested coercive measures may nonetheless be executed with the consent of the person concerned.

Part Two: Exchange of Information Between the Concerned Authorities and Foreign Counterpart and Non-Counterpart Authorities

Article (61)

The Concerned Authorities shall exchange Crime-related information with competent foreign authorities, and in doing so, they may:

1. Exchange information indirectly with non-counterpart foreign authorities, provided that the competent authority requesting the information indirectly shall always clarify, to the authority from which the information is requested, the purpose of the request and the authority on whose behalf the request is made.

2. Obtain an acknowledgment or undertaking from the foreign authorities that the information exchanged through international cooperation shall be used solely for the purpose for which it was requested, unless such authorities obtain prior consent for its use for another purpose.

Article (62)

1. The Concerned Authorities shall exchange information relating to Companies and Legal Arrangements with competent foreign authorities without imposing unjustified restrictive conditions. This cooperation shall include the following:

    a. Facilitating access by competent foreign authorities to Basic Information and Beneficial Owner information of Companies and Legal Arrangements and other information held by or available in relevant registers;

    b. Exchanging information on shareholders;

    c. Exercising their powers to obtain all Beneficial Owner information on behalf of competent foreign authorities.

2. The Concerned Authorities shall oversee the quality of execution of incoming international cooperation relating to requests for Basic Information and Beneficial Owner information of Companies and Legal Arrangements,

including requests concerning the identification of a Beneficial Owners resident outside the State.

3. The Concerned Authorities shall retain Basic Information and Beneficial Owner information of Companies and Legal Arrangements in a secure and easily accessible manner.

4. The Concerned Authorities shall designate and make publicly available contact points responsible for exchanging Basic Information and Beneficial Owner information of Companies and Legal Arrangements.

Article (63)

The Supervisory Authority for Financial Institutions shall:

1. Exchange Crime-related information that it holds or has access to, directly or indirectly, with foreign counterpart authorities, regardless of their nature, in accordance with International Core Principles for Financial Supervision, particularly those relating to the exchange of supervisory information relevant to Anti-Money Laundering, Combating the Financing of Terrorism, as applied by each authority.

2. Exchange information for Crime countermeasures purposes with other Supervisory Authorities having shared responsibility over Financial Institutions operating within the same Financial Group, including:

    a. Regulatory information, such as information relating to the regulatory system and general information on financial sectors;

    b. Prudential information under the Core Principles, such as information on the Financial Institution activities and operations, their Beneficial Owners, management, and fit and properness;

    c. Crime countermeasure information, such as internal policies and procedures of Financial Institutions for combating Crime, customer due diligence information, customer files, and samples of accounts and Transaction information.

3. Obtain prior consent from foreign Supervisory Authorities providing information before referring or using such information for supervisory or non-supervisory purposes, and notify them where disclosure results from a legal obligation.

4. Request information on behalf of foreign Supervisory Authorities or facilitate their access to information for the purpose of enhancing supervision over the Financial Group.

Article (64)

1. The Concerned Authorities shall apply the provisions of this Chapter in exchanging information and executing international cooperation requests relating to Crimes involving Virtual Assets and Virtual Asset Service Providers as promptly and comprehensively as possible.

2. The Supervisory Authority over Virtual Asset Service Providers shall exchange information with foreign counterpart authorities, regardless of differences in designation or regulatory status of the counterpart authority or the Virtual Asset Service Providers in other countries.

Article (65)

The Law Enforcement Authorities shall:

1. Exchange information that they hold or have access to, directly or indirectly, including disclosure system and customs information, with foreign counterpart authorities for detection or intelligence-gathering purposes related to a Crime, identification and tracing of Criminal Property or Funds of equivalent value, and support freezing, seizure, and confiscation measures through mutual judicial assistance.

2. Initiate domestic reports based on information received from foreign counterpart authorities, on their own initiative or upon request of the Public Prosecution, and conduct detections and gather intelligence accordingly.

3. Spontaneously exchange information relating to Criminal Property or Funds of equivalent value with foreign counterpart authorities, and identify and trace them within the State where there are grounds to believe they are linked to investigations in another country, without impeding any ongoing domestic detections or investigations in the State.

4. Exercise all legally available powers to conduct investigations, gather intelligence, and provide information, documents, or other evidence in execution of international cooperation requests.

5. Obtain information on behalf of foreign counterpart authorities and coordinate the formation of bilateral or multilateral joint investigation teams to carry out joint detection.

Part Three: International Judicial Cooperation

Article (66)

Competent judicial authorities shall, upon request from judicial authorities of another country with which the State has a valid agreement, or on the basis of reciprocity, promptly, and in a constructive, and effective manner provide judicial assistance in investigations, prosecutions, or proceedings relating to the Crime, and may order:

1. The identification, tracing, evaluation, seizure, freezing, or confiscation of Criminal Funds or Property, or funds of equivalent value. The fact that the accused is unknown, lacks criminal responsibility, or that the criminal proceedings have lapsed shall not prevent the adoption of such measures.

2. Any other investigative measures or methods that may be applied in accordance with the legislation in force in the State, including the provision of records held by Financial Institutions, Designated Non-Financial Businesses and Professions, Virtual Asset Service Providers, or Non-Profit Organizations, the search of persons and premises, the collection of witness statements, evidence gathering, and the use of investigative methods such as covert operations, interception of communications, the collection of electronic data and information, and controlled delivery.

3. The surrender and recovery of persons and Criminal Property expeditiously without undue delay.

Article (67)

International judicial cooperation requests relating to judgments or judicial orders providing for seizure, freezing, or other provisional measures, or confiscation in all its forms of Criminal Property or funds of equivalent value issued by competent courts or judicial authorities of another country may be executed. For the execution of such request, it shall not be required to conduct national investigations, where the request contains sufficient information and facts on which its execution may be based.

Article (68)

Execution of judgments or judicial orders referred to in Article (67) of this Resolution, shall be subject to the condition that it does not conflict with a judgment or order previously issued by a court in the State, and that there is no case pending in the State concerning the same subject matter as that in respect of which the judgment was issued by the requesting country. The request shall include the following documents and information:

1. A certified copy of the confiscation judgment or order, the law upon which it is based, and the statement of the reasons for its issuance where not stated therein;

2. Proof that the convicted person was duly summoned, properly represented, and was enabled to defend themselves;

3. A document confirming that the judgment or order is final and enforceable;

4. A description of the Criminal Property or funds of equivalent value sought to be confiscated, an assessment of their value, their probable location, and information on any person who may be holding or possessing them;

5. A statement of the value of the amount sought to be recovered from the funds subject to confiscation;

6. Any information relating to third-party rights in the criminal property or funds of equivalent value subject to confiscation;

7. A statement of measures taken by the requesting country to protect bona fide third parties.

Article (69)

1. Competent judicial authorities may request judicial assistance from judicial authorities of another country to uncover the Crime, its circumstances, and perpetrators, and to identify, trace, evaluate, freeze, seize, or confiscate Criminal funds or property, or funds of equivalent value, or to recover such funds or property, or to request the recovery of objects or persons.

2. Where the competent judicial authorities of another country requires a judicial order issued by courts of the State for execution of judicial assistance pursuant to Clause (1), competent court, as the case may be, shall issue such order on its own initiative or upon request of the Public Prosecution following the approval of the Attorney General or their delegate.

Chapter Nine: Final Provisions

Article (70)

Cabinet Resolution No. (10) of 2019, referred to herein, is hereby repealed, and any provision that contradicts or conflicts with the provisions of this Resolution is also repealed.

Article (71)

This Resolution shall be published in the Official Gazette and shall enter into force thirty (30) days after the date of its publication.

Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

CBUAE-BOD 59/4/2019 Effective from 13/7/2019

Central Bank Board of Directors' Decision No. 59/4/2019 Regarding Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations

CBUAE-BOD 59/4/2019 Effective from 13/7/2019 **Status:** In-Force

Chairman of the Board,

Having perused the provisions of the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities;

Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations;

Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations; and

Circular No. 24/2000 - Regulation concerning Procedures for Anti-Money Laundering and its amendments.

The Central Bank's Board of Directors has issued the following resolution:

Article (1):

	Definitions
UAE:	United Arab Emirates.
Decree Federal Law:	Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
Executive Regulation:	Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.
The Central Bank:	Central Bank of the UAE.
Financial Institution:	Anyone, licensed or registered by the Central Bank, who conducts one or several of the financial activities or operations, defined in Article (2) of the Executive Regulation, of or on behalf of a customer.

Article (2):

Financial Institution and its concerned persons must comply with the requirements mentioned in the Decree Federal Law, the Executive Regulation, instructions, guidelines and notices issued by the Central Bank relating to implementation of the Decree Federal Law and the Executive Regulation.

Article (3):

The Central Bank shall supervise and examine, periodically or unexpectedly, without prior notice to the Financial Institution, to verify the Financial Institution's compliance with the Decree Federal Law, the Executive Regulation, relevant instructions, guidelines and notices issued by the Central Bank and shall identify any violations resulting from the examination.

The Central Bank shall request all information and documents it deems necessary for the purpose of supervision and verification from the Financial Institution or its employees.

Article (4):

Without prejudice to any of the sanctions or measures contained in any other legislation, the Central Bank may, upon the violation by any Financial Institution of any of the provisions referred to in Article (2) of this Decision, impose any of the administrative sanctions specified in the Decree Federal Law.

Article (5):

The violator may appeal against the decision on the violation, in accordance with the procedures prescribed by the Central Bank in this regard.

Article (6):

The Central Bank may publish its administrative sanctions in the various means of publication.

Article (7):

Circular No. 24/2000 - Regulation concerning Procedures for Anti-Money Laundering and its amendments shall be canceled.

Article (8):

This Decision shall be communicated to whomsoever is concerned for implementation, and shall be published in the Official Gazette in both Arabic and English.

Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions

Effective from 13/7/2023 **Status:** In-Force

Part I—Overview

1. Introduction

1.1 Purpose and Scope

The purpose of these **Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organisations Guidelines for Financial Institutions (FIs)** (Guidelines) is to provide guidance and assistance to

supervised institutions that are FIs, in order to assist their better understanding and effective performance of their statutory obligations under the legal and regulatory framework in force in the United Arab Emirates (UAE or State).

These Guidelines have been prepared as a joint effort between the Supervisory Authorities of the UAE, and set out the minimum expectations of the Supervisory Authorities regarding the factors that should be taken into consideration by each of the supervised financial institutions which fall under their respective jurisdictions, when identifying, assessing and mitigating the risks of money laundering (ML), the financing of terrorism (FT), and the financing of illegal organisations.

Nothing in these Guidelines is intended to limit or otherwise circumscribe additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback, whether direct or indirect, which may be published on occasion by any of the Supervisory Authorities in respect of the supervised institutions which fall under their respective jurisdictions, or in respect of any specific supervised institution.

Finally, it should be noted that, guidance on the subject of the United Nations Targeted Financial Sanctions (TFS) regime, and the related Cabinet Decision No. (74) of 2020 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* is outside of the scope of these Guidelines.

1.2 Applicability

Unless otherwise noted, these Guidelines apply to all Financial Institutions, and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and their respective Financial and Commercial Free Zones, whether they establish or maintain a Business Relationship with a Customer, or engage in any of the financial activities and/or transactions or the trade and/or business activities outlined in Articles (2) and (3) of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations*.

Specifically, they are applicable to all such natural and legal persons in the following categories:

- Banks, finance companies, exchange houses, money service businesses (including *hawaladar* or other monetary value transfer services);
- Insurance companies, agencies, and brokers;
- Securities and commodities brokers, dealers, advisors, investment managers;
- Virtual asset service providers (VASPs);
- Other financial institutions not mentioned above.

1.3 Legal Status

Article 44.11 of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

As such, these Guidelines do not constitute additional legislation or regulation, and are not intended to set legal, regulatory, or judicial precedent. They are intended rather to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE and their respective Free Zones, and supervised institutions are reminded that the Guidelines do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between these Guidelines and the legal or

regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in these Guidelines should be interpreted as providing any explicit or implicit guarantee or assurance that the Supervisory or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

These Guidelines, and any lists and/or examples provided in them, are not exhaustive and do not set limitations on the measures to be taken by supervised institutions in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, these Guidelines should not be construed as legal advice or legal interpretation. Supervised institutions should perform their own assessments of the manner in which they should meet their statutory obligations, and they should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to their particular circumstances.

1.4 Organisation of the Guidelines

These Guidelines are organized into five (5) parts, roughly corresponding to the following major themes:

Part I—Overview (including background information on the UAE's AML/CFT legislative and strategy framework, and highlights of key provisions of the law and regulations affecting Financial Institutions);

Part II—Identification and Assessment of ML/FT Risks;

Part III—Mitigation of ML/FT Risks;

Part IV—AML/CFT Compliance Administration and Reporting (including guidance on governance, suspicious transaction reporting, and record-keeping);

Part V—Appendices.

The various sections and sub-sections of each part are organized according to subject matter. In general, each section or subsection includes references to the articles of the AML-CFT Law and/or the AML-CFT Decision to which it pertains. While it has been kept to a minimum, users may find that there are instances of repetition of some content throughout various sections of the Guidelines. This has been done in order to ensure that each section or sub-section pertaining to a specific subject matter is comprehensive, and to minimize the need for cross-referencing between sections.

In some cases, the requirements or provisions of specific sections of the relevant legal and regulatory frameworks are deemed sufficiently clear with regard to the statutory obligations of supervised institutions such that no additional guidance on those sections is provided for in these Guidelines. In other cases, guidance is provided with regard to subjects which are not covered explicitly in the AML-CFT Law or the AML-CFT Decision, but which are nevertheless addressed either implicitly or by reference to international best practices.

In certain instances in which there are meaningful differences between the relevant legal and regulatory framework currently in force and previous laws or regulations, or in which there are differences in specific regulatory requirements between various Supervisory Authorities, the Guidelines may or may not highlight these differences. In the event of such differences or discrepancies, supervised institutions seeking further clarification on matters related to those sections are invited to contact their relevant Supervisory Authority through the established channels.

It is the Supervisory Authorities' intention to update or amend these Guidelines from time to time, as and when it is deemed appropriate. Supervised institutions are reminded that these Guidelines are not the only source of guidance on the assessment and management of ML/FT risk, and that other bodies, including international organisations such as FATF,

MENAFATF and other FATF-style regional bodies (FSRBs), the Egmont Group, and others also publish information that may be helpful to them in carrying out their statutory obligations. It is the sole responsibility of supervised institutions to keep apprised and updated at all times regarding the ML/FT risks to which they are exposed, and to

maintain appropriate risk identification, assessment, and mitigation programmes, and to ensure their responsible officers, managers and employees are adequately informed and trained on the relevant policies, processes, and procedures.

Text from the AML-CFT and the AML-CFT Decision are quoted, or otherwise summarized or paraphrased, from time to time throughout these Guidelines. For the sake of convenience, unless specifically noted to the contrary, all references in the text to the term "financing of terrorism" also encompass the financing of illegal organisations. In general, capitalized terms in the text of these Guidelines have the meanings provided in the Glossary of Terms (see Appendix 11.1). However, in the event of any inconsistency or discrepancy between the text or definitions provided for in the Law and/or the Cabinet Decision and such quotations, summaries or paraphrases, or such defined terms, the former shall prevail.

2. Overview of the AML/CFT Legal, Regulatory, and National Strategy Frameworks of the United Arab Emirates

2.1 National Legislative and Regulatory Framework

The legal and regulatory structure of the UAE is comprised of a matrix of federal civil, commercial and criminal laws and regulations, together with the various regulatory and Supervisory Authorities responsible for their implementation and enforcement, and various local civil and commercial legislative and regulatory frameworks in the Financial and Commercial Free Zones. As criminal legislation is under federal jurisdiction throughout the State, including the Financial and Commercial Free Zones, the crimes of money laundering, the financing of terrorism, and the financing of illegal organisations are covered under federal criminal statutes and the federal penal code. Likewise, federal legislation and implementing regulations on the combating of these crimes are in force throughout the UAE, including the Financial and Commercial Free Zones. Their implementation and enforcement are the responsibility of the relevant regulatory and Supervisory Authorities in either the federal or local jurisdictions.

The principal AML/CFT legislation within the State is Federal Decree-Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations* (the "AML-CFT Law" or "the Law") and implementing regulation, Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* (the "AML-CFT Decision" or "the Cabinet Decision").

The UAE issued Cabinet UBO Resolution No. 58 of 2020 on the Regulation of the Procedures of the Real Beneficiary (UBO Resolution) which came into effect on 28 August 2020 and replaced Cabinet Resolution No. 34 of 2020 issued earlier this year.

The UBO Resolution introduces the requirement for a beneficial ownership register in the UAE mainland and unifies the minimum disclosure requirements for corporate entities incorporated in the UAE mainland and in the non-financial free zones. Financial free zones (Abu Dhabi Global Market (ADGM) and Dubai International Financial Centre (DIFC) and companies owned by the Federal Government and their subsidiaries are not covered by the UBO Resolution.

2.2 International Legislative and Regulatory Framework

The AML/CFT legislative and regulatory framework of the UAE is part of a larger international AML/CFT legislative and regulatory framework made up of a system of intergovernmental legislative bodies and international and regional regulatory organisations. On the basis of international treaties and conventions in relation to combating money laundering, the financing of terrorism and the prevention and suppression of the proliferation of weapons of mass destruction, intergovernmental legislative bodies create laws at the international level, which participating member countries then transpose into their national counterparts. In parallel, international and regional regulatory

organisations develop policies and recommend, assess and monitor the implementation by participating member countries of international regulatory standards in respect of AML/CFT.

Among the major intergovernmental legislative bodies, and international and regional regulatory organisations, with which the government and the Competent Authorities of the State actively collaborate within the sphere of the international AML/CFT framework are:

- The United Nations (UN): The UN is the international organization with the broadest range of membership. Founded in October of 1945, there are currently 191 member states of the UN from throughout the world. The UN actively operates a program to fight money laundering, the Global Programme against Money Laundering (GPML), which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).

- The Financial Action Task Force (FATF): The Financial Action Task Force (FATF) is an intergovernmental body established in 1989, which sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF also monitors the implementation of its standards, the 40 FATF Recommendations and 11 Immediate Outcomes, by its members and members of FSRBs, ensures that the 'FATF Methodology' for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems is properly applied.

- The Middle East and North Africa Financial Action Task Force (MENAFATF): Recognizing the FATF 40 Recommendations on Combating Money Laundering and the Financing of Terrorism and Proliferation, and the related UN Conventions and UN Security Council Resolutions, as the worldwide-accepted international standards in the fight against money laundering and the financing of terrorism and proliferation, MENAFATF was established in 2004 as a FATF Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with those standards. The UAE is one of the founding members of MENAFATF.

- The Egmont Group of Financial Intelligence Units: In 1995, a number of FIUs began working together and formed the Egmont Group of Financial Intelligence Units (Egmont Group) (named for the location of its first meeting at the Egmont-Arenberg Palace in Brussels). The purpose of the group is to provide a forum for FIUs to improve support for each of their national AML/CFT programs and to coordinate AML/CFT initiatives. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel, and fostering better communication among FIUs through technology, and helping to develop FIUs worldwide.

2.3 AML/CFT National Strategy Framework

Money laundering and the financing of terrorism are crimes that threaten the security, stability and integrity of the global economic and financial system, and of society as a whole. The estimated volume of the proceeds of crime, including the financing of terrorism, that are laundered each year is between 2-5% of global GDP. Yet, by some estimates, the volume of criminal proceeds that are actually seized is in the range of only 2% of the total, while roughly only half of that amount eventually ends up being confiscated by competent judicial authorities. Combating money laundering and the financing of terrorist activities is therefore an urgent priority in the global fight against organised crime.

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organisations. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and

promoted by FATF, MENAFATF and the other FSRBs, as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

As part of these efforts, the Competent Authorities of the UAE have taken a number of substantive actions, including among others:

- Enhancing the federal legislative and regulatory framework, embodied by the introduction of the new AML/CFT Law and Cabinet Decision, which incorporate the FATF standards;

- Conducting the National Risk Assessment (NRA) to identify and assess the ML/FT threats and inherent vulnerabilities to which the country is exposed, as well as to assess its capacity in regard to combating ML/FT at the national level;

- Formulating a National AML/CFT Strategy and Action Plan that incorporate the results of the NRA and which are designed to ensure the effective implementation, supervision, and continuous improvement of a national framework for the combating of ML/FT, as well as to provide the necessary strategic and tactical direction to the country's public and private sector institutions in this regard.

The National Strategy on Anti-Money Laundering and Countering the Financing of Terrorism of the United Arab Emirates is based on four pillars, each of which is associated with its own strategic priorities. These strategic priorities in turn inform and shape the key initiatives of the country's National Action Plan on AML/CFT.

The pillars of the National Strategy, together with their strategic priorities are summarised in the table below:

National AML/CFT Strategic Pillars	Strategic Priorities
Legislative & Regulatory Measures	Increase effectiveness and efficiency of legislative and regulatory policies and ensure compliance
Transparent Analysis of Intelligence	Leverage the use of financial databases and the development of information analysis systems to enhance the transparent analysis and dissemination of financial intelligence information
Domestic and International Cooperation & Coordination	Promote the efficiency and effectiveness of domestic and international coordination and cooperation with regard to the availability and exchange of information
Compliance and Law Enforcement	Ensure the effective investigation and prosecution of ML/FT crimes and the timely implementation of TFS

The National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations has identified a number of key drivers of success in achieving the goals of the National AML/CFT Strategy. These include, among other things, ensuring:

- Effective coordination between the Financial Intelligence Unit, Law Enforcement Authorities, Public Prosecutors, Supervisory Authorities, and other Competent Authorities within the country;

- Effective compliance with the laws and regulations governing banking activities and other financial services;

- Awareness by FIs of the relevant ML/FT risks facing the UAE in general, and their sectors in particular, as informed by the results of the NRA, as well as their awareness of their statutory obligations in regard to the management and mitigation of those risks.

The present *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions* are thus intended to advance the efforts of the Committee, the Supervisory Authorities, and the other Competent Authorities of the State in this direction.

3. Highlights of Key Provisions Affecting Financial Institutions

The AML-CFT Law and the AML-CFT Decision contain numerous provisions setting out the rights and obligations of supervised institutions, including Financial Institutions, as well as their senior managers and employees. This section highlights some of the key provisions affecting FIs that are of immediate concern. FIs are reminded that it is their sole responsibility to adhere to all provisions of the AML-CFT Law, the AML-CFT Decision, and all regulatory notices, rulings and circulars affecting them.

3.1 Summary of Minimum Statutory Obligations of Supervised Institutions

The AML-CFT Law and the AML-CFT Decision set out the minimum statutory obligations of supervised institutions as follows:

- To identify, assess, understand risks (AML-CFT Law Article 16.1(a), AML-CFT Decision Article 4.1);
- To define the scope of and take necessary due diligence measures (AML-CFT Law Article 16.1(b), AML-CFT Decision Article 4.1(a) and 2);
- To appoint a compliance officer, with relevant qualification and expertise and in line with the requirements of the relevant Supervisory Authority (AML-CFT Decision Article 21, 44.12);
- To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation (AML-CFT Law Article 16.1(d), AML-CFT Decision Article 4.2(a));
- To put in place indicators to identify suspicious transactions (AML-CFT Law Article 15, AML-CFT Decision Article 16);
- To report suspicious activity and cooperate with Competent Authorities (AML-CFT Law Article 9.1, 15, 30, AML-CFT Decision Article 13.2, 17.1, 20.2);
- To promptly apply directives of Competent Authorities for implementing UN Security Council decisions under Chapter 7 of the UN Convention for the Prohibition and Suppression of the FT and Proliferation (AML-CFT Law Article 16.1(e), AML-CFT Decision Article 60);
- To maintain adequate records (AML-CFT Law Article 16.1(f), AML-CFT Decision Article 7.2, 24).

Specific guidance on these and other provisions of the AML-CFT Law and the AML-CFT Decision is provided in the following sections.

3.2 Confidentiality and Data Protection

(AML-CFT Law Article 15; AML-CFT Decision Articles 17.2, 21.2, 31.3, 39)

Financial Institutions are obliged to report to the UAE's Financial Intelligence Unit (FIU) when they have reasonable grounds to suspect a transaction or funds representing all or some proceeds, or suspicion of their relationship to a Crime (see Section 7, Suspicious Transaction Reporting). In reporting their suspicions, they must maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorised person.

It should be noted that the confidentiality requirement does not pertain to communication within the FI or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of a Crime. However, under no circumstances are FIs, or their managers or employees, permitted to inform a Customer or the representative of a Business Relationship, either directly or indirectly, that a report has been made, under penalty of sanctions (see Section 3.9, Sanctions against Persons Violating Obligations). This is the so-called "tipping off" requirement. This also extends to any related information that might be provided to the FIU or information that is being requested by the FIU.

FIs are not permitted to object to the statutory reporting of suspicions on the grounds of Customer confidentiality or data privacy, under penalty of sanctions. Moreover, data protection laws include provisions that allow the FI to report to the authorities. (see Section 3.9, Sanctions against Persons Violating Obligations).

3.3 Protection against Liability for Reporting Persons

(AML-CFT Law Article 27; **AML-CFT Decision** Article 17.3**)**

The AML-CFT Law and the AML-CFT Decision provide Financial Institutions, as well as their board members, employees and authorised representatives, with protection from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This protection is also applicable if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

3.4 Statutory Prohibitions

(AML-CFT Law Article 16.1(c)**; AML-CFT Decision** Articles 13.1, 14, 35.4, 38**)**

Financial Institutions are prohibited from the following activities:

- Establishing or maintaining any Customer or Business Relationship, conducting any financial or commercial transactions, keeping any accounts under an anonymous or fictitious name or by pseudonym or number;
- Establishing or maintaining a Business Relationship or executing any transaction in the event they are unable to complete adequate risk-based CDD measures in respect of the Customer for any reason;
- Dealing in any way with Shell Banks, whether to open (correspondent) bank accounts in their names, or to accept funds or deposits from them;
- Invoking banking, professional or contractual secrecy as a pretext for refusing to perform their statutory reporting obligation in regard to suspicious activity;
- Issuing or dealing in bearer shares or bearer share warrants.

3.5 Money Laundering

(AML-CFT Law Articles 2.1-3, 4, 29.3, **AML-CFT Decision** Article 1**)**

The AML-CFT Law defines money laundering as engaging in any of the following acts willfully, having knowledge that the funds are the proceeds of a felony or a misdemeanour (i.e., a predicate offence):

- Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source;

- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds;

- Acquiring, possessing or using proceeds upon receipt;

- Assisting the perpetrator of the predicate offense to escape punishment.

Both the AML-CFT Law and the AML-CFT Decision define "funds" in a very broad sense as "assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets." They likewise define "proceeds" as "funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds."

Therefore, in order to be considered money laundering, it is not necessary for any of the above-stipulated acts to involve only money or monetary instruments per se, but any number of tangible or intangible assets such as, but not limited to:

- Funds bank or other financial accounts, including so-called virtual or crypto currencies;

- Financial instruments or securities, such as shares, bonds, notes, commercial paper, promissory notes, IOUs, share warrants, options, rights (including land rights), or other transferrable securities or bearer negotiable instruments;

- Contracts, loan instruments, titles, claims, insurance policies, or their assignment;

- Intellectual property (including but not limited to patents or registered trademarks), royalties, licenses, or the rights thereto;

- Physical property, including but not limited to commodities, land, precious metals and stones, motor vehicles or vessels, works of art, or any other goods exchanged as payment-in-kind.

The size or monetary value of the financial or commercial transaction, the timeframe during which it took place, and the nature of the funds or proceeds (whether in liquid funds or some other tangible or intangible asset) are irrelevant to the suspicion and reporting of a suspicious transaction.

The AML-CFT Law designates money laundering as a criminal offence. Its prosecution is independent of that of any predicate offence to which it is related or from which the proceeds are derived. The suspicion of money laundering is not dependent on proving that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved, but can be inferred from certain information, including indicators or behavioural patterns.

According to the 2018 National Risk Assessment, professional third-party money laundering has been identified as one of the top ML/FT threats in the UAE.

3.6 Predicate Offences

The AML-CFT Law defines a predicate offence as "any act constituting an offence or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries." A predicate offence is therefore any crime, whether felony or misdemeanour, which is punishable in the UAE, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

FATF has designated 21 (twenty-one) categories of predicate offences. Each of these categories of predicate offences has been criminalised in the legislative framework of the State. FIs are reminded that this is not an

exhaustive list of predicate offences, but simply a convenient categorisation, since in the UAE according to the AML-CFT Law, even crimes that do not appear on this list, whether felonies or misdemeanours, can be predicate offences to money laundering.

Based on expert analysis of these categories conducted on behalf of the UAE's Competent Authorities for the 2018 National Risk Assessment, the top (highest) threats to the State in relation to money laundering have been identified as: fraud, counterfeiting and piracy of products, illicit trafficking in narcotic drugs and psychotropic substances, and professional third-party money laundering.

Similarly, other (medium-high) threats of particular concern to the UAE in relation to money laundering have been identified as the categories of: insider trading and market manipulation, robbery and theft, illicit trafficking in stolen and other goods, forgery, smuggling (including in relation to customs and excise duties and taxes), tax crimes (related to direct taxes and indirect taxes), and terrorism (including terrorist financing).

While FIs should pay special attention to the most serious threats identified in the NRA and any topical risk assessment when performing their own ML/FT business risk assessments, they are reminded that their risk assessment operations should consider all categories of risk for applicability to their own particular circumstances.

3.7 Financing of Terrorism

(AML-CFT Law Articles 3.1, 4, 29.3, **AML-CFT Decision** Article 1**)**

The AML-CFT Law designates the financing of terrorism as a criminal offence, which is not subject to the statute of limitations. It defines the financing of terrorism as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organisation or terrorist person or intended to finance a terrorist organisation, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or

- Providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or committing such acts on behalf of a terrorist organisation or a terrorist person while aware of their true background or purpose.

There are numerous risk factors that FIs should consider important when assessing their exposure to the risk of terrorist financing (see Section 4.1.1, Risk Factors), including geographic-, sector-, channel-, product-, service- and customer-specific risks.

In a 2019 report by MENAFATF, an assessment of the global threat posed by the financing of terrorism stated:

> "The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organisations such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfil their basic need to generate and manage funds is also evolving.
>
> Terrorist organisations use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation; and social services. These financial requirements are usually high for large terrorist organisations, particularly those that aim to, or do, control territory. In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management."[1]

[1] *Social Media and Terrorism Financing: A joint project by Asia/Pacific Group on Money Laundering & Middle East and North Africa Financial Action Task Force*, APG/MENAFATF, January 2019, p.4.

3.8 Financing of Illegal Organisations

(AML-CFT Law Articles **3.2**, **4**, **29.3**, **AML-CFT Decision** Article **1)**

Like the financing of terrorism, the AML-CFT Law designates the financing of illegal organisations as a criminal offence that is not subject to the statute of limitations. The Law defines the financing of illegal organisations as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by an illegal organisation or by any person belonging to an illegal organisation or intended to finance such illegal organisation or any person belonging to it, even if without the intention to conceal or disguise their illicit origin.

- Providing, collecting, preparing, obtaining proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an Illegal organisation or of any of its members, with knowledge of its true identity or purpose.

- When assessing their risk exposure to the financing of illegal organisations, FIs should pay special attention to the regulatory disclosure, accounting, financial reporting and audit requirements of organisations with which they conduct Business Relationships or transactions. This is particularly important where non-profit, community/social, or religious/cultural organisations are involved, especially when those organisations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason.

3.9 The ML Phases

To identify, understand and accurately assess the ML/FT risks to which FIs are exposed at both the enterprise and business relationship levels, FIs should be aware of the three phases of money laundering. By determining for which ML/FT phase a certain product can be misused or the FI itself can be misused, will help the FI understand its specific inherent ML/FT risks. The paragraphs below describe the crime of money laundering as consisting of three distinct (though sometimes overlapping) phases:

Placement. In this phase, criminals attempt to introduce Funds or the Proceeds of Crime into the financial system using a variety of techniques or typologies (see Section 3.10, ML/FT Typologies).

Examples of placement transactions include the following:

- Blending of funds: Commingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned businesses.
- Foreign exchange: Purchasing of foreign exchange with illegal funds.
- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade attention or reporting requirements.
- Currency smuggling: Cross-border physical movement of cash or monetary instruments.
- Loans: Repayment of legitimate loans using laundered cash.

Layering. Once the Funds or Proceeds are introduced, or placed, into the financial system, they can proceed to the next phase of the process; often, this is accomplished by placing the funds into circulation through formal financial institutions, and other legitimate businesses, both domestic and international." In this layering phase, criminals attempt to disguise the illicit nature of the Funds or Proceeds of Crime by engaging in transactions, or layers of transactions, which aim to conceal their origin.

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- Moving funds from one financial institution to another or within accounts at the same institution;
- Converting the cash placed into monetary instruments;
- Reselling high-value goods and prepaid access/stored value products;
- Investing in real estate and other legitimate businesses;
- Placing money in stocks, bonds or life insurance products; and
- Using shell companies to obscure the ultimate beneficial owner and assets.

Integration. In this phase, criminals attempt to return, or integrate, their "laundered" Funds or the Proceeds of Crime back into the economy, or to use it to commit new criminal offences, through transactions or activities that appear to be legitimate.

A key objective for criminals engaged in money laundering—and therefore a key generic risk underlying the specific risks faced by FIs—is the exploitation of situations and factors (including products, services, structures, transactions, and geographic locations) which favour anonymity and complexity, thereby facilitating a break in the "paper trail" and concealment of the illicit source of the Funds.

Although the sizes of transactions related to the financing of terrorism and illegal organisations can be (much) smaller than those involved in money laundering operations, and some of the typologies and specific techniques used may differ, the overall principles and generic risks are the same. The terrorists and criminals involved in these acts attempt to exploit situations and factors favouring anonymity and complexity, in order to obscure and conceal the illicit source of the Funds, or the illicit destination or purpose for which they are intended, or both. FIs should remain careful that their services are not being used either directly or indirectly to facilitate Money Laundering or the Financing of Terrorism or Illegal Organisations in any of the three stages described above.

3.10 ML/FT Typologies

The methods used by criminals for money laundering, the financing of terrorism, and the financing of illegal organisations are continually evolving and becoming more sophisticated. It is therefore critical in combating these crimes for FIs to ensure that their personnel are kept up-to-date on the latest ML/FT trends and typologies.

There are numerous useful sources of research and information related to ML/FT typologies, including by the Supervisory Authorities, the FATF, MENAFATF and other FSRBs, the Egmont Group, and others. FIs should incorporate the regular review of ML/FT trends and typologies into their compliance training programmes (see Section 8.2, Staff Screening and Training), as well as into their risk identification and assessment procedures.

Examples of some of the key ML/FT typologies with which FIs should be familiar include (but are not limited to):

- **Currency exchanges / cash conversion**: used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimize risk of detection – e.g., purchasing of travellers cheques to transport value to another jurisdiction.
- **Cash couriers / currency smuggling**: concealed movement of currency to avoid transaction / cash reporting measures.
- **Structuring (smurfing)**: A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.
- **Use of credit cards, cheques, promissory notes, etc.**: Used as instruments to access funds held in a financial institution, often in another jurisdiction.

- **Purchase of portable valuable commodities (gems, precious metals, etc.)**: A technique to purchase instruments to conceal ownership or move value without detection and avoid AML/CFT measures – e.g., movement of diamonds or gold to another jurisdiction.
- **Purchase of valuable assets (real estate, race horses, vehicles, etc.)**: Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.
- **Commodity exchanges (barter)**: Avoiding the use of money or financial instruments in value transactions to avoid AML/CFT measures - e.g., a direct exchange of heroin for gold bullion.
- **Use of wire transfers**: to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation.
- **Underground banking / unlicensed remittance services**: Illegal mechanisms based on networks of trust used to remit monies, without the proper license or registration. Often work in parallel with the traditional banking sector and exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.
- **Trade-based money laundering and terrorist financing**: usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.
- **Abuse of non-profit organizations (NPOs)**: May be used to raise terrorist funds, obscure the source and nature of funds and to distribute funds for terrorist activities.
- **Investment in capital markets**: to obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low reporting requirements.
- **Mingling (business investment)**: A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the illegal source of the funds.
- **Use of shell companies/corporations**: a technique to obscure the identity of persons controlling funds and exploit relatively low reporting requirements.
- **Use of offshore banks/businesses, including trust company service providers**: to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.
- **Use of nominees, trusts, family members or third parties, etc**: to obscure the identity of persons controlling illicit funds.
- **Use of foreign bank accounts**: to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.
- **Identity fraud / false identification**: used to obscure the identity of those involved in many methods of money laundering and terrorist financing.
- **Use "gatekeepers" professional services (lawyers, accountants, brokers, etc.)**: to obscure the identity of beneficiaries and the illicit source of funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.
- **New Payment technologies**: use of emerging payment technologies for money laundering and terrorist financing. Examples include cell phone-based remittance and payment systems.
- **Virtual assets:** (VA) and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. FIs may refer to the FATF Recommendations that place AML/CFT requirements on Virtual Assets (VA) and Virtual Asset Service Providers (VASPs). The FATF has also issued a document on Guidance on Risk Based Approach to VAs and VASPs. FIs should be familiar with the AML/CFT risks of dealing with VAs and VASPs in accordance with the FATF guidance.
- **Life insurance products** can be for instance be used for money laundering when they have saving or investment features which may include the options for full or partial withdrawals or early surrenders.
- **General insurance product**: there are several cases where the early cancellation of policies with return of premium has been used to launder money.
    - A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;
    - Return premium being credited to an account different from the original account;
    - Requests for return premiums in currencies different from the original premium;

    - Regular purchase and cancellation of policies.
- **Overpayment of premiums**: arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made, in this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally' but on a recurring basis, significantly overpay his premiums and request a refund for the excess.

The UAE FIU releases reports on Trends and Typologies of Money Laundering which is an analysis based on the information extracted from the suspicious transaction reports (STRs) filed by reporting entities. This is a very useful resource for FIs for understanding the prevalent typologies of ML and FT crimes as well as getting information on the latest trends on these crimes in the country. This report is released on the FIU's GoAML System for STR reporting and therefore, is accessible to registered users of this system.

Links to some other official sources, which may be useful in keeping up-to-date with regard to ML/FT typologies, may be found in Appendix 11.2.

3.11 Sanctions against Persons Violating Reporting Obligations

(AML-CFT Law Articles **15**, **24**, **25)**

The AML-CFT Law provides for the following sanctions against any Financial Institutions, their managers or their employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering or the financing of terrorism or of illegal organisations:

- Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- Any of these two sanctions.

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a Crime. It should also be noted that the transactions or funds that are the subject of the suspicion may represent only part of the proceeds of the criminal offence, regardless of their value.

Likewise, the AML-CFT Law provides for sanctions against anyone who warns or notifies a person of a suspicious transaction report or reveals that a transaction is under review or investigation by the Competent Authorities, as follows:

- Imprisonment for no less than six months and a penalty of no less than AED100,000 and no more than AED500,000; or
- Any of these two sanctions.

Part II—Identification and Assessment of ML/FT Risks

4. Identification and Assessment of ML/FT Risks

(AML-CFT Law Article **16.1**; **AML-CFT Decision** Article **4.1)**

Both the AML-CFT Law and the AML-CFT Decision provide that FIs may utilize a risk-based approach with respect to the identification and assessment of ML/FT risks.

FIs are obliged to assess and to understand the ML/FT risks to which they are exposed, and how they may be affected by those risks. Specifically, the AML-CFT Law provides that they shall:

> *"...continuously assess, document, and update such assessment based on the various risk factors established in the Implementing Regulation of this Decree-Law and maintain a risk identification and assessment analysis with*

its supporting data to be provided to the Supervisory Authority upon request."

Furthermore, the AML-CFT Decision charges supervised institutions with:

"...Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."

Guidance on these subjects is provided in the following sections.

4.1 Risk-Based Approach (RBA)

A risk-based approach (RBA) is central to the effective implementation of the AML/CFT legislation. It means that FIs identify, assess, and understand the ML/TF risks to which they are exposed, and implement the most appropriate mitigation measures. An RBA requires financial institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good AML/CFT compliance program and will enable FIs to focus their resources where the risks are higher. In this regard, FIs can take into account their business nature, size and complexity.

(AML-CFT Law Article **16.1; AML-CFT Decision** Article **4.1-3)**

Implicit in both the AML-CFT Law and the AML-CFT Decision is the well-established concept of a risk-based approach (RBA) to the identification and assessment of ML/FT risks. Specifically, the AML-CFT Law states that FIs should "identify crime risks within (their) scope of work" and should update their risk assessments on the basis of the various risk factors set out in the AML-CFT Decision. Likewise, the AML-CFT Decision states that FIs' identification, assessment and understanding of the risks should be carried out "in concert with their business nature and size," and that various risk factors should be considered in determining the level of mitigation required. The AML-CFT Decision further provides that enhanced due diligence should be performed in cases where high risks are identified, while simplified due diligence may be performed in certain cases where low risk is identified, unless there is a suspicion of ML/FT.

An RBA to AML/CFT means that FIs should identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. This will require an understanding of the ML/TF risk faced by UAE (national risks), risks by the sector and the FI as well as specific products and services, customer base, the capacity in which customers are operating, jurisdictions in which they operate , the delivery channel and the effectiveness of risk controls put in place.

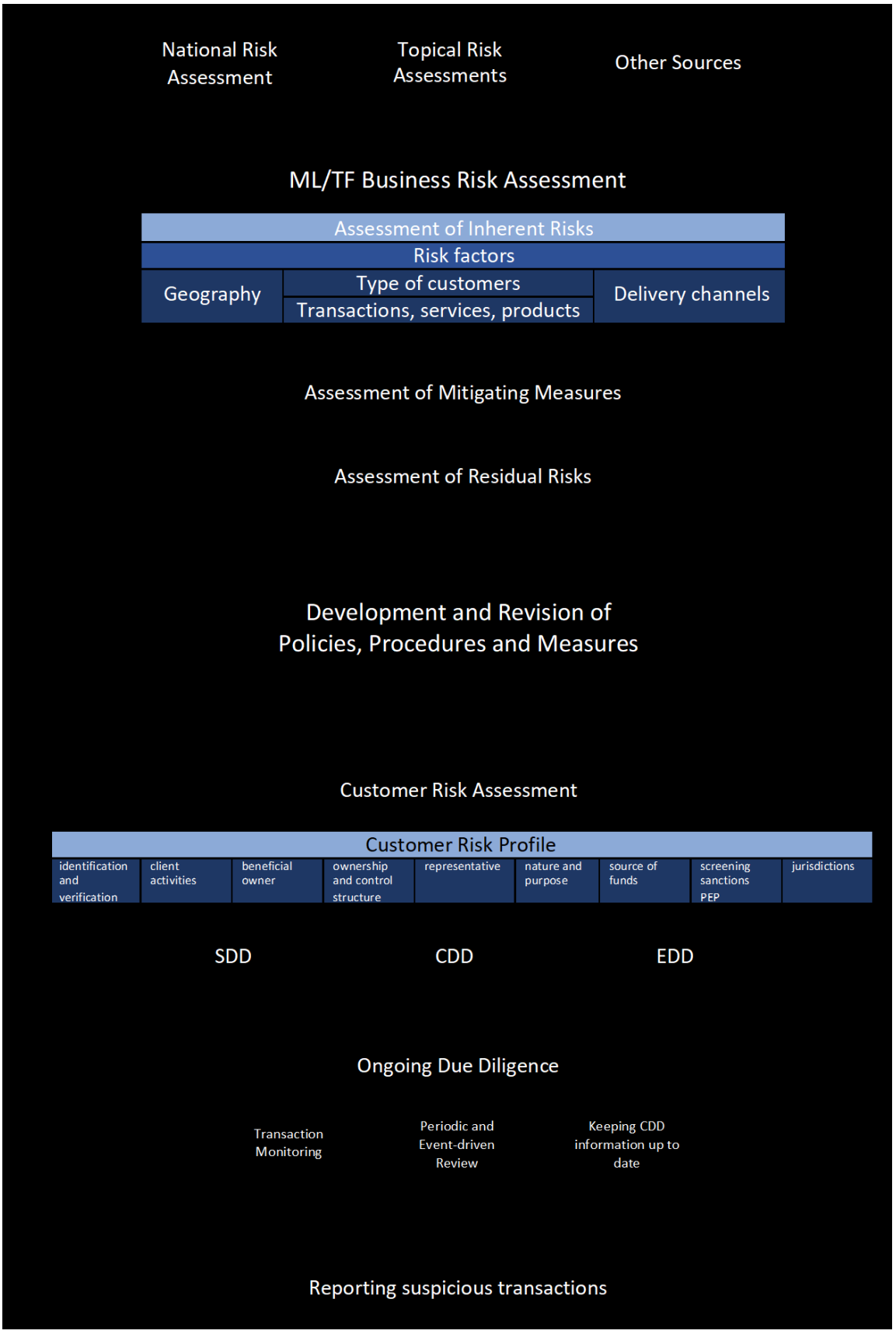
The use of an RBA thus allows FIs to allocate their resources more efficiently and effectively, within the scope of the national AML/CFT legislative and regulatory framework, by adopting and applying preventative measures that are targeted at and commensurate with the nature of risks they face.

While there are limits to any risk-management approach, and no RBA can be considered as completely failsafe; there may be occasions where an FI has taken all reasonable measures to identify and mitigate ML/TF risks, but it is still used for ML/TF in isolated instances. FIs should nevertheless understand that a risk-based approach is not a justification for ignoring certain ML/FT risks, nor does it exempt them from taking reasonable and proportionate mitigation measures, even for risks that are assessed as low. Their statutory obligations require them to identify, assess and understand the level of (inherent) risks presented by their (types of) customers, products and services, transactions, geographic areas and delivery channels, and to be in a position to apply sufficient AML/CFT mitigation measures on a risk-appropriate basis at all times.

In order to do so, they should identify and assess their exposure to ML/FT risks on the basis of a variety of risk factors (see Section 4.1, Risk Factors), some of which are related to the nature, size, complexity and operational environment of their businesses, and others of which are customer- or relationship-specific. Furthermore, they should take reasonable and proportionate risk mitigation measures based on the severity of the risks identified.

Conducting an ML/TF business risk assessments can assist FIs to understand their risk exposure and the areas they should give priority in combating ML/FT. The extent of business-wide risks to which an FI is exposed may require different levels of AML/CFT resources and mitigation strategies.

The following picture is a schematic overview of the RBA process from an ML/TF business risk assessments to developing policies, procedures and measures to CDD and the reporting of suspicious transactions.



4.1.1 Assessing Business-wide Risks

(AML-CFT Law Article 16.1; AML-CFT Decision Article 4.1)

An important first step in applying an RBA is to identify, assess and understand the ML/FT risks by way of an ML/FT risk assessment of the entire business. The purpose of such an ML/FT business risk assessment is to improve the effectiveness of ML/FT risk management, by identifying the inherent ML/FT risks faced by the enterprise as a whole, determining how these risks are effectively mitigated through internal policies, procedures and controls, and establishing the residual ML/FT risks and any gaps in the controls that should be addressed.

Thus, an effective ML/TF business risk assessment can allow FIs to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are appropriately aligned with residual risks.

The first step of conducting an ML/TF business risk assessment for FIs is to identify, assess and understand the inherent ML/FT risks (i.e., the risks that an FI is exposed to if there were no control measures in place to mitigate them) across all business lines and processes with respect to the following risk factors: customers, products, services and transactions, delivery channels, geographic locations, and any other risk factors.

With the inherent risks as a basis, the FI can determine the nature and intensity of risk mitigating controls to apply to the inherent risks. The level of inherent ML/FT risks influence the kinds and levels of AML/CFT resources and mitigation strategies which FIs require to put in place. The assessment of inherent ML/FT risks and of the effectiveness of the risk mitigation measures will result in a residual risk assessment, i.e., the risks that remain when effective control measures are in place. In case the residual risk falls outside the risk appetite of the FI, additional control measures will need to be implemented to ensure that the level of ML/FT risk is acceptable to the FI.

FIs may utilise a variety of models or methodologies to analyse their risks, in keeping with the nature and size of their businesses. FIs should decide on both the frequency and methodology of an ML/FT business risk assessment, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/FT risks to which they are exposed, as well as the results of the NRA and Topical Risk Assessments. In most cases, FIs should consider performing the ML/FT business risk assessment at least annually; however assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. They should also decide on policies and procedures related to the periodic review of their ML/TF business risk assessment methodology, taking into consideration changes in internal or external factors. These decisions should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

As part of the model or methodology, FIs should consider including in their ML/FT risk assessment the following elements:

- Likelihood or probability of occurrence of identified inherent risks;
- Timing of identified inherent risks;
- Impact on the organisation of identified inherent risks.

The result of an effective ML/FT business risk assessment will be the classification of identified risks into different categories, such as high, medium, low, or some combination of those categories (such as medium-high, medium-low). Such classifications may assist FIs to prioritise their ML/FT risk exposures more effectively, so that they may determine the appropriate types and levels of AML/CFT resources needed, and adopt and apply reasonable and risk-proportionate mitigation measures.

4.1.2 Risk Factors

As part of the business-wide ML/TF risk assessment, a proper identification of risk factors is crucial to the effective assessment of ML/FT risk. Risks will often occur as combinations of these risk factors. A risk can for instance occur

because of the interrelationship between a customer and the jurisdictions where the customer is from or is active, or because of the connection between a product and the delivery channel.

Identified risk factors are used for the accurate categorisation of inherent risks, as well as for the application of appropriate mitigation measures. At the enterprise level, this includes adopting and applying adequate policies, procedures, and controls to business processes (see Section 5.1, Internal Policies, Controls and Procedures). The policies, procedures, and controls will in turn address the risks at the individual customer level, including assigning appropriate risk classifications to customers and applying due diligence measures that are commensurate with the identified risks (see Section 6, Customer Due Diligence).

The AML-CFT Decision outlines several risk factors which FIs must consider, when identifying and assessing their ML/FT risk exposure. FIs may also consider a wide array of additional risk factors, utilising various sources, such as:

- ML/FT red-flag indicators;
- Input and information from relevant internal sources, including the designated AML/CFT compliance officer;
- Information from national sources, including the results of the NRA or any Topical Risk Assessment with regard to ML/FT trends and sectoral threats and notices or circulars from the relevant Supervisory Authorities;
- Information from publications of relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, UNODC, and others. (Links to some of these sources may be found in Appendix 11.2.)

In keeping with the ever-evolving nature of ML/FT risks, and in order to ensure that FIs implement a model for conducting the ML/TF business risk assessment that is appropriate to the nature and size of their businesses, FIs should continuously update the risk factors which they consider, in order to reflect new and emerging ML/FT risks and typologies.

A good practice to assess the inherent risk factors, is for FIs to formulate risk scenarios and assess the likelihood that a scenario occurs and the impact should a scenario materialize. The likelihood can be assessed based on the number of times per year that a risk scenario can occur. The impact can be assessed based on the possible financial and reputational effects that can result if a scenario indeed occurs. In this way, the FI can determine the inherent risks of a risk factor.

When assessing the inherent risks, an FI should make an inventory of the customers it services, the products and services it offers, define the scope of business areas to assess, including business units, legal entities, divisions, countries and regions. For this, an FI should make use of up-to-date quantitative and qualitative information on for instance, the types and number of customers, the volume of operations for the types of customers, volume of business per product and services and geographic locations.

Examples with regard to some of the major risk factors that should be taken into account by FIs when conducting the ML/TF business risk assessment are provided in the sections below. Even though some of these risk factors will also be relevant for the risk assessment of an individual Customer or Business Relationship, for the ML/TF business risk assessment, FIs are reminded that they should take a holistic view when evaluating exposure to these categories of customers.

4.1.3 Customer Risk

The customer risk factors relate to types or categories of customers. Certain customer or business relationship categories pose a risk that should be taken into account when assessing the overall level of inherent customer risk. When identifying certain categories of customers as inherently high risk, FIs should also consider the results of the NRA or any Topical Risk Assessment, as well as information from official sources, including the Supervisory Authorities, the FIU, the FATF, MENAFATF and other FSRBs, the Egmont Group, etc.

When assessing the customer risk factors with respect to the business-wide ML/FT risk assessment, an FI can take into account:

- Type of customers: The risks related to retail customers in combination with their product/service needs may be different from those related to high net worth or corporate customers and their respective product/service needs. Likewise, the risks associated with resident customers may be different from those associated with non-resident customers.

- Customer base. FIs with small, homogenous customer bases may face different risks from those with larger, more diverse customer bases. Similarly, FIs targeting growing or emerging markets may face different customer risks than those with more established customer bases.

- Maturity of relationship. FIs that rely on more transactional, occasional, or one-off interactions with their customers may be exposed to different risks from institutions with more repetitive or long-term business relationships.

The specific customer risk factors that FIs should consider, include:

- Categories of business relationships with complex legal, ownership, or direct or indirect group or network structures, or with less transparency with regard to Beneficial Ownership, effective control, or tax residency, may pose different ML/FT risks than those with simpler legal/ownership structures or with greater transparency.

- Categories of Customers involved in highly regulated and supervised activities and those involved in activities that are unregulated.

- Customers associated with higher-risk persons or professions (for example, foreign PEPs and/or their companies), or those linked to sectors associated with higher ML/FT risks.

- Non-resident entities particularly those with connections to offshore and high risk jurisdictions.

- Professionals (e.g., lawyers, accountants and TCSPs) acting as introducer or intermediary on behalf of customers or groups of customers (whereby there is no direct contact with the customer).

- High net worth individuals.

- Respondent banks from high risk countries.

Some of these customer risk factors are also relevant when determining the customer risk classification of an individual customer and the type and extent of customer due diligence to be performed (see Section 6, Customer Due Diligence).

4.1.4 Geographic Risk

FIs should consider geographic ML/FT risk factors both from domestically and cross-border sources. These risks arise from: (i) the locations where the FI has offices, branches and subsidiaries and (ii) locations in which the customers reside or conduct their activities. Examples of some of these factors include:

- Regulatory/supervisory framework. Countries with stronger AML/CFT controls present a different level of risk than countries with weaker regulatory and supervisory frameworks, for instance countries identified by the FATF as jurisdictions with weak AML/CFT measures.

- International Sanctions. FIs should consider whether the countries or jurisdictions they deal with are the subject of international sanctions, such as targeted financial sanctions (TFS), UAE, OFAC, UN and EU restrictive

measures, that could impact their ML/FT risk exposure and mitigation requirements.

- Reputation. FIs should consider whether the countries or jurisdictions they deal with are associated with higher or lower levels of ML/FT, corruption, and (lack of) transparency (particularly as regards financial and fiscal reporting, criminal and legal matters, and Beneficial Ownership, but also including such factors as freedom of information and the press).

- Combination with customers' inherent risk factors. FIs should consider the countries risk in combination with customers risks, including principal residential or operating locations of customers.

4.1.5 Product-, Service-, Transaction-Related Risk

When assessing the inherent ML/FT risks associated with product, service, and transaction types, an FI should take stock of its lines of business, products and services that are more vulnerable to ML/FT abuse. FIs should assess the inherent ML/FT risks of abuse of the products and services by their customers taking into account a number of factors such as their ease for holding and transferring value or their complexity and transparency. Some of the risk factors that FIs should consider, among others, are:

- Typology. FIs should consider whether the product, service, or transaction type is associated with any established ML/FT typologies (see Section 3.10, ML/FT Typologies).

- Complexity. Products, services, or transaction types that favour complexity, especially when that complexity is excessive or unnecessary, can often be exploited for the purpose of money laundering and/or the financing of terrorism or illegal organisations. FIs should consider the conceptual, operational, legal, technological and other complexities of the product, service, or transaction type. Those with higher complexity or greater dependencies on the interactions between multiple systems and/or market participants may expose FIs to different types and levels of ML/FT risk than those with lower complexity or with fewer dependencies on multiple systems and/or market participants.

- Transparency and transferability. Situations that favour anonymity can often be exploited for the purpose of ML/FT. FIs should consider the level of transparency and transferability of ownership or control of products, services, or transaction types, particularly in respect of the ability to monitor the identities and the roles/responsibilities of all parties involved at each stage. Special attention should be given to products, services, or transaction types in which funds can be pooled or co-mingled, or in which multiple or anonymous parties can have authority over the disposition of funds, or for which the transferability of Beneficial Ownership or control can be accomplished with relative ease and/or with limited disclosure of information.

- Size/value. Products, services, or transaction types with different size or value parameters or limits may pose different levels of ML/FT risk.

4.1.6 Delivery Channel-Related Risk

Different delivery channels for the acquisition and management of customers and business relationships, as well as for the delivery of products and services, entail different types and levels of ML/FT risk.

When evaluating delivery channel-related risk, FIs should pay particular attention to those channels, whether related to customer acquisition and/or relationship management, or to product or service delivery, which have the potential to favour anonymity. Among others, these may include non-face-to-face channels (especially in cases where there are no safeguards in place such as electronic identification means), such as internet-, phone-, or other remote-access services or technologies; the use of third-party business introducers, intermediaries, agents or distributors; and the use of third-party payment, or other transaction intermediaries.

4.1.7 Other Risk Factors

Given the ever-evolving nature of ML/FT risks, new risks are constantly emerging, while existing ones may change in their relative importance due to legal or regulatory developments, changes in the marketplace, or as a result of new or disruptive products or technologies. For this reason, no list of risks can ever be considered as exhaustive.

Nevertheless, additional factors that may present specific risks are, e.g., the introduction of new products or services, new technologies or delivery processes or the establishment of new branches and subsidiaries locally and abroad.

In order to ensure, therefore, that FIs are in a position to review and update the ML/TF business risk assessment as well as mitigation measures, FIs should take into consideration the results of the NRA or any Topical Risk Assessment. They should also consult publications from official sources on a regular basis, including those of the relevant Supervisory Authorities, the FIU, the FATF, MENAFATF and other FSRBs, the Egmont Group, and others. Links to some of these sources may be found in Appendix 11.2.

Examples of some of the types of additional risk factors which FIs may consider in identifying and assessing their ML/FT risk exposure include:

- Novelty/innovation. FIs should consider the depth of experience with and knowledge of the product, service, transaction, or channel type. Products, services, transaction, or delivery channel types that are new to the market or to the enterprise may not be as well understood as, and may therefore pose a different level of ML/FT risk than, more established ones. Likewise, products, services, transaction, or delivery channel types which are unexpected or unusual with respect to a particular type of customer may indicate a different level of potential ML/FT risk exposure than would more traditional or expected product, service, transaction, or channel types in regard to that same type of customer.

- Cyber security/distributed networks. FIs may consider evaluating the degree to which their operational processes and/or their customers expose them to the risk of exploitation for the purpose of professional third-party money laundering and/or the financing of terrorism or of illegal organisations, through cyber-attacks or through other means, such as the use of distributed technology or social networks. An example of such a risk is the recent dramatic increase in the global incidence of so-called CEO fraud, in which fraudsters troll companies with phishing e-mails that are purportedly from the CEO or other senior executives, and attempt to conduct fraudulent transactions or obtain sensitive data that can be used for criminal purposes.

4.1.8 Assessing New Product and New Technologies Risks

(AML-CFT Decision Article 23)

As part of their obligation to update their ML/FT risk assessments on an ongoing basis, the AML-CFT Decision specifically requires FIs to "identify and assess the risks of money laundering and terrorism financing that may arise when developing new products and new professional practices, including means of providing new services and using new or under-development techniques for both new and existing products."

FIs must complete the assessment of such risks, and take the appropriate risk management measures, prior to launching new products and services, practices or techniques, or technologies. In general, they should integrate these ML/FT risk assessment and mitigation requirements into their new product, service, channel, or technology development processes.

For the purpose of assessing the ML/FT risks associated with new products, services, practices, techniques, or technologies, FIs may consider utilising the same or similar risk assessment models or methodologies as those utilised for their ML/FT business risk assessments, updated as necessary for the particular circumstances. They

should also document the new product, service, practice, technique, or technology risk assessments, in keeping with the nature and size of their businesses (see Section 4.6.1, Documentation, Updating and Analysis).

4.2 Risk Assessment Methodology and Documentation

(AML-CFT Law Article **16.1(a) and AML-CFT Decision** Article **4.1)**

A well-documented assessment of the identified inherent risk factors (see Section 4.1, Risk Factors) is fundamental to the adoption and effective application of reasonable and proportionate ML/FT risk-mitigation measures. Thus, the result of such an ML/TF business risk assessment allows for a systematic categorisation and prioritization of inherent and residual ML/FT risks, which in turn allows FIs to determine the types and appropriate levels of AML/CFT resources needed for mitigation purposes.

An effective ML/TF business risk assessment is not necessarily a complex one. The principle of a risk-based approach means that FIs' risk assessments should be commensurate with the nature and size of their businesses. FIs with smaller or less complex business models may have simpler risk assessments than those of institutions with larger or more complex business models, which may require more sophisticated risk assessments.

4.2.1 Risk Assessment Methodology

(AML-CFT Decision Article 4.1(b))

The AML-CFT Decision obliges FIs to document their risk assessment operations. FIs may utilise a variety of models or methodologies in assessing their ML/FT risk. FIs should determine the type and extent of the risk assessment methodology that they consider to be appropriate for the size and nature of their businesses, and should document the rationale for these decisions.

To be effective, a risk assessment should be based on a methodology that:

- Is based on quantitative and qualitative data and information and makes use of internal meetings or interviews; internal questionnaires concerning risk identification and controls; review of internal audit reports;
- Reflects the FI's management-approved AML/CFT risk appetite and strategy;
- Takes into consideration input from relevant internal sources, including input and views from the designated AML/CFT compliance officer and other relevant units like risk management and internal control;
- Takes into consideration relevant information (such as ML/FT trends and sectoral risks) from external sources, including the NRA or any Topical Risk Assessment, Supervisory and other Competent Authorities, and the FATF, MENAFATF and other FSRBs, the Egmont Group, and others where appropriate;
- Describes the weighting of risk factors, the classification of risks into different categories, and the prioritisation of risks.
- Evaluates the likelihood or probability of occurrence of identified ML/FT risks, and determining their timing and impact on the organization.
- Takes into account whether the AML/CFT controls are effective, specifically whether there are adequate controls to mitigate risks concerning customers, products, services, or transactions.
- Determines the effectiveness of the AML/CFT risk mitigating measures in place by using information such as audit and compliance reports or management information reports.

- Determines the residual risk as a result of the inherent risks and the effectiveness of the AML/CFT risk mitigating measures.
- Establishes based on the residual risk and the risk appetite, whether additional AML/CFT controls have to be put in place.
- Determines the rationale and circumstances for approving and performing manual interventions or exceptions to model-based risk weightings or classifications.
- Is properly documented and maintained, regularly evaluated and updated, and communicated to management and relevant personnel within the organisation.
- Is tested and audited for the effectiveness and consistency of the risk methodology and its output with regard to statutory obligations.

4.2.2 Documentation and Updating

(AML-CFT Law Article 16.1(a) and AML-CFT Decision Article 4.1(a)-(b))

Documentation

FIs are obliged to document their ML/TF business risk assessment, including methodology, analysis, and supporting data, and to make them available to the Supervisory Authorities upon request. FIs should incorporate into their documentation, the information used to conduct the ML/TF business risk assessment in order to demonstrate the effectiveness of their risk assessment processes. Examples of such information include, but are not limited to:

- Organization's overall risk policies (for example, risk appetite statement, customer acceptance policy, and others, where applicable).
- ML/FT risk assessment model, methodology and procedures, including such information as organizational roles and responsibilities; process flows, timing and frequency; internal reporting requirements; and review, testing, and updating requirements.
- Risk factors identified, and input received from relevant internal sources, including the designated AML/CFT compliance officer.
- Details of the inherent and residual risk-factor analysis that constitutes the risk assessment.

The documentation measures taken by FIs should be reasonable and commensurate with the nature and size of their businesses.

Updating

FIs are obliged to keep their ML/TF business risk assessment up-to-date on an ongoing basis. In fulfilling this obligation, they should review and evaluate their ML/FT business risk assessment processes, models, and methodologies periodically, in keeping with the nature and size of their businesses. FIs should also update their ML/TF business risk assessment whenever they become aware of any internal or external events or developments which could affect their accuracy or effectiveness.

Such developments may include, among other things, changes in business strategies or objectives, technological developments, legislative or regulatory developments, or the identification of material new ML/FT threats or risk factors. In this regard, FIs should take into consideration the results of the most recent NRA or any Topical Risk Assessment, as well as circulars, notifications and occasional published information from official sources, such as

the Supervisory Authorities; other national Competent Authorities; or relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others. Links to some of these sources may be found in Appendix 11.2.

Part III—Mitigation of ML/FT Risks

The Elements of an AML/CFT Program

Commonly referred to as the three lines of defense, the basic elements that must be addressed in an AML/ CFT program are

- A system of internal policies, procedures and controls, including an ongoing employee training program (first line of defense);
- A designated compliance function with a compliance officer or money laundering reporting officer (second line of defense); and
- An independent audit function to test the overall effectiveness of the AML program (third line of defense).

In setting up these three lines of defense, FIs can take into account their business nature, size and complexity.

(AML-CFT Law Article 16.1(b), 16.1(d); AML-CFT Decision Articles 4.2 , 4.3)

FIs are obliged to take the necessary measures to manage and mitigate the ML/FT risks to which they are exposed. Both the AML-CFT Law and the AML-CFT Decision provide that FIs may utilize a risk-based approach with respect to mitigation of ML/FT risks.

5. Internal Policies, Controls and Procedures

Policies:

Clear and simple high-level statements that are uniform across the entire organization (sets the tone from the top).

Procedures:

Translates the AML/CFT policies into an acceptable and workable practice, tasking the stakeholders with their respective responsibilities.

Controls:

The internal technology or tools the financial institution utilizes to ensure the AML/CFT program is functioning as intended and within predefined parameters.

(AML-CFT Law Article 16.1(d); AML-CFT Decision Articles 4.2(a), 20)

The AML-CFT Law and the AML-CFT Decision require FIs to implement internal policies, controls and procedures that enable them to manage and mitigate the ML/FT risks they have identified in their ML/TF business risk assessment, in keeping with the nature and size of their businesses. Such policies, controls and procedures must be approved by senior management, reviewed for effectiveness and continuously updated, and must apply to all branches, subsidiaries and affiliated entities in which FIs hold a majority interest (see Section 8.3, Group Oversight for more guidance). They must also take into consideration the results of the NRA and Topical Risk Assessments.

Additionally, FIs should ensure that the policies, controls and procedures they implement to manage and mitigate ML/FT risks are reasonable, proportionate to the risks involved, and consistent with the results of their ML/TF business risk assessments.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, FIs should consider the results of the NRA and any Topical Risk Assessment as well as their own ML/FT business risk assessment. Commensurate with the nature and size of the FIs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

In developing the internal AML/CFT control systems, FIs should also take into account their IT infrastructure and management information systems capabilities. FIs should consider how well their technical infrastructure, including their data management and management information reporting capabilities, are suited to the ML/FT risk mitigation requirements of the types of customers they deal with, particularly in respect of the size and growth dynamics of their customer base.

The internal policies, controls and procedures that FIs design to prevent, detect and deter ML/FT risks can be categorised broadly as those related to:

- The identification and assessment of ML/FT risks (see Section 4.5, Business-wide Risk Assessment).
- Customer due diligence (CDD), including enhance due diligence (EDD), and simplified due diligence (SDD) (see Section 6, Customer Due Diligence), including its review and updating, and reliance on third parties in regard to it.
- Customer and transaction monitoring, and the reporting of suspicious transactions (see Section 7, Suspicious Transaction Reporting).
- AML/CFT governance, including compliance staffing and training, senior management responsibilities, and the independent auditing of risk mitigation measures (see Section 8, Governance).
- Record-keeping requirements (see Section 9, Record Keeping).

Guidance in relation to these categories is provided in the above-referenced sections.

6. Customer Due Diligence (CDD)

MAIN ELEMENTS OF A CUSTOMER DUE DILIGENCE PROGRAM

- Customer Identification;
- Profiles;
- Customer Acceptance;
- Risk rating;
- Monitoring;
- Investigation; and
- Documentation

(AML-CFT Law Article 16.1(b); AML-CFT Decision Articles 4.2(b), 4.3, 5-13, 14, 15, 19, 20.1, 22, 24.2-4, 25, 27, 29.2, 30, 31.1, 35.1-2 and 5, 37.1-2, 44.10, 55.1)

6.1 Risk-Based Application of CDD Measures

The AML-CFT Law implicitly recognises the need for an RBA to customer due diligence measures, by obliging FIs to "take the necessary due diligence measures and procedures and define their scope, taking into account the various risk factors and the results of the national risk assessment…." This principle is further emphasised by the AML-CFT Decision, which explicitly provides for the application of enhanced due diligence (EDD) measures to manage identified high risks (see Section 6.4, Enhanced Due Diligence (EDD) Measures), and of simplified due diligence (SDD) to manage identified low risks in the absence of a suspicion of ML/FT (see Section 6.5, Simplified Due Diligence (SDD) Measures).

FIs are reminded, that each customer's ML/FT risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behaviour, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, FIs should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/FT risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/FT risk category. This means that the CDD measures are not to be taken as a static formula but that depending on the risk of a customer the intensity and depth of the CDD measures should vary.

6.1.1. Assessing Customer and Business Relationship Risk

(AML-CFT Law Article 16.1; AML-CFT Decision Article 4.1)

A customer can be anyone who performs a one-off or occasional financial activity or transaction or anyone who establishes an ongoing commercial or financial relationship with the FI.

The accurate assessment of customer or business relationship risk is fundamental to the risk classification of customers and the effective application of appropriate risk-based customer due diligence measures. FIs should take the necessary steps to ensure that their customer or business relationship risk assessment processes are robust and reliable, and that they incorporate the results of the NRA, any Topical Risk Assessment and their own ML/TF business risk assessment, as well as the input of relevant internal stakeholders, including the designated AML/CFT compliance officer.

In assessing customer or business relationship risk, FIs should analyse customers on the basis of the identified risk factors in order to arrive at a risk classification. FIs may utilize different methodologies to accomplish their risk classification, depending on the nature and size of their businesses, and of the risks involved. For example, some entities with smaller or less complex businesses, or with more homogenous customer bases, may elect to assess business relationship risk and assign customer risk classifications on the basis of generic profiles for customers of the same type. Other larger or more complex FIs may elect to assess business relationship risk and assign customer risk classifications using more sophisticated models or scorecards based on weightings of various risk factors.

Regardless of the methodologies they choose, FIs should ensure that their business relationship risk assessment processes and the rationale for their methodologies are well-documented, approved by senior management, and communicated at the appropriate levels of the organisation. They should also decide on policies and procedures related to both the periodic review of their business relationship risk assessment processes, and to the frequency for updating the individual business relationship risk assessments and customer risk classifications produced by them, taking into consideration changes in internal or external factors.

6.1.2 Establishing a Customer Risk Profile

(AML-CFT Decision Articles 7.1, 8.3-4)

FIs should establish a risk profile for their customers, commensurate with the types and levels of risk involved. Such risk profiles allow FIs to compare a customer's actual activity with the expected activity more effectively, and thus contribute to their capacity to discover unusual circumstances or potentially suspicious transactions.

Where legal persons or legal arrangements are concerned, FIs are obliged to identify any natural person who owns or controls an interest of 25% or more. In order to achieve an effective understanding of the ownership and control structure of a customer that is a legal person or arrangement, FIs should obtain from the customer and including in the risk profile a detailed explanation or a company structure chart providing the details of any ownership interests of 25% or more, and tracing them through any intermediate entities (whether legal persons or arrangements, or natural persons who are nominee stakeholders) to the natural persons who ultimately own or control them.

Furthermore, in order to understand the nature of the business of a legal person or Legal Arrangement, FIs should obtain and include in the profile a detailed explanation or company structure chart showing the entity's internal

management structure, identifying the persons holding senior management positions, or other positions of control. They should also obtain information about the legal person's or arrangement's majority-owned or controlled operating subsidiaries, including the nature of the business and the operating locations of those subsidiaries.

FIs are also required to understand the intended purpose and nature of the Business Relationship, and, for legal persons or arrangements, the nature of the customer's business and its ownership and control structure.

Based on the risk profile, FIs should carry out ongoing due diligence of their Business Relationships, so as to be able to ensure that the transactions conducted are consistent with the information they have about the customer, the type of activity they are engaged in, the risks they entail, and, where necessary, their source of funds.

When dealing with higher-risk or more complex customers, in addition to the type of information referred to above, FIs may obtain and include in the customer's risk profile more detailed information about their customers' activities, such as:

- Anticipated size and/or turnover of account balances or transactional activity;
- Expected types and volumes of transactions;
- Known or expected counterparties or third-party intermediaries with whom the customer conducts transactions;
- Known or expected locations related to transactional activity;
- Anticipated timing or seasonality of transactional activity.

Where lower-risk customers are concerned, FIs may consider applying more generic risk profiles in order to compare actual and expected types and levels of activity.

6.2 Circumstances and Timing for Undertaking CDD Measures

(AML-CFT Decision Article 5.1)

Under normal circumstances, FIs are obliged to undertake CDD measures (including verifying the identity of customers, Beneficial Owners, beneficiaries, and controlling persons) either prior to or during the establishment of a Business Relationship or the opening of an account, or prior to the execution of a transaction for a customer with whom there is no Business Relationship. Guidance in regard to these requirements and certain exceptional circumstances provided for in the AML-CFT Decision is provided in the sub-sections below.

6.2.1 Establishment of a Business Relationship

FIs establish a Business Relationship with a customer when they perform any act for, on behalf of, or at the direction or request of the customer, with the anticipation that it will be of an ongoing or recurring nature, whether permanent or temporary. Such acts may include, but are not limited to:

- Assigning an account number or opening an account in the customer's name;
- Effecting any transaction in the customer's name or on their behalf, or at the customer's direction or request for the benefit of someone else;
- Providing any form of tangible or intangible product or service (including but not limited to granting credits, guarantees, or other forms of value) to or on behalf of the customer, or at the customer's direction or request for the benefit of someone else;

- Signing any form of contract, agreement, letter of intent, memorandum of understanding, or other document with the customer in relation to the performance of a transaction or series of transactions, or to the provision of any form of tangible or intangible product or service as described above;

- Accepting any form of compensation or remuneration (including a promise of future payment) for the provision of tangible or intangible products or services, as described above, from or on behalf of the customer;

- Receiving funds or proceeds of any kind (including those held on a fiduciary basis, for safekeeping, or in escrow) from or on behalf of the customer, whether for their account or for the benefit of someone else;

- Any other act performed by FIs in the course of conducting their ordinary business, when done on behalf of, or at the request or direction of, a customer.

In such cases, and other than in the exceptional circumstances described below (see Section 6.2.3, Exceptional Circumstances), FIs are required to undertake appropriate risk-based CDD measures (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures for further guidance).

In addition, CDD also needs to be conducted when

- there is a ML/FT suspicion (see Section 7.2, Identification of Suspicious Transactions);

- there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Among other things, the CDD measures should include verifying the identity of the customer as well as the Beneficial Owners, beneficiaries, and controlling persons, and understanding the nature of their business and the purpose of the Business Relationship.

6.2.2 Occasional Transactions

During the course of business, FIs may be called upon to perform occasional or non-recurring transactions for customers with whom there is no ongoing account or Business Relationship. Examples of such transactions include, but are not limited to:

- Exchange of currencies;

- Issue or cashing/redemption of traveler's cheques;

- Transfer of money or other value for a walk-in customer;

On such occasions, and other than in the exceptional circumstances described below (see Section 6.2.3, Exceptional Circumstances), FIs are required to identify the customer and verify the customer's identity as well as that of the Beneficial Owners, beneficiaries, and controlling persons. Furthermore, FIs are required to undertake appropriate risk-based CDD measures (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures for further guidance), including among other things understanding the nature of the customer's business and the purpose of the transaction, in the cases specified in Article 6 of the AML-CFT Decision, as follows:

- When carrying out occasional transactions in favour of a Customer for amounts equal to or exceeding AED 55,000 (or equivalent in any other currency), whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;

- When carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding AED 3,500 (or equivalent in any other currency) (see Section 6.3.2, CDD Requirements Concerning Wire Transfers);

- When there is a ML/FT suspicion (see Section 7.2, Identification of Suspicious Transactions);

- When there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Some of the indicators of transactions that may appear to be linked include, but are not limited to the following:

- Multiple transactions with the same or similar customer reference codes;
- Transactions executed sequentially or in close time proximity, and involving the same or related counterparties;
- Multiple transactions attempted by a customer with whom there is no Business Relationship at different branches of the same FI on the same day.

6.2.3 Exceptional Circumstances

(AML-CFT Decision Articles 4.3, 5.1(a)-(c), 10, 11.1(b), 13.2)

From time to time, certain situations may arise which fall outside of the normal course of CDD processes. Under these circumstances, described below, FIs are permitted to handle the timing, customer identification, and other aspects of customer due diligence procedures exceptionally. Specifically:

- When there is no ML/FT suspicion, and the ML/FT risks are identified as low, FIs may complete the verification of the customer's identity after establishing the Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision. In such circumstances, the verification of the identity must be conducted in a timely fashion, and FIs must ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefiting from the Business Relationship prior to the completion of the verification process. Examples of such measures which FIs may consider taking in this regard are, among others:

  - Holding funds in suspense or in escrow until the verification of the identity is completed;
  - Making the completion of the verification of the identity a condition precedent to the closing of a transaction.

- In the case of Legal Arrangements, such as Trusts or foundations, or of life insurance policies (including funds-generating transactions, such as life insurance products relating to investments and family Takaful insurance) in which there are beneficiaries who are not named, but instead belong to a designated class of future or contingent beneficiaries, FIs are required to obtain sufficient information about the details of the class of beneficiaries so as to be in a position to establish the identity of each beneficiary at the time of the settlement, pay-out, or exercise of their legally acquired rights. Furthermore, FIs must verify the identity of the beneficiaries at the time of settlement or pay-out and prior to the exercise of any related legally acquired rights. They should also ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefiting from the Business Relationship prior to the completion of the verification process. Examples of such measures which FIs may consider taking in this regard are, among others:

  - Holding funds in suspense or in escrow until the verification of the identity is completed;
  - Making the completion of the verification of the identity a condition precedent to the closing of a transaction.

- When a legal entity customer or its controlling stakeholder meets the conditions specified in Article 10.1-2 of the AML-CFT Decision with regard to publicly listed companies (including the condition that information concerning the identity of the shareholders, partners, or Beneficial Owners with an interest of 25% or more is available from reliable sources), FIs are exempted from taking the normally required identity verification measures. In this regard, FIs should ensure that the disclosure and transparency requirements of the regulated stock exchange are at least equivalent to those of the State, and should document the evidence they obtain concerning the relevant disclosure and transparency requirements.

  It is important to note that, while FIs are exempted in such situations from identifying and verifying the identity of the shareholders, partners or Beneficial Owners (or in the event that no such person can be identified, of the relevant senior management officers), they are not exempted from ascertaining the identity of senior management.

  Examples of reliable information sources in this regard include, but are not limited to:

  - Stock exchange disclosure reports or websites;
  - Corporate annual reports, websites, or other forms of official public disclosure;
  - Official or public registries;
  - Credit reporting agencies;
  - Recognized, well-established media outlets.

- When FIs suspect that a customer or Beneficial Owner is involved in the commitment of a crime related to money laundering, the financing of terrorism, or the financing of illegal organisations, and they have reasonable grounds to believe that undertaking customer due diligence measures would tip off the customer, then they should not apply CDD measures, but should instead report their suspicion to the FIU along with the reasons that prevented them from carrying out the CDD measures.

6.3 Customer Due Diligence (CDD) Measures

The application of risk-based CDD measures is comprised of several components, in keeping with the customer's ML/FT risk classification and the specific risk indicators that are identified. Generally, these components include, but are not limited to, the following categories:

- Identification of the customer, Beneficial Owners, beneficiaries, and controlling persons; and the verification of their identity on the basis of documents, data or information from reliable and independent sources (see Section 6.3.1, Customer and Beneficial Owner Identification/Verification).

- Screening of the customer, Beneficial Owners, beneficiaries, and controlling persons, to screen for the applicability of targeted or other international financial sanctions, and, particularly in higher risk situations, to identify any potentially adverse information such as criminal history (see Section 6.4, Enhanced Due Diligence (EDD) Measures).

- Obtaining an understanding of the intended purpose and nature of the Business Relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure (see Section 6.3.3, Establishing a Customer Due Diligence Profile).

- Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behaviour (see Section 6.3.4, Ongoing Monitoring of the Business Relationship).

- Scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the FI's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

- Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

In cases involving higher levels of risk, FIs are generally required to exercise enhanced levels of customer due diligence, such as identifying and/or verifying the customer's source of funds and taking other appropriate risk-mitigation measures (see Section 6.4, Enhanced Due Diligence (EDD) Measures).

As part of their overall AML/CFT framework, FIs should take a risk-based approach in developing the internal CDD policies, procedures and controls. Factors to take into account, include:

- The outcomes of the ML/TF business risk assessment;

- Circumstances, timing, and composition in regard to the application of CDD measures;

- Frequency of reviews and updates in relation to CDD information;

- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which CDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, supervised institutions should consider the results of both the NRA and any Topical Risk Assessment. Commensurate with the nature and size of the FIs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

Additional guidance related to these and other key aspects of risk-based CDD measures is provided in the following sub-sections.

6.3.1 Customer and Beneficial Owner Identification and Verification of the Identity

(AML-CFT Decision Articles 4.2(b), 3(a), 5.1, 8.1, 9, 10, 11.2, 13.1, 14.2)

Grounded on the principles of "Know Your Customer" and risk-based CDD, the identification and verification of the identity of customers is a fundamental component of an effective ML/FT risk management and mitigation programme. In accordance with Cabinet Resolution no. 58 of 2020 regulating the Beneficial Owner Procedures (the UBO Resolution), FIs are obliged to identify customers, including the Beneficial Owners, beneficiaries, and controlling persons, whether permanent or walk-in, and whether a natural or legal person or Legal Arrangement, and to verify their identity using documents, data or information obtained from reliable and independent sources.

The specific requirements concerning the timing, extent, and methods of identifying and verifying the identity of customers and Beneficial Owners depend in part on the type of customer (whether a natural or legal person) and on the level of risk involved (also see Sections 6.4, Enhanced Due Diligence (EDD) Measures, and 6.5, Simplified Due Diligence (SDD) Measures). Thus, the type and nature of the customer (including Beneficial Owners, beneficiaries, and controlling persons) should be considered as risk factors in determining the type of CDD that should be applied, whether standard CDD, EDD or SDD. However, the core components of a customer's identification generally remain the same in all cases. They are:

- Personal data, including details such as the name, passport or identity card number, country of issuance, date issuance and expiry date of the identity card or passport, nationality, date and place of birth (or date and place of

establishment or incorporation, in the case of a legal person or arrangement); and

- Principal address, including evidence of the permanent residential address of a natural person, or the registered address of a legal person or arrangement.

In taking adequate CDD measures, FIs are obliged at a minimum to identify and verify the identity of the customer as specified in the relevant articles of the AML-CFT Decision. In fulfilling these requirements, FIs should use a risk-based approach to determine the internal policies, procedures and controls they implement in relation to the identification and verification of customers (including the Beneficial Owners, beneficiaries, and controlling persons). The CDD policies and procedures that FIs apply should be reasonable and proportionate to the risks involved, and, in formulating them, entities should consider the following guiding principles.

In relation to natural persons:

- The verification of a customer's identity, including their address, should be based on original, official (i.e. government-issued) documents whenever possible. When that is not possible, FIs should augment the number of verifying documents or the amount of information they obtain from different independent sources. In particular, when verifying the UAE ID card, FIs licensed by the Central Bank must use the online validation gateway of the Federal Authority for Identity & Citizenship and keep a copy of the UAE ID and its digital verification. They should also identify the lack of official documents and the use of alternative means of verification as risk factors when assessing the customer's ML/FT risk classification.

  An example of alternative verification means is verification by way of digital identification systems. Such a digital identification systems should rely upon technology, adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results. The FATF Guidance on Digital Identity of March 2020 provides further information on how to making a risk-based determination of whether a particular digital ID system provides an appropriate level of reliability and independence.

- The identification data should include the name, nationality, date of birth and place of birth, and national identification number of a natural person.

- With regard to the identification and verification of the identity of foreign nationals, whether customers or Beneficial Owners, beneficiaries or controlling persons, FIs should take steps to understand and request only those types of identification documents that are legally valid in the relevant jurisdictions. Furthermore, when verifying the identity of foreign nationals associated with high-risk factors, FIs should validate the authenticity of customer identification documents obtained. Some of the methods that FIs may consider in order to do so, commensurate with the nature and size of their businesses, include but are not limited to:

  - Relying on information from the relevant foreign embassy or consulate, or the relevant issuing authority;
  - Using commercially available applications to validate the information in machine-readable zones (MRZs) or biometric data chips of foreign identification documents.

- The types of address verification that may generally be considered acceptable include, but are not limited to, the following categories of documents issued in the name of the customer:

  - Bills or account statements from public utilities, including electricity, water, gas, or telephone line providers;
  - Local and national government-issued documents, including municipal tax records;
  - Registered property purchase, lease or rental agreements;
  - Documents from supervised third-party financial institutions, such as bank statements, credit or debit card statements, or insurance policies.

In situations where natural persons do not have this documentation in their own name, for instance because they share accommodation or do not (yet) have a permanent or own residence, other evidence of address may be used as long as this evidence gives the FI reasonable confidence. Where the FI has determined that an individual has a valid reason for being unable to produce the usual documentation to verify the address and who would otherwise be excluded from establishing a business relationship with the FI, the address can be verified by other means, provided the FI is satisfied that the method employed adequately verifies the address of the natural person and any additional risk has been appropriately mitigated.

This can for instance be evidence of entitlement to a state or local authority-funded benefit, pension, educational or other grant, or a letter from a reputable employer or school stating the address.

In relation to legal persons and legal arrangements:

- In addition to the identifying and verifying the identity of customers, Beneficial Owners, beneficiaries, and controlling persons, FIs should verify the identity of any person legally empowered to act or transact business on behalf of the customer, whether the customer is a legal or natural person. Such persons may include:

    - Signatories or other authorized persons, or persons with authorised remote access credentials to an account, such as internet or phone banking users;
    - Parents or legal guardians of a minor child, or legal guardians of a physically or mentally disabled or incapacitated person;
    - Attorneys or other legal representatives, including liquidators or official receivers of a legal person or arrangement.

    In the event that a legally empowered representative is also a legal person or Legal Arrangement, the normal CDD procedures for such entities should be applied.

- When verifying that a person purporting to act on behalf of a customer is so authorised, the following types of documents may generally be considered to be acceptable:

    - A legally valid power-of-attorney;
    - A properly executed resolution of a legal person's or Legal Arrangement's governing board or committee;
    - A document from an official registry or other official source, evidencing ownership or the person's status as an authorised legal representative;
    - A court order or other official decision.

- As part of their procedures for identifying and verifying the identity of customers, and for authenticating the original documents upon which the verification is based, FIs should include procedures for the certification of the customer identification and address documentation they obtain. Such procedures may encompass certification by employees of the FI (for example, by including the name, title of position, date and signature of the verifying employee(s) on the copies of documents maintained on file), as well as by reputable third parties (for example, by including the name, organization, title of position, date and signature of the verifying person, along with a statement representing that the copy of the document is a "true copy of the original"). In cases where documents are obtained from foreign sources in countries which are members of The Hague Apostille Convention, consideration should be given to requesting documents certified by Apostille seal.

- Whenever possible, FIs should incorporate a "four-eyes" principle (review by at least two people) into their procedures with regard to the verification of customer identification documentation and other CDD information, as well as with regard to the entry of the relevant data into their information systems.

6.3.2 CDD Measures Concerning Wire Transfers

(AML-CFT Decision Articles 27-30)

Financial institutions are obliged to undertake certain CDD measures concerning wire transfers, as laid out in detail in the above-referenced articles of the AML-CFT Decision. In particular, these measures relate to the identification of the originators and beneficiaries; the maintenance of information in regard to the same; and the implementation of risk-based policies and procedures for handling the disposition of wire transfers and for taking appropriate follow-up action.

The purpose of these measures are to ensure that information on the originator and the beneficiary shall accompany (meaning sent at the same time but not necessarily in the same message) cross-border wire transfers at all stages of its execution in case the amount of the transfer of funds equals or exceeds AED 3,500 or equivalent in any other currency.

The FI of the originator (or payer) shall ensure that the transfer of funds is accompanied by the information on the originator and beneficiary (or payee) as follows:

Information on the originator:

- The name of the originator (in case of natural person – the name and surname);
- The originator's account number (or in absence thereof the transfer shall be accompanied by a unique transaction reference number);
- The originator's address, identification document number or customer identification number, and date and place of birth.

Information on the beneficiary:

- The name of the beneficiary (in case of natural person – the name and surname);
- The beneficiary's account number (or in absence thereof, a unique transaction reference number).

In case of cross-border wire transfers of less than AED 3,500 or equivalent it not required to verify the accuracy of the above-mentioned information, unless there are suspicions of ML or TF.

Also for domestic wire transfers, the FI of the originator shall ensure that above-mentioned information is included, unless this information can be made available to the FI of the and by other means.

The FI of the originator shall not execute the transfer if it has not verified the identity of the originator. The FI of the beneficiary shall not credit the beneficiary's account or make the funds available for the beneficiary if it has not conducted verification of the beneficiary's identity.

The FI of the beneficiary is required to implement effective procedures to identify the received transfers that lack information about the originator and the beneficiary, in real-time or as part of the post-event monitoring process. This will include risk-based procedures whether transactions that lack the required information are to be executed, returned, suspended or transferred to the account of the beneficiary, as well as procedures related to the follow-up actions regarding these transfers, including to request the information on the originator and the beneficiary.

An intermediary FI ensures that all information about the originator and the beneficiary accompanied with the cross-border wire transfer is transferred to the beneficiary or other intermediary provider. Should there be technical limitations that prevent the required information accompanying a cross-border wire transfer from remaining with a

related domestic wire transfer, the intermediary FI shall keep a record of all the information received from the ordering FI or another cross-border intermediary FI.

The intermediary FI is required to implement effective risk-based procedures to identify the received transfers that lack information about the originator and the beneficiary, in real-time or as part of the post-event monitoring process.

The procedures can include defining and documenting specific AML/CFT system parameters (such as transaction value, aggregate transaction amounts at the customer level, customer risk classification, or others) which would trigger an exception to straight-through processing and require manual review and intervention. This will also include procedures for determining when to execute, reject, or suspend a wire transfer lacking required information and the appropriate follow-up action.

Where an FI repeatedly fails to provide the required information on the originator and the beneficiary, the beneficiary's or intermediary FI, taking into consideration the risks and frequency of the violations by the FI of the originator, shall take steps, which may initially include the issuing of warnings and setting deadlines. These steps can ultimately consist of rejecting any future transactions from the FI or restricting or terminating its business relationship with that FI.

Similar requirements apply to VASPs. Originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or FI (if any) immediately and securely. Beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers. For the purposes of applying the wire transfer requirements to VASPs, all virtual asset transfers are to be treated as cross-border.

In addition to the above, as part of their ongoing account monitoring procedures, FIs should also review the purpose of wire transfers, as indicated in their description fields, for potential red-flag indicators (see Section 7.2, Identification of Suspicious Transactions).

6.3.3 CDD Measures Concerning Legal Persons and Arrangements

(AML-CFT Decision Articles 8, 9, 37.1-3)

FIs are obliged to undertake CDD measures concerning legal persons and Legal Arrangements, including identification and verification of the identity of the Beneficial Owners, beneficiaries, and other controlling persons, in accordance with the provisions of the AML-CFT Decision. In fulfilling these requirements, they should take the following guidance into consideration:

- Without prejudice to the provisions of Article 9.1(b) of the AML-CFT Decision, when customers that are legal persons are owned or controlled by other legal persons or Legal Arrangements (for example, when customers are subsidiaries of a parent company or a Trust), FIs should make reasonable efforts to identify and verify the Beneficial Owners by looking through each layer of legal persons or Legal Arrangements (intermediate entities) until the natural persons with owning or controlling interests of 25% or more in aggregate are identified. Furthermore, in the event of multiple legal persons or arrangements with ownership or controlling interests, even where each legal person or Legal Arrangement owns or controls less than 25%, FIs should consider whether there are indications that the entities may be related by common ownership, which could reach or surpass the Beneficial Ownership threshold level of 25% in aggregate.

- When undertaking CDD measures on Legal Arrangements which allow funds or other forms of assets to be added or contributed to the arrangement after the initial settlement and by any persons other than the identified settlor(s), FIs should take the necessary steps to ascertain and verify the identity of the Beneficial Owners, and to understand the nature of their relationship with the Legal Arrangement. For customers that are trusts or other legal arrangements, the FI should verify the identity of beneficial owners, being the settlor, the trustee(s), the

protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership), or equivalent or similar positions for other legal arrangements. For beneficiaries of trusts or other legal arrangements that are designated by characteristics or by class, the FI should obtain sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

- The AML-CFT Decision obliges trustees in Legal Arrangements to maintain basic information relating to intermediaries, who are subject to supervision, and service providers, including consultants, investors or investment advisors, directors, accountants and tax advisors, who have responsibilities in relation to its management. In order to understand the control structure of a customer that is a Legal Arrangement, FIs should obtain this information from the trustees, representatives, or governing or managing officials and including it in the customer's CDD profile. They should also give the same consideration to other forms of Legal Arrangements and their controlling persons (such as, for example, foundations, membership clubs, religious institutions, or others, along with their founders, representatives and other governing or managing officials).

6.3.4 CDD Measures for Life Insurance Activities

(AML-CFT Decision Article 11)

For life or other investment-related insurance business, FIs should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance and other investment related insurance policies, as soon as the beneficiary(ies) are identified/designated:

(a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiary(ies) that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will) – obtaining sufficient information concerning the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout. The information collected under (a) and/or (b) should be recorded and maintained.

For both the cases referred to above, the verification of the identity of the beneficiary(ies) should occur at the time of the payout.

In determining whether enhanced CDD measures are applicable, an FI should take into account as a factor the beneficiary of a life insurance policy. If an FI determines that a beneficiary who is a legal person or a Legal Arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

In case an FI cannot comply with this, the FI should consider filing an STR with the FIU.

6.3.5 Ongoing Monitoring of the Business Relationship

(AML-CFT Decision Article 4.2(b), Article 4.3(c), 7.1)

With regard to established Business Relationships, FIs are obliged to undertake ongoing supervision of customers' activity, including monitoring of transactions executed throughout the course of the relationship to ensure that they are consistent with the information, types of activity, and the risk profiles of the customers. FIs should use a risk-based approach to determine the policies, methods, procedures and controls they implement in relation to monitoring customers' transactions and activities, as well as in regard to the extent of monitoring for specific customers or categories of customers.

As part of a risk-based approach to AML/CFT, in the case of customers or Business Relationships identified as high risk, FIs are expected to investigate and obtain more information about the purpose of transactions, and to enhance ongoing monitoring and review of transactions in order to identify potentially unusual or suspicious activities. In the case of customers or Business Relationships that are identified as low risk, FIs may consider monitoring and reviewing transactions at a reduced frequency.

Thus, in keeping with the level of risk involved, FIs should monitor and examine transactions in relation to the CDD information and risk profile of the customer (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures). Where necessary, FIs should also obtain sufficient information on the counterparties and/or other parties involved (including but not limited to information from public sources, such as internet searches), in order to determine whether the transactions appear to be:

- Normal (consideration should be given as to whether the transactions are typical for the customer, for the other parties involved, and for similar types of customers);
- Reasonable (consideration should be given as to whether the transactions have a clear rationale and are compatible with the types of activities that the customer and the counterparties are usually engaged in);
- Legitimate (consideration should be given as to whether the customer and the counterparties are permitted to engage in such transactions, such as when specific licenses, permits, or official authorisations are required).

Examples of some of the methods that may be employed for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;
- Transaction-based rules, in which the transactions of a certain type are examined;
- Location-based rules, in which the transactions involving a specific location (either as origin or destination) are examined;
- Customer-based rules, in which the transactions of particular customers are examined.

FIs may use all or any combination of the above methods, or any others that are appropriate to their particular circumstances, to effect ongoing monitoring of the Business Relationship. Furthermore, monitoring systems and methods may be automated, semi-automated, or manual, depending on the nature and size of their businesses. Whichever methods FIs elect to use, however, FIs should document them (see Section 9, Record Keeping), obtain senior management approval for them, and periodically review and update them to ensure their effectiveness. FIs should also establish specific monitoring procedures for customers and business relationships which have been reported as suspicious to the FIU (see Section 7.11, Handling of Transactions and Business Relationships after Filing of STRs).

6.3.6 Reviewing and Updating the Customer Due Diligence Information

(AML-CFT Decision Articles 4.2(b), 4.3(b), 7.2, 12)

The timely review and update of CDD information is a fundamental component of an effective ML/FT risk management and mitigation programme. FIs are obliged to maintain the CDD documents, data and information obtained on customers, and their Beneficial Owners or beneficiaries in the case of legal persons or arrangements, up to date. The AML-CFT Decision provides that FIs should update the CDD information on High Risk Customers more

frequently, and that, in the absence of a ML/FT suspicion, FIs may update the CDD information of identified low-risk customers less frequently.

In order to be able to update the CDD information of customer in a risk-based manner, FIs should develop internal policies, procedures and controls in relation to the periodic or event-driven review and updating of CDD information. These policies and procedures should be reasonable and proportionate to the risks involved, and, in formulating them, FIs are advised to consider parameters such as:

- Circumstances, timing and frequency of reviews and updates. Generally, FIs should establish clear rules per customer risk category with respect to the maximum period of time that should be allowed to elapse between CDD reviews and updates of customer records. The expiry of a customer's or Beneficial Owner's identification documents is a circumstance that call for updating the customer information. Changes in legislation or internal procedures are also a cause for reviewing and updating customer files.

- Additionally, FIs should also establish clear rules with respect to circumstances that would trigger an interim or event-driven review, or the acceleration of a particular customer's review cycle. Circumstances or events that might trigger an interim review include:

    - Discovery of information about a customer that is either contradictory or otherwise puts in doubt the appropriateness of the customer's existing risk classification or the accuracy of previously gathered CDD information;
    - Material change in ownership, legal structure, or other relevant data (such as name, registered address, purpose, capital structure) of a legal person or arrangement;
    - Initiation of legal or judicial proceedings against a customer or Beneficial Owner;
    - Finding materially adverse information about a customer or Beneficial Owner, such as media reports about allegations or investigations of fraud, corruption or other crimes;
    - Qualified opinion from an independent auditor on the financial statements of a legal entity customer;
    - Transactions that indicate potentially unusual or suspicious transactions or activities.

- Components and extent of reviews and updates. In keeping with the nature and size of their businesses, FIs should clearly define the moments, contents and extent of CDD reviews for Business Relationships in different risk categories, including which data elements, documents, or information should be examined and updated if necessary. In this regard, FIs are advised that tools such as checklists and procedural manuals will help to enhance the effectiveness of CDD reviews and updates. Examples of procedures might include, but are not necessarily limited to:

    - When the source of wealth or the source funds of a customer should be verified;
    - When additional inquiries or investigations should be made pertaining to the nature of a customer's business, the purpose of a Business Relationship, or the reasons for a transaction;
    - How much of a customer's transactional history, including how many and which specific transactions or transaction types, should be reviewed as part of a periodic or an interim review.

- Organisational responsibilities. In keeping with the nature and size of their businesses, FIs should consider clearly defining the relevant organisational arrangements in relation to the CDD review and update process. Examples of such responsibilities might include, but are not necessarily limited to:

    - Carrying out reviews and updates;
    - Escalating and/or reporting situations in which risk classifications should be changed, Business Relationships should be suspended or terminated, or potentially unusual or suspicious activities should be further investigated;
    - Approving or rejecting reviews of Business Relationships (including senior management involvement with regard to PEPs and other High Risk Customers);
    - Undertaking CDD file remediation measures when necessary;

- Auditing the quality of CDD reviews and updates;
- Maintaining records with regard to CDD reviews and updates, in accordance with statutory record-keeping requirements (see Section 9, Record Keeping).

6.4 Enhanced Due Diligence (EDD) Measures

(AML-CFT Decision Articles 4.2(b), 7.2, 15, 22, 25)

In keeping with a risk-based approach to CDD, FIs are obliged to enhance their CDD measures with regard to customers identified as high-risk, including the specific categories of customers as provided for in the relevant articles of the AML-CFT Decision, such as politically exposed persons (PEPs) (see Section 6.4.1, Requirements for Politically Exposed Persons), customers associated with high-risk countries (see Section 6.4.3, Requirements for High-Risk Countries), and correspondent relationships (see Section 6.4.4, Requirements for Correspondent Relationships).

Generally speaking, EDD involves a more rigorous application of CDD measures, including elements such as:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to customer identity;

- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds and source of wealth, and the purpose of individual transactions;

- Increased supervision of the Business Relationship, including the requirement for higher levels of management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

EDD means that FIs should intensify their measures, specifically by obtaining further evidence and supporting documentation. FIs should obtain additional information and evidence from high-risk customers such as:

  - Source of funds (revenue) and source of wealth;
  - Identifying information on individuals with control over the customer (legal person or arrangement) or account, such as signatories or guarantors;
  - Occupation or type of business;
  - Financial statements;
  - Banking references;
  - Domicile;
  - Proximity of the customer's residence, place of employment or place of business to the FI;
  - Description of the customer's primary trade area and whether international transactions are expected to be routine;
  - Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
  - Explanations for changes in account activity.

In addition, FIs should also apply specific EDD measures in case there are doubts about the accuracy or appropriateness of a customer's ML/FT risk classification in order to determine the appropriate risk classification. EDD should also be applied when there are red-flag indicators of potentially unusual or suspicious transactions or activities. In all cases in which EDD is applied, FIs should ensure that they take reasonable measures to obtain adequate, substantiated, information about the customer, commensurate with the level of the risks identified.

As part of their overall AML/CFT framework, FIs should develop risk-based internal policies, procedures and controls in connection with the application of EDD measures. Examples of the some of the factors they should consider when developing the risk-based policies include:

- the ML/FT risks identified in the ML/TF business risk assessment;
- Circumstances, timing, and composition regarding the application of EDD measures;
- Frequency of reviews and updates in relation to information on high-risk customers;
- Extent and frequency of ongoing monitoring of the Business Relationship and monitoring of transactions in relation to high-risk customers.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, FIs should consider the results of the NRA, any Topical Risk Assessment and their own ML/FT business risk assessments. Commensurate with the nature and size of the FIs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

Additional guidance regarding the application of EDD measures to statutory high-risk Business Relationship categories is provided in the following sub-sections.

6.4.1 Requirements for Politically Exposed Persons (PEPs)

(AML-CFT Decision Article 15)

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. The AML-CFT Law and the AML-CFT Decision define PEPs as:

> *"Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:*
>
> - *Direct family members (of the PEP, who are spouses, children, spouses of children, parents).*
> - *Associates known to be close to the PEP, which include:*
>   - *Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP.*
>   - *Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.*

FIs are obliged to put in place appropriate risk management systems to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP. In addition to undertaking standard CDD procedures, FIs are also required to take reasonable measures to establish the source of funds and the source of wealth of customers and Beneficial Owners identified as PEPs. In this regard, and commensurate with the nature and size of their businesses, FIs should take measures that include:

- Implementing automated screening systems which screen customer and transaction information for matches with known PEPs;

- Incorporating thorough background searches into their CDD procedures, using tools such as:

    - Manual internet search protocols;
    - Public or private databases;
    - Publicly accessible or subscription information aggregation services;
    - Commercially available background investigation services.

If a customer, Beneficial Owner, beneficiary, or controlling person is identified as a PEP, FIs are required to take reasonable measures to establish the PEP's source of funds and source of wealth. In this regard, they should also evaluate the legitimacy of the source of funds and source of wealth, including making reasonable investigations into the individual's professional and financial background.

Furthermore, FIs are also required to obtain senior management approval before establishing a Business Relationship with a PEP, or before continuing an existing one. In regard to the latter, senior management should be notified and their approval should be obtained for the continuance of a PEP relationship each time any of the following situations occur:

- An existing customer, Beneficial Owner, beneficiary, or controlling person becomes, or is newly identified as, a PEP;

- An existing PEP Business Relationship is reviewed and the CDD information is updated, either on a periodic or an interim basis, according to the organisation's internal policies and procedures;

- A material transaction that appears unusual or illogical for the PEP Business Relationship is identified;

- The beneficiary or Beneficial Owner of a life insurance policy or family *takaful* insurance policy is identified as a PEP, and in case higher risks are identified, the overall Business Relationship should also be thoroughly examined and consideration given to filing an STR. Senior management should be informed before the payout of the policy proceeds.

With regard to identified Domestic PEPs and individuals who were previously (but are no longer) entrusted with prominent functions at international organisations, the AML-CFT Decision provides that FIs should implement the measures described above when, apart from their PEP status, the Business Relationships associated with such persons could be classified as high-risk for any other reason.

The handling of a customer who is no longer entrusted with a prominent public function should be based on an assessment of risk. This risk based approach requires that FIs assess the ML/FT risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors are the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

6.4.2 EDD Measures for High-Risk Customers or Transactions

(AML-CFT Decision Article 4.2(b))

FIs are obliged to apply EDD measures to manage and mitigate the risks associated with identified High Risk Customers and/or transactions. The AML-CFT Decision defines a High Risk Customers as including those who represent a risk:

> *"…either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a customer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-*

intensive operations, or operations with an unknown third party..."

Examples of the EDD measures that should be taken by FIs are laid out in the relevant article of the AML-CFT Decision. When carrying out such measures (especially as regards obtaining and investigating more information about the nature of the customer's business, purpose of the Business Relationship, or reason for the transaction), FIs should pay particular attention to the reasonableness of the information obtained, and should evaluate it for possible inconsistencies and for potentially unusual or suspicious circumstances. Examples of factors that FIs should take into consideration in this regard include, but are not limited to:

- An illogical reason for a foreign customer's or Beneficial Owner's presence, or establishment of a Business Relationship, in the UAE;
- Consistency between the nature of the customer's business and transactions and the customer's or Beneficial Owner's professional background and employment history, in regard to which FIs may find it helpful to obtain background information from reliable and independent sources, as well as from internet and social media searches, and from the customer's or Beneficial Owner's CV;
- The level of complexity and transparency of the customer's transactions, especially in comparison with the customer's or Beneficial Owner's educational and professional background;
- The level of complexity and transparency of the customer's legal structure of legal persons or arrangements;
- The nature of any other business interests of the customer or Beneficial Owner, including any other legal persons or arrangements owned or controlled;
- Consistency between the customer's line of business and that of the counterparty to the customer's transactions (as identified, for example, through internet searches).

Additionally, and commensurate with the nature and size of their businesses, when carrying out EDD measures in respect of High Risk Customers or Beneficial Owners, FIs should take appropriate risk-mitigation measures such as, but not limited to:

- Performing background checks (among other via internet searches, public databases, or subscription information aggregation services) to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information;
- Using more rigorous methods for the verification of the customer's or Beneficial Owner's identity in regard to High Risk Customers (see Section 6.3.1, Customer and Beneficial Owner Identification/Verification for more information).

6.4.3 Requirements for High-Risk Countries

(AML-CFT Law Article 16.1(e); AML-CFT Decision Article 22, 44.7, 60)

FIs are obliged to implement EDD measures commensurate with the ML/FT risks associated with Business Relationships and transactions with customers from high-risk countries subject to a Call for Action and Jurisdictions under Increased Monitoring and the countries identified by NAMLCFTFC. In the case of legal persons and arrangements, their Beneficial Owners, beneficiaries and other controlling persons from high-risk countries.

FIs can obtain guidance on high risk countries from NAMLCFTFC, from the FATF list of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring, and from NRA report. In addition, reference can also be made to the Organisation for Economic Cooperation and Development (OECD) list of jurisdictions classified as tax havens. The Basel AML index can be a useful source to determine the risk of a country.

Examples of some of the measures FIs should apply in this regard include:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;

- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;

- Increased investigation to ascertain whether the customers or related persons (Beneficial Owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPs;

- Increased supervision of the Business Relationship, including the requirement for higher levels of internal reporting and management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information.

Additionally, FIs are obliged to implement all specific CDD measures and countermeasures regarding High Risk Countries as defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, including those related to the implementation of the decisions of the UN Security Council under Chapter VII of the Charter of the United Nations, the *International Convention for the Suppression of the Financing of Terrorism* and the *Treaty on the Non-Proliferation of Nuclear Weapons*, and other related directives, and those called for by the Financial Action Task Force (FATF) and/or other FSRBs.

In order to fulfil these obligations, and commensurate with the nature and size of their businesses and the risks involved, FIs should establish adequate internal policies, procedures and controls in relation to the application of EDD measures and risk-proportionate effective countermeasures to customers and Business Relationships associated with high-risk countries. Some of the factors to which FIs should give consideration when formulating such policies, procedures and controls, include but are not limited to the following:

- The organisation's risk appetite with respect to Business Relationships involving high-risk countries;

- Methodologies and procedures for assessing and categorising country risk, and identifying high-risk countries, including the statutorily defined High Risk Countries as established by the NAMLCFTC, and taking into consideration advice or notifications of concerns about weaknesses in the AML/CFT system of other countries issued by the relevant Supervisory Authorities and/or Competent Authorities;

- Determination and implementation of appropriate risk-based controls (for example, certain product or service restrictions, transaction limits, or others) with regard to customers and Business Relationships associated with high-risk countries;

- Organisational roles and responsibilities in relation to the monitoring, management reporting, and risk management of high-risk country Business Relationships;

- Appropriate procedures for the enhanced investigation of Business Relationships involving high-risk countries in relation to their assessment for possible PEP associations;

- Independent audit policies in respect of EDD procedures pertaining to customers/Business Relationships involving high-risk countries and the business units that deal with them.

For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply EDD, and in the most serious cases, countries are called upon to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the

country. However, specific countermeasures which need to be applied by FIs shall be advised by the corresponding supervisory authorities, the FIU or the NAMLCFTC.

6.4.4 Requirements for Correspondent Relationships

(AML-CFT Decision 25)

Financial Institutions are obliged to fulfil certain due diligence requirements with regard to the correspondent banking relationships and other similar relationships they maintain, regardless of whether these involve foreign or domestic financial institutions. Additional guidance in respect of the measures specified in the relevant article of the AML-CFT Decision is provided below. Similar relationships to which FIs should apply the guidance below include, for example those established for securities transactions or funds transfers.

FIs are prohibited from entering into or maintaining correspondent relationships with shell banks, or with institutions that allow their accounts to be used by shell banks. The AML-CFT Decision defines a shell bank as a "bank that has no physical presence in the country in which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision."

- FIs are required to collect sufficient information about any receiving correspondent institution for the purpose of identifying and achieving a full understanding of the nature of its business, and to determine, through publicly available information, its reputation and level of AML/CFT controls, including whether it has been subject to a ML/FT investigation or regulatory action.

- FIs are obliged to evaluate the AML/CFT controls applied by the receiving correspondent institution.

- FIs are required to obtain approval from senior management before establishing new correspondent relationships.

- FIs are obliged to understand the responsibilities of each institution in the field of combating the crimes of money laundering, the financing of terrorism and of illegal organisations.

Regulatory and supervisory environments governing the operation of financial institutions around the world vary greatly. Thus, not all foreign financial institutions are subject to the same AML/CFT requirements as FIs in the UAE; and as a consequence, some of these foreign institutions may pose a higher ML/FT risk. To mitigate against these risks, FIs that maintain correspondent relationships with foreign financial institutions should consider implementing adequate procedures to assess and periodically review the relevant regulatory and supervisory frameworks of the countries concerned.

Furthermore, when gathering information about financial institutions with which they maintain correspondent relationships, whether foreign or domestic, FIs should take appropriate steps to assess the nature, size and extent of their businesses in the countries where they are incorporated and licensed, as well as their ownership and management structures (taking into consideration the nature and extent of any PEP involvement), in order to evaluate whether they exhibit the characteristics of shell banks, and whether they offer downstream correspondent services (also known as "nested accounts") to other banks. If they do offer downstream correspondent services, FIs should also take reasonable steps to understand the types of services offered, the number and types of financial institutions they are offered to, the types of customers those institutions serve, and to identify the associated ML/FT risk issues.

In order to collect sufficient information about the nature of a financial institution and the AML/CFT controls it applies, and to assess the ML/FT risks associated with it, FIs should take appropriate measures such as implementing a suitable correspondent relationships questionnaire and, when necessary, conducting follow-up interviews. (FIs may find the correspondent banking questionnaire which has been developed by the Wolfsberg Group, as well as the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking, instructive in this regard. See Appendix 11.2, Useful Links.)

In addition to obtaining senior management approval prior to establishing new correspondent relationships, FIs should also periodically review and update their due diligence information in relation to the financial institutions with which they maintain correspondent relationships, commensurate with the risks involved (see 6.3.6 Reviewing and Updating the Customer Due Diligence Information). In the event of a deterioration in the risk profile of a financial institution with which a correspondent relationship is maintained, including the discovery of material adverse information concerning the institution, FIs should ensure that senior management is informed and appropriate risk-based measures are taken to assess and mitigate the ML/FT risks involved.

FIs should also maintain agreements or contracts with financial institutions with which they maintain correspondent relationships. In addition to operational details concerning the products and services covered, these agreements should clearly describe each party's responsibilities in regard to ML/FT risk mitigation, due diligence procedures, and the detailed conditions related to any permitted third-party usage of the correspondent account.

6.4.5 Requirements for Money or Value Transfer Services

(AML-CFT Decision Articles 26, 30)

As part of a risk-based AML/CFT approach, FIs that enter into or maintain Business Relationships with Money or Value Transfer Services (MVTSs) should take adequate CDD measures that are commensurate with the risks involved (see Sections 6.3, Customer Due Diligence (CDD) Measures and 6.4, Enhanced Due Diligence (EDD) Measures). Examples of measures that FIs should consider in this regard include, but are not limited to:

- Ensuring that the MVTS is properly licensed or registered; in particular, when opening any accounts for Hawala Providers, FIs licensed by the Central Bank must physically check the original Hawala Provider registration certificate issued by the Central Bank and keep a copy thereof;

- Obtaining information about and assessing the adequacy of the MVTS's AML/CFT policies, procedures and controls, including those related to Wire Transfers as stipulated in the relevant provisions of the AML-CFT Decision;

- Obtaining the MVTS's list of agents, and identifying and assessing the associated ML/FT risks, especially with regard to high-risk countries or other identified high-risk factors;

- Obtaining sufficient information about the MVTS's ownership and management structure (including taking into consideration the possibility of PEP involvement), the nature and scope of its business, the nature of its customer base, and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks.

FIs that enter into or maintain relationships with MTVSs should also use a risk-based approach to determine the appropriate internal AML/CFT policies, procedures and controls FIs implement in relation to the risk assessment, risk classification, and the type and extent of CDD they perform on the MVTSs. The policies and procedures that FIs apply should be reasonable and proportionate to the risks involved, and should be adequately documented, senior management approved, and communicated to the relevant employees of the organisation.

6.4.6 Requirements for Non-Profit Organisations

Non-Profit Organisations (NPOs) can often pose increased risks in regard to money laundering, the financing of terrorism, and the financing of illegal organisations. As part of an effective risk-based approach to AML/CFT, FIs that enter into or maintain Business Relationships with NPOs should take adequate CDD measures that are commensurate with the risks involved (see Sections 6.3, Customer Due Diligence (CDD) Measures and 6.4, Enhanced Due Diligence (EDD) Measures). Examples of measures that FIs should consider include, but are not limited to:

- Ensuring that the NPO is properly licensed or registered; in particular, when opening any accounts for Non-Profit Organisations, FIs licensed by the Central Bank must obtain an original signed letter from the Ministry of

Community Development for opening accounts to collect donations and an authorization from the UAE Red Crescent for conducting financial transfers out of the UAE through some of these accounts;

- Obtaining information about and assessing the adequacy of the NPO's AML/CFT policies, procedures and controls;

- Obtaining sufficient information about the NPO's legal, regulatory and supervisory status, including requirements relating to regulatory disclosure, accounting, financial reporting and audit (especially where community/social or religious/cultural organisations are involved, and when those organisations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason);

- Obtaining sufficient information about the NPO's ownership and management structure (including taking into consideration the possibility of PEP involvement); the nature and scope of its activities; the nature of its donor base, as well as of that of the beneficiaries of its activities and programmes; and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks;

- Performing thorough background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) on the NPO's key persons, such as senior management, branch or field managers, major donors and major beneficiaries, to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information.

FIs that enter into or maintain relationships with NPOs should also use a risk-based approach to determine the appropriate internal AML/CFT policies, procedures and controls the FIs implement in relation to the risk assessment, risk classification, and the type and extent of CDD they perform on NPOs. The policies and procedures that FIs apply should be reasonable and proportionate to the risks involved, and should be adequately documented, senior management approved, and communicated to the relevant employees of the organisation.

6.5 Simplified Due Diligence (SDD) Measures

(AML-CFT Decision Articles 4.3, 5, 10)

In keeping with a risk-based approach to CDD, under certain circumstances and in the absence of a ML/FT suspicion, FIs are only permitted to exercise simplified customer due diligence measures (SDD) with regard to customers identified as low-risk through an adequate analysis of risks.

SDD generally involves a more lenient application of certain aspects of CDD measures, including elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification;

- Fewer and less detailed inquiries in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;

- More limited supervision of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

Specifically, the AML-CFT Decision permits the application of SDD in the following circumstances:

- Identified low-risk customers. When the customer or Beneficial Owner is identified as posing a low risk of ML/FT, FIs are permitted to complete the verification of their identity after the establishment of a Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision. In this regard, FIs are required to implement appropriate and effective measures to control the risks of ML/FT, including the risks in regard to the customer or Beneficial Owner benefitting from the Business Relationship prior to the completion of the

verification process. Examples of such measures which FIs may consider taking in this regard are, among others:

- Holding funds in suspense or in escrow until the verification of the identity is completed;
- Making the completion of verification of the identity a condition precedent to the closing of a transaction.

It should be noted that the provision allowing a relaxation of the timing for the completion of the identity verification procedures does not imply that FIs are permitted to establish a Business Relationship without any customer identification at all. On the contrary, in all cases, the basic identification information in relation to the customer (whether a natural or legal person or arrangement) should be obtained; however under the specified conditions, FIs are permitted to establish the Business Relationship prior to the completion of the verification process, which may include such steps as: obtaining appropriate supporting documentation, certifications or attestations, when necessary (for example, as regards the corporate documents of a legal person); or obtaining all the necessary information related to the relevant parties of a legal person or Legal Arrangement, such as Beneficial Owners, settlors, trustees or executors, protectors, beneficiaries, or other controlling persons.

- Listed companies. FIs are exempted from identifying and verifying the identity of any shareholder, partner or Beneficial Owner of a legal person under the conditions specified in the relevant provisions of the AML-CFT Decision. Namely:

  - When the relevant information on the shareholder, partner or Beneficial Owner is obtained from reliable sources; and
  - When the customer, or the owner holding the controlling interest of the customer, is a company listed on a regulated stock exchange subject to adequate disclosure and transparency requirements related to Beneficial Ownership; or when the customer, or the owner holding the controlling interest of a legal entity customer, is the majority-held subsidiary of such a listed company.

Without prejudice to the above, in the case of foreign stock exchanges, FIs should take steps to adequately assess and document the relevant disclosure and transparency requirements related to Beneficial Ownership, and to ensure that they are at least equivalent to those of the UAE.

In addition, FIs should be aware that, regardless of the exemption mentioned above, FIs are required with respect to listed companies to verify that any person purporting to act on behalf of the customer is so authorised, and verify the identity of that person.

As part of their overall AML/CFT framework, FIs should use a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of SDD procedures. Examples of some of the factors they should consider when developing their risk-based policies include:

- the ML/FT risks identified in the ML/TF business risk assessment, especially with regard to low-risk categories of customers;

- Circumstances, timing, and composition in regard to the application of SDD measures;

- Frequency of reviews and updates in relation to customer SDD information;

- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which SDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, FIs should consider the results of both the NRA and any Topical Risk Assessment and their own ML/FT business risk assessments. Commensurate with the nature and size of the FIs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

6.6 Reliance on a Third Party

(AML-CFT Decision Articles 19)

Under certain conditions, the AML-CFT Decision permits FIs to rely on third parties to undertake the required CDD measures, including those measures specifically laid out in regard to identified high-risk countries (see Section 6.4.3, Requirements for High-Risk Countries), with the responsibility for the validity of the measures resting directly with the FIs. Among the conditions set forth in the AML-CFT Decision concerning the reliance on third parties, it is stipulated that FIs shall:

> *"Ensure that the third party is regulated and supervised, and adheres to the CDD measures towards Customers and record-keeping provisions of the present Decision."*

In order to fulfil this obligation, FIs that rely on third parties to undertake CDD measures on their behalf should implement adequate measures, in keeping with the nature and size of their businesses, to ensure the third party's adherence to the requirements of the AML-CFT Law and the AML-CFT Decision in relation to CDD measures. Examples of such measures include:

- Clearly defined procedures for determining the adequacy of a third-party's CDD and record-keeping measures, including the evaluation of such factors as the comprehensiveness and quality of its AML/CFT policies, procedures and controls; the number of personnel dedicated to CDD; and its audit and/or quality assurance policies in regard to CDD. In this regard, FIs are advised that tools such as questionnaires, scorecards, and on-site visits may be useful in evaluating the adequacy of a third party's adherence.

- Service-level agreements, clearly setting out the roles and responsibilities of the FI and the third party and specifying the nature of the CDD and record-keeping requirements to be fulfilled.

- Procedures for the certification by third parties of documents and other records pertaining to the CDD measures undertaken.

In addition to the above, when relying on foreign third parties for the undertaking of CDD measures, FIs should take steps to ensure that the AML/CFT regulatory and supervisory framework under which the third party operates is at least equivalent to that of the State. This means that FIs should ensure that the third party is regulated and supervised for AML/CFT purposes, and adheres to the equivalent CDD and record-keeping measures.

Whichever methods are utilized to ensure the adherence of third parties to the statutory CDD and record-keeping requirements, FIs should document and periodically review them for effectiveness.

Reliance on a third party refers to an FI's reliance on a third party of the entire or part of the CDD process as well as reliance on a third party when to introducing business. FIs should therefore take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay. This includes the identification and verification of the identity of customers and Beneficial Owners, beneficiaries or controlling persons of legal entities or arrangements, as well as the investigation and assembly of other relevant customer documents, information and data, as per the statutory CDD and record-keeping requirements. Nevertheless, FIs remain ultimately responsible for the outcome of the CDD process. Furthermore, FIs should themselves assess the risks of the customer, including the customer's risk profile. FIs should thus document their rationale for the assignment of relevant customer risk classifications, as well as their analysis of the CDD information obtained from the third parties. Moreover, FIs remain themselves responsible for conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.

For the purpose of this guidance, it is important to note that FIs are expected to use documents, data or information from reliable and independent sources in carrying out their CDD obligations, which include, among other things,

verifying the identity of customers and Beneficial Owners, beneficiaries or controlling persons of legal entities or arrangements.

Reliable and independent sources may include, but are not necessarily limited to, official bodies such as Competent Authorities, governmental departments or agencies, governmental or state-sponsored business registries, public utilities or similar official enterprises; as well as non-official organisations, such as publicly accessible free or subscription information aggregation services, credit reporting agencies, and others.

FIs are reminded that simply obtaining CDD documents and supporting information from reliable and independent sources during the course of performing their own CDD procedures is not necessarily considered as reliance on a third party. On occasion that FIs during the course of carrying out their own CDD procedures, receive certain documents, information or data from a third-party, FIs should obtain evidence of the third party's regulatory and supervisory status and good standing, and they should also consider obtaining the third party's certification that any CDD documents provided by them (such as identification documents, proof of address, or documents corroborating a customer's source of funds) are true copies of the originals.

Part IV—AML/CFT Administration and Reporting

7. Suspicious Transaction Reporting

(AML-CFT Law Articles 9.1, 15, 30; AML-CFT Decision Articles 16-18)

Under the AML/CFT legal and regulatory framework of the UAE, all FIs are obliged to promptly report to the Financial Intelligence Unit (FIU) suspicious transactions and any additional information required in relation to them, when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime. FIs are required to put in place and update indicators that can be used to identify possible suspicious transactions.

In order to fulfil these obligations, FIs should implement adequate internal policies, procedures and controls in relation to the identification and the immediate reporting of suspicious transactions. The following sub-sections provide additional guidance in this regard.

7.1 Role of the Financial Intelligence Unit

(AML-CFT Law Articles 9-10; AML-CFT Decision Articles 13, 16, 17.1, 21.2 and 5, 40-43, 46.1-4, 49.2-3)

The FIU of the UAE is established within the premises of the Central Bank, however, the FIU operates independently by legal and regulatory mandate as the central national agency with sole responsibility for performing the following functions:

- Receiving and analysing STRs from FIs and DNFBPs, and disseminating the results of its analysis to the Competent Authorities of the State;
- Receiving and analysing reports of suspicious cases from the Federal Customs Authority;
- Requesting additional information and documents relating to STRs, or any other data or information it deems necessary to perform its duties, from FIs, DNFBPs, and Competent Authorities, including information relating to customs disclosures;
- Cooperating and coordinating with Supervisory Authorities by disseminating the outcomes of its analysis, specifically with respect to the quality of STRs, to ensure the compliance of FIs and DNFBPs with their statutory AML/CFT obligations;

- Sending data relating to STRs and the outcomes of its analyses and other relevant data, including information obtained from foreign FIUs, to national Law Enforcement Authorities, prosecutorial authorities and judiciary authorities when actions are required by those authorities in relation to a suspected crime;

- Exchanging information with its counterparts in other countries, with respect to STRs or any other information to which it has access.

Under the aegis of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, and for the effective performance of its functions, the FIU maintains operational protocols with numerous national and international Competent Authorities.

The FIU has launched the GoAML system for the purposes of facilitating the filing of STRs by all FIs. FIs shall register themselves on the GoAML system by following the procedure manual and maintain their registration in an active status. The Compliance Officer of the company can register as the user of the system. GoAML provides a secure link of each FI to the FIU through their respective supervisory authorities. The system hosts processes for facilitating filing of STRs. It also has an .xml schema for filing batches of STRs. The guidance documents for filing of STRs are posted on the dashboard of this system. All new licensed FIs shall register themselves immediately after obtaining their financial services license so as to confirm their readiness for filing of STRs from the beginning.

The STRs are received by the FIU and processed for any required further information or documents or for further action by Law Enforcement or Supervisory Authorities. The FIU maintains a record of these STRs, performs a trend analysis to understand the prevailing trends in transactions and sectors or Institutions where possibility of ML or FT exists and this trend analysis is shared with all the registered users of GoAML through the system by means of a periodic trends and typologies report.

7.2 Processing of STRs by the FIU

(AML-CFT Law Articles 9-10; AML-CFT Decision Articles 42, 43.1-3, 49.3)

A core function of the FIU is to conduct operational analysis on STRs and information received from FIs, DNFBPs, as well as from Competent Authorities, and to support the investigations of Law Enforcement Authorities. It does so by identifying specific targets (such as persons, funds, or criminal networks) and by following the trail of specific transactions in order to determine the linkages between those targets and the possible proceeds of crime, money laundering, predicate offences and terrorist financing.

Upon the receipt of STRs or information from reporting institutions or other sources, the FIU assesses the information, prioritises the risk, and performs its own analyses using a variety of information sources and analytical techniques.

In certain cases, the FIU may request additional information from the reporting entity, Competent Authorities, or even from other FIs which also have a business relationship with the subject of its analysis or investigation, through the Integrated Enquiries Management System (IEMS). Upon concluding its analysis or investigation, the FIU may disseminate information about the case to Law Enforcement Authorities or foreign FIUs, and may, at its own discretion, also provide feedback to the reporting entity in the form of instructions regarding required actions to be taken, or recommendations and guidance.

In addition to the above, the FIU also performs strategic analysis, using data aggregated from the STRs and other information it receives, including from national and international Competent Authorities and FIUs of other countries, to identify trends and patterns relating to ML/FT. As a result of this analysis, the FIU may from time to time disseminate enhanced due diligence and fraud alerts to FIs as a preventive measure, and may also disseminate information to FIs about prevalent or new and emerging ML/FT typologies, or other specific risks which FIs should take into consideration.

7.3 Meaning of Suspicious Transaction

(AML-CFT Law Article 16; AML-CFT Decision Article 17.1)

Within the meaning of the AML-CFT Law and its implementing AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds which an FI has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing—any of the following:

- The proceeds of crime (whether designated as a misdemeanour or felony, and whether committed within the State or in another country in which it is also a crime);
- Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations;
- Being intended to be used in an activity related to such crimes.

It should be noted that the only requirement for a transaction to be considered as suspicious is "reasonable grounds" in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators, behavioural patterns, or CDD information, and it is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved. FIs do not need to have knowledge of the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; reasonable grounds are sufficient.

FIs should also note that transactions need not be completed, in progress or pending completion in order to be considered as suspicious. Attempted transactions, transactions that are not executed and past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

7.4 Identification of Suspicious Transactions

(AML-CFT Decision 16)

FIs are obliged to put in place indicators that can be used to identify suspicious transactions, and to update those indicators on an ongoing basis in accordance with the instructions of the Supervisory Authorities or the FIU, as well as in keeping with relevant developments concerning ML/FT typologies. FIs should also consider the results of the NRA, any Topical Risk Assessment and their own ML/FT business risk assessments in this regard.

As part of their overall AML/CFT framework, and commensurate with the nature and size of their businesses, FIs should determine the internal policies, procedures and controls they apply in connection with the identification, implementation, and updating of indicators, as well as with the identification and evaluation of potentially suspicious transactions. Some factors that should be considered include, but are not limited to:

- Organisational roles and responsibilities with respect to the implementation and review/updating of the relevant indicators, especially in relation to obligatory indicators required by the Supervisory Authorities or the FIU;
- Operational and IT systems procedures and controls in connection with the application of relevant indicators to processes such as transaction handling and monitoring, customer due diligence measures and review, and alert escalation;
- Staff training in relation to the identification and reporting of suspicious transactions (including attempted transactions), the appropriate use and assessment of the relevant indicators, and the degree and extent of internal investigation that is appropriate prior to the reporting of a suspicious transaction.

FIs should ensure that they have an adequate process and dedicated, experienced staff for the investigation of and dealing with alerts. The investigation of alerts and the conclusion of the investigation should be documented, including the decision to close the alert or to promptly report the transaction as suspicious.

Prompt reporting to the FIU is one of the key elements of the AML/CFT process. This means that FIs must report to the FIU the transaction immediately once the suspicious nature of the transaction becomes clear. This will be the case when from an objective point of view, taking the available information into account, there is a reason to believe that a transaction is suspicious. This means that FIs expeditiously investigate alerts and possible indications of ML/FT and immediately report the transaction upon determining that the transaction should be reported to the FIU. FIs therefore need to able to show that from the moment of the alert immediate and continuous action has been taken.

In this respect, FIs must have a procedure in place that defines the reporting process, and what steps to take in such cases. When investigating alerts it is important to examine the customer's earlier and related transactions, and to reconsider the customer's risk profile.

When identifying suspicious transactions, FIs, and their management and employees, should be aware of the facts that, in relation to ML/FT crimes, there is no minimum threshold or monetary value for reporting, and that no amount or transaction size should be considered too small for suspicion. This is of particular significance where the crimes of the financing of terrorism and of illegal organisations is concerned, since typologies related to them may often involve very small amounts of money.

Furthermore, with the exception of obligatory indicators for which reporting is required by the relevant Supervisory Authorities or the FIU, FIs should note that the presence of an *indicator* means that a transaction needs to be immediately investigated in order to determine whether the transaction needs to be reported. When determining whether a transaction is suspicious or whether there is reasonable ground for a suspicion, FIs should give consideration to the nature of the specific circumstances, including the products or services involved, and the details of the customer in the context of its risk profile. In some cases, patterns of activity or behaviour that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another. For this reason, clear internal policies and procedures with regard to alert escalation and investigation, and internal suspicious transaction reporting are critical to an effective ML/FT risk-mitigation programme. This includes an adequate training program that will allow staff to detect possible unusual or suspicious transactions.

While it is impossible to list all the indicators of suspicion in these Guidelines, some useful links to sources of AML/CFT suspicious transaction indicators are provided in Appendix 11.2, Useful Links. A few examples of potentially suspicious transaction types that FIs should take into consideration include:

- Transactions or series of transactions that appear to be unnecessarily complex, that make it difficult to identify the Beneficial Owner, or that do not appear to have an economic or commercial rationale;
- Numbers, sizes, or types of transactions that appear to be inconsistent with the customer's expected activity and/or previous activity;
- Transactions that appear to be exceptionally large in relation to a customer's declared income or turnover;
- Large unexplained cash deposits and/or withdrawals, especially when they are inconsistent with the nature of the customer's business;
- Loan repayments that appear to be inconsistent with a customer's declared income or turnover;
- Early repayment of a loan followed by an application for another loan;
- Third-party loan agreements, especially when there are amendments to or assignments of the loan agreement;
- Requests for third-party payments, including those involving transactions related to loans, investments, or insurance policies;

- Transactions involving high-risk countries, including those involving "own funds" transfers, particularly in circumstances in which there are no clear reasons for the specific transaction routing;
- Frequent or unexplained changes in ownership or management of Business Relationships;
- Illogical changes in business activities, especially where high-risk activities are involved;
- Situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide CDD documentation, or provide documentation that is false, misleading, fraudulent or forged.

When reporting an STR in the GoAML system, the user is required to select the most appropriate reason for reporting available from the menu selection provided. More than one reason may also be provided, if deemed necessary. In order to select the appropriate indicator, click 'Add' to select the appropriate reason for the report.

Select the reason(s) applicable and then press 'Close'. Alternatively, the user may search for reasons using the search bar available on the top left when expanding the form. It is imperative that a minimum of one reason for reporting must be selected to avoid rejection of the report by the GoAML system.

7.5 Requirement to Report

(AML-CFT Law Articles 9.1, 15, 24; AML-CFT Decision Articles 13.2, 17.1, 20.2)

FIs are obliged to report transactions to the FIU without delay when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime. There is no minimum reporting threshold; all suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. There is also no statute of limitations with regard to when the possible crimes or the suspicious transaction took place.

Under federal law and regulations, whether the FI operates in the mainland UAE or in a Financial or Commercial Free Zone, the designated Competent Authority for the reporting of suspicious transactions is the FIU.

Failure to – immediately - report a suspicious transaction, whether intentionally or by gross negligence, is a federal crime. Any person, including FIs or their managers and employees, who fails to perform their statutory obligation to report a suspicion of money laundering, or the financing of terrorism or of illegal organisations, is liable to a fine of no less than AED100,000 and no more than AED1,000,000 and/or imprisonment.

There are no exemptions from the statutory reporting requirement provided for FIs under the AML-CFT Law or AML-CFT Cabinet Decision.

7.6 Procedures for the Reporting of Suspicious Transactions

(AML-CFT Law Article 9; AML-CFT Decision Articles 17.1(a), 21.2)

As the designated Competent Authority for receiving and analysing STRs from all FIs, it is within the purview of the FIU to determine the procedures for the reporting of suspicious transactions. As stated in the AML-CFT Decision, FIs shall report STRs "via the electronic system of the FIU or by any other means approved by the FIU", which is the FIU's GoAML system.

Without prejudice to the above, it should be noted that the AML-CFT Decision provides for the reporting of STRs to be effected by the designated compliance officer of the FI. Specifically, the Cabinet Decision states that the duty of a compliance officer is to:

"Review, scrutinise and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality."

In this regard, as part of their overall risk-based AML/CFT framework and commensurate with the nature and size of their businesses, FIs should establish appropriate policies, procedures and controls pertaining to the internal reporting by their managers and employees of potentially suspicious transactions, including the provision of the necessary records and data, to the designated AML/CFT compliance officer for further analysis and reporting decisions, as well as to the reporting of STRs by the compliance officer to the FIU. The relevant policies, procedures and controls should take into consideration such factors as:

- Policies and procedures for the internal investigation of potentially suspicious transactions prior to the reporting of STRs;
- Conditions, timing, and methods for filing internal potentially suspicious transactions;
- Content requirements and format of internal potentially suspicious transactions;
- Appropriate controls for ensuring confidentiality and the protection of data from unauthorized access (also see Section 7.8, Confidentiality and Prohibition against "Tipping Off");
- Procedures related to the provision of additional information, follow-up actions pertaining to the transactions, and the handling of Business Relationships after the filing of STRs;
- Policies and procedures for the analysis and decision-making of suspicious transactions by the compliance officer in regard to reporting to the FIU;
- Other conditions deemed appropriate by the AML/CFT compliance officer.

Such policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation, in keeping with the nature and size of the FI's business.

7.7 Timing of Suspicious Transaction Reports (STRs)

(AML-CFT Law 9; AML-CFT Decision 17.1(a), 21.2)

FIs are obliged to report STRs to the FIU without delay. Since it is the responsibility of the designated AML/CFT compliance officer to "review, scrutinise and study records, receive data concerning suspicious transactions, and take decisions to either notify the FIU or maintain the transaction," (see Section 8.1, Compliance Officer) it follows that the STRs should be immediately reported once the suspicious nature of the transaction becomes clear. This means that the internal reporting of suspicious transactions to the compliance officer should be done directly once the suspicion or reasonable grounds for suspicion are established, and immediately the designated AML/CFT compliance officer has confirmed that the transaction (whether pending, in progress, or past) is suspicious, it should be reported.

Without prejudice to the above, FIs should note that, with the exception of any obligatory indicators for which immediate reporting to the FIU is required by the relevant Competent Authorities, some potentially suspicious transactions or indicators of suspicion may require a degree of internal investigation before a suspicion or reasonable grounds for suspicion are established and an internal STR is reported to the designated AML/CFT compliance officer. The FI should however be able to demonstrate that this investigation is started immediately and has been ongoing continuously until the transaction is reported to the FIU. In this regard, and commensurate with the nature and size of their businesses, FIs should establish clear policies, procedures and staff training programmes pertaining to the identification, investigation and internal reporting of suspicious transactions (including attempted transactions), and the degree and extent of investigations that are appropriate prior to the internal reporting of a

suspicious transaction (also see Section 7.2, Identification of Suspicious Transactions). These policies and procedures should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

7.8 Confidentiality and Prohibition against "Tipping Off"

(AML-CFT Law Article 25; AML-CFT Decision Articles 17.2, 21.2, 31.3, 39)

When reporting suspicious transactions to the FIU, FIs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, FIs, and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

FIs must ensure that all relevant information relating to STRs is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. FIs need to ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used for case management and notifications, secure information flows and guidance/training to all staff members involved. This guidance and training is primarily important for the first-line staff who have contact with customers. It is essential that these staff know when there may be cases of suspicious transactions, what questions they have to ask the customer and which information they must not under any circumstances disclose to the customer.

It should be noted that the confidentiality requirement does not pertain to communication within the FI or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/FT.

It is a federal crime for FIs or their managers, employees or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction. Any person violating this prohibition is liable to a penalty of no less than AED100,000 and no more than AED500,000 and imprisonment for a term of not less than six months.

7.9 Protection against Liability for Reporting Persons

(AML-CFT Law Article 27; AML-CFT Decision Article 17.3)

FIs, as well as their board members, employees and authorised representatives, are protected by the relevant articles of the AML-CFT Law and AML-CFT Decision from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

7.10 Handling of Transactions and Business Relationships after Filing of STRs

Once a Suspicious Transaction or other suspicious information related to a Customer or Business Relationship has been reported to the FIU, there are two immediate consequences:

- FIs are obliged to follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general.

- The Customer or Business Relationship should immediately be classified as a High Risk Customer and appropriate risk-based enhanced due diligence and ongoing monitoring procedures should be implemented in order to mitigate the associated ML/FT risks (see Sections 6.4, Enhanced Due Diligence (EDD) Measures, especially 6.4.2, EDD Measures for High-Risk Customers or Transactions, and 6.3.5 Ongoing Monitoring of the Business Relationship). It is however not required to terminated the relationship.

Further guidance on both of these topics is provided below.

FIU Instructions

After receiving an STR from an FI, the FIU may or may not revert to the reporting institution with specific instructions, requests for additional information, feedback or further guidance related to the STR or to the business relationship in general. In such cases, these communications will generally be directed to the designated AML/CFT compliance officer of the FI.

Confidentiality of FIU's Instructions

The responsibility for coordinating the FI's prompt compliance with the FIU's instructions or requests lies with the designated AML/CFT compliance officer. It should be noted that, depending on the nature of the case, the FIU may require the compliance officer to maintain certain information related to its instructions or requests privileged and/or confidential within the FI's organisation. In other words, in some cases, the compliance officer could be restricted from divulging information about a transaction or business relationship to anyone other than certain members of senior management or the board of directors of the FI. Regardless of the circumstances surrounding the FIU's instructions or requests, including whether or not the compliance officer is permitted to provide explanations to the staff of the FI, the FI is obliged at all times to follow the compliance officer's instructions in regard to any follow-up actions required in relation to an STR.

Timing of FIU's Instructions

Whether or not the FIU issues instructions or requests for additional information to a reporting institution, or how quickly this may occur after the STR is initially reported, both depend on numerous factors. These may include the prioritisation of the incoming STR among all of the STRs received by the FIU, the results of the ensuing analysis, or the possible need for information to be exchanged with other Competent Authorities or international FIUs, as well as the timing and the results of such exchanges.

When an STR involves an anticipated, pending, or already in-progress transaction, FIs should use their best efforts to delay the execution or completion of the transaction, in order to allow for a reasonable amount of time in which to receive feedback, instructions, or additional information requests from the FIU. In taking such measures, FIs should take the necessary steps to avoid "tipping off" or arousing the customer's suspicion that the transaction is being investigated or reported. Examples of some of the measures FIs may consider taking, either singly or in combination, in order to delay the execution or completion of transactions include but are not limited to:

- Delaying processing of the transaction without explanation for as long as possible;

- Advising the customer that the transaction has been delayed due to an unspecified operational, technical or other problem, and that efforts are underway to resolve it;

- Requesting additional information and/or supporting documentation (for example, evidence of relevant licences or authorisations, shipping or customs documents, additional identification documents, bank or other

references) relating to the transaction, the customer, or the counterparty;

- Advising the customer that paperwork related to the transaction has been lost and requesting that it be resubmitted;

- Advising the customer that the transaction is pending an internal approval process;

- Any other reasonable delaying tactics, bearing in mind the obligation to avoid "tipping off" the customer.

During the time interval during which an anticipated, pending, or in-progress STR that has already been reported to the FIU is being delayed by the FI, any additional suspicions that may arise should also be immediately reported to the FIU as a follow-up to the original STR. Examples of such additional suspicions may include, but are not limited to:

- New adverse information obtained in relation to the transaction, the business relationship, or the counterparty to the transaction;

- Unusual behaviour of the customer as a result of the transaction being delayed, such as but not limited to:

    - Sudden material amendments or changes to the circumstances or details of the transaction;
    - Excessive pressure, intimidation, displays of anger (beyond what would normally be expected) or threats of any kind, aimed at forcing the FI or its employees to complete the transaction;
    - Abrupt cancellation of the transaction, termination of the business relationship, or sudden attempts to close out the customer's account and/or withdraw the balance of funds or other assets held by the FI;
    - Any other indication or reasonable grounds to suspect that the customer has become aware that the transaction is being investigated or reported as suspicious.

If a reasonable amount of time has not yet elapsed before the receipt of feedback, instructions, or requests for additional information from the FIU in regard to an STR, and it becomes impossible for the FI to delay the execution or completion of the reported transaction any longer without arousing the customer's suspicion that the transaction is being investigated or reported, then the FI should request specific instructions or permission from the FIU in regard to executing or rejecting the transaction.

No Instructions, Feedback or Additional Information Requests from the FIU

Due to the factors previously mentioned, FIs may not receive instructions, additional information requests, or other feedback from the FIU in regard to STRs that have been filed; or the receipt of such communications may be delayed beyond what they consider to be a reasonable time period. In such instances, FIs should determine the appropriate handling of the STR and of the business relationship in general, taking into consideration all of the risk factors involved.

In particular, FIs are reminded that, unless they are specifically instructed by the FIU to do so, they are under no obligation to carry out transactions they suspect, or have reasonable grounds to suspect, of being related to a Crime. Furthermore, unless they are specifically instructed by the FIU to maintain the business relationship (for example, so that the Competent Authorities may monitor the customer's activity), FIs should take appropriate steps in order to decide whether or not to maintain the business relationship. These steps may include, but are not limited to:

- Reassessing the business relationship risk and re-evaluate the customer's risk profile, where necessary;

- Initiating an enhanced customer due diligence review;

- Considering the performance of an enhanced background investigation (including, if appropriate, the use of a third-party investigation service);

- Any other reasonable steps, commensurate with the nature and size of their businesses, and bearing in mind the obligation to avoid "tipping off" the customer.

FIs should be aware that filing an STR does not automatically mean that the relationship with the customer needs to be terminated. However, when deciding to terminate a business relationship for which an STR has been filed and no feedback has been received from the FIU after a reasonable time period, FIs should formally advise the FIU of their intention to do so unless there is an official objection.

Reasonable Time Period for Receiving Feedback from the FIU

FIs should note that there are no pre-established processing times, and no statute of limitations, in regard to the time interval during which the FIU may provide feedback, including instructions or requests for additional information in response to an STR. Furthermore, the time period that may be considered reasonable in relation to such feedback depends on numerous factors, including but not limited to the:

- Type, size and circumstances of the transaction;
- Normal average processing times for the specific transaction type;
- Type of customer or business relationship;
- Nature and size of the FI's business;
- Precise nature of the suspicion.

The time period considered to be reasonable could thus vary widely from one case to another.

As a general guideline, the reasonable time periods for feedback from the FIU concerning transaction types that are less complex, more routine, and have faster average processing times (such as account-to-account or wire transfers, the exchange of currencies, or over-the-counter purchases of precious metals or stones, for example) would normally be expected to be shorter than those for more complex, less routine transaction types (such as, for example, purchases of real estate or other complex assets, trade finance transactions, or various forms of loan or credit agreements). FIs that require further assistance in determining reasonable time periods should consult with the FIU or the relevant Supervisory Authorities.

High-Risk Classification of Reported Business Relationships

When a transaction or other information about a business relationship is reported to the FIU as suspicious, it means that, by definition, the customer or business relationship to which it pertains should be classified as high risk (in case the business relationship has not yet been classified as such). In situations in which no feedback or instructions have been received from the FIU, FIs that determine to maintain the business relationship should, commensurate with the nature and size of their businesses:

- Document the process by which the decision was made to maintain the business relationship, along with the rationale for, and any conditions related to, the decision;
- Implement adequate EDD measures to manage and mitigate the ML/FT risks associated with the business relationship.

In such cases, beyond the EDD measures described in previous sections (see Sections 6.4, Enhanced Due Diligence (EDD) Measures and 6.3.5, Ongoing Monitoring of the Business Relationship), FIs should also implement additional control measures such as, but not limited to:

- Requiring additional data, information or documents from the customer in order to carry out transactions (for example, evidence of relevant licenses or authorisations, customs documents, additional identification

documents, bank or other references);

- Restricting the customer's use of certain products or services;

- Placing restrictions and/or additional approval requirements on the processing of the customer's transactions (for example, transaction size and/or volume limits, or limits to the number of transactions of certain types that can be executed during a given time period).

FIs should also document the specific EDD, ongoing monitoring, and additional control measures to be taken. In this regard, FIs should obtain senior management approval for the plan, including its specific conditions, duration and any requirements for its removal, as well as the roles and responsibilities for its implementation, monitoring and reporting, commensurate with the nature and degree of the ML/FT risks associated with the business relationship.

8. Governance

(AML-CFT Law Article 16.1(d); AML-CFT Decision Articles 4.2(a), 20, 21, 44.4)

In order for the AML/CFT framework of any organisation to be effective, it must be based on the foundation of a sound governance structure, and held together by a strong compliance culture.

The governance structure should take the following into consideration:

- Establish clear accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities which may pose a greater AML/CFT risk.
- Have the mechanism to inform the board of directors (or a committee of the board) and senior management of compliance initiatives, compliance deficiencies, STRs filed and corrective actions taken;
- Develop and maintain a system of reporting that provides accurate and timely information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created and STRs filed;
- Develop and implement quality assurance testing programs to assess the effectiveness of the AML/CFT program's implementation and execution of its requirements.

FIs should also make sure to have management structures which are accountable for clear ML/FT risk management and mitigation measures, as well as appropriate independent control functions. Implicit in both the AML-CFT Law and the AML-CFT Decision are the elements of both, concerning which additional guidance is provided in the sections below.

8.1 Compliance Officer

(AML-CFT Decision Articles 20.3, 21 and 44.12)

8.1.1 Appointment and Approval

FIs are obliged to appoint a compliance officer (CO) with the appropriate competencies and experience to perform the statutory duties and responsibilities associated with this role. The AML-CFT Decision stipulates that the CO performs these duties "under his or her own responsibility", referring to the independent nature of the function and from which it should be understood that the position should be at a management level.

FIs must take all appropriate steps to identify and to prevent or manage confilicts of interests between:

- The FI, its' personnel including its CO, or any other representatives, including any person who is directly or indirectly associated with the organization and who has control to make decisions, and the FI's customer.
- The CO and senior management of the organization including the Board of Directors. The CO must be independent and must hold a position of sufficient seniority within the organization, to ensure informed

decisions are made without undue pressure to challenge decisions that are considered ill-suited, to protect the organization from possible ML/TF abuse. The MLRO's independence of judgement is required to be free from conflicts of interest, whether it is pecuniary or otherwise.

The AML-CFT Decision further provides that the appointment of a person to the position of CO requires the prior consent of the relevant Supervisory Authority. Some FIs might also have appointed a Money Laundering Reporting Officer (MLRO).

In determining the competencies, level of experience, and organizational reporting structures that are appropriate for their COs, FIs should take several factors into consideration, including but not limited to:

- The results of the NRA and any topical risk assessment
- The nature, size, complexity, and risk profile of their industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- The organisation's governance framework and management structure, with particular consideration given to the independent nature of compliance as a control function;
- The specific duties and responsibilities of the CO's role (described below).

Where appropriate, FIs may also consider engaging in dialogue with Supervisory Authorities, professional associations in their sectors, and industry peers, in relation to the competencies, experience, and governance structures that make for an effective compliance officer and an effective AML/CFT programme.

8.1.2 Responsibilities

(AML-CFT Decision Article 21.1-5)

The specific tasks of the CO are detailed in the relevant provisions of the AML-CFT Decision. In general, the CO will collaborate with the relevant Supervisory Authority and the FIU to ensure that these can perform their respective duties. The CO's tasks can be grouped broadly into the following categories:

- ML/FT Reporting. The compliance officer is FI's officer in charge of reviewing, scrutinizing and reporting STRs. In this capacity, the CO is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organisations, for reporting suspicions to the FIU, and for cooperating with the Competent Authorities in relation to the performance of their duties in regard to AML/CFT.
- AML/CFT Programme Management. The CO should ensure the quality, strength and effectiveness of the FI's AML/CFT programme. As such, the CO should be a stakeholder with respect to the FI's ML/FT business risk assessment, and the overarching AML/CFT risk mitigation framework, including its AML/CFT policies, controls and CDD measures. The CO is in charge of informing and reporting to senior management on the level of compliance and report on that to the relevant Supervisory Authority.
- AML/CFT Training and Development. The CO is responsible for helping to establish and maintain a strong and effective AML/CFT compliance culture within the FI. This duty includes working with senior management and other internal and external stakeholders to ensure that the FI's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

8.2 Staff Screening and Training

(AML-CFT Decision Articles 20.4-5, 21.4)

In order for their ML/FT risk assessment and AML/CFT mitigation measures to be effective, FIs should ensure that their employees have a clear understanding of the ML/FT risks that the FI is exposed to and can exercise sound judgment, both when adhering to the FI's AML/CFT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/FT risks, FIs should ensure that their employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks. . Depending on the nature, size and level of complexity of an FI, an FI should also screen staff to ensure high standards when hiring employees.

Thus, to ensure a high level of competence and AML/CFT programme effectiveness, FIs should formulate and implement appropriate policies, procedures and controls with regard to staff screening and training. An effective training program should not only explain the relevant AML/CFT laws and regulations, but also cover the institutions' policies and procedures used to mitigate ML/FT risks, scope of target employees such as but not limited:

- Customer-facing staff.
- AML/CFT compliance staff.
- Senior management and board of directors

These measures should be applied across organisations and financial groups, including their foreign branches and majority-owned subsidiaries. Examples of some of the factors that should be considered when determining appropriate staff screening and training measures include, but are not limited to:

- The results of the NRA and any topical risk assessment
- The nature, size, complexity, and risk profile of FIs' sectors and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- Effective screening and selection methods in relation the AML/CFT cultural compatibility of their employment candidates;
- Assessment of staff AML/CFT competency in relation to training and development needs;
- The type, frequency, structure, content, and delivery channels of AML/CFT training programmes and development opportunities;
- The effective identification, deployment and management of both internal and external training resources;
- Appropriate methods and tools for assessing the effectiveness of staff hiring, training, and development programmes, including screening procedures to ensure high standards when hiring employees.

8.3 Group Oversight

(AML-CFT Decision Articles 20, 31, 32)

When an FI is part of a group, the FI is obliged to implement appropriate group-wide AML/CFT programmes, and to apply them in relation to all branches and majority-owned subsidiaries of the financial group. The specific requirements that must be met by FIs with respect to their foreign branches and majority-owned subsidiaries are set out in the relevant provisions of the AML-CFT Decision, and reflect those to which FIs are subject within the State.

In meeting these obligations with regard to their branches and majority-owned subsidiaries in foreign countries, FIs, and in particular FIs that are members of financial groups, should ensure that the measures they apply are consistent with the requirements of the AML-CFT Law and AML-CFT Decision. In this regard, FIs should establish appropriate policies and procedures for the exchange and sharing of data and information, including those required for the

purposes of CDD and ML/FT risk management, between the foreign branches and subsidiaries and the head office, for the purpose of combating the crimes of money laundering and the financing of terrorism and of illegal organisations, and for reporting suspicious transactions.

In situations where these measures are not possible due to legislative or regulatory restrictions in the foreign countries in which their branches and majority-owned subsidiaries operate, FIs (including those which are members of Financial Groups) should implement the necessary additional measures, commensurate with the nature and size of their businesses, that will enable them to manage and mitigate appropriately the ML/FT risks that relate to their foreign operations. Examples of some of the measures that should be considered include but are not limited to:

- Assessing the effectiveness of foreign branches and majority-owned subsidiaries' AML/CFT measures, including evaluating such factors as the comprehensiveness and quality of their policies, procedures and controls, and performing gap analyses in relation to the requirements of the AML-CFT Law and AML-CFT Decision;

- Establishing clear policies, procedures and controls in relation to the type and extent of access which managers and employees of foreign branches and majority-owned subsidiaries have to the FIs' IT and operational systems, including CDD and transaction processing systems;

- Establishing clear policies, procedures and controls in relation to the type and extent of access which customers and Business Relationships of foreign branches and majority-owned subsidiaries have to the FIs' products, services and transactional processing capabilities;

- Establishing clear policies, procedures and controls in relation to the type of CDD and transaction-related information, data, and analysis FIs accept from their foreign branches and majority-owned subsidiaries in relation to customer or Business Relationship referrals, and the extent of their reliance on such information (see Section 6.6, Reliance on a Third Party);

- Implementing service-level agreements, clearly setting out the roles and responsibilities of the parties and specifying the nature of the CDD and record-keeping requirements to be fulfilled in relation to customer or Business Relationship referrals;

- Establishing protocols for the certification by the foreign branches and subsidiaries of documents and other records pertaining to the CDD measures undertaken in relation to customer or Business Relationship referrals.

In particular, in cases in which the minimum AML/CFT requirements of host countries in which FIs maintain foreign operations are less strict than those of the State, FIs should take the necessary measures to ensure that their foreign branches and/or majority-owned subsidiaries in those countries implement requirements consistent with those of the State, to the extent permitted by the laws and regulations of the host countries. If such host countries do not permit the proper implementation of the AML/CFT requirements consistent with those of the State, FIs should apply appropriate additional measures to manage and mitigate the ML/FT risks (including but not limited to those described above). They should also inform the relevant Supervisory Authorities of the circumstances and comply with any additional supervisory actions, controls, or requirements of the Competent Authorities of the State (up to and including, if requested, terminating their operations in the host countries).

8.4 Independent Audit Function

(AML-CFT Decision Article 20.6)

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. FIs are obliged to have in place an independent audit function to test the effectiveness and adequacy of their internal polices, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organisations. In this regard, FIs should ensure that

their independent audit function is appropriately staffed and organized, and that it has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/FT risks to which the FIs are exposed, and with the nature and size of their businesses.

It should be noted that, while most FIs are expected to have the capacity to meet these requirements internally, depending on the nature and size of their businesses, some FIs (particularly smaller ones) may not necessarily have the resources to maintain a fully functioning and effective internal audit unit. In such cases, those FIs should ensure that they take adequate measures to obtain the necessary capabilities from qualified external sources. They should also ensure that they have in place adequate internal capabilities to provide sufficient coordination with and oversight of any external resources they may utilise, and that such external resources are adequately regulated and supervised by relevant Competent Authorities.

FIs should ensure that the periodic inspection and testing of all aspects of their AML/CFT compliance programmes, including ML/FT business risk assessment and AML/CFT mitigation measures, and CDD policies, procedures and controls, is incorporated into their regular audit plans. They should also ensure that all their branches and the subsidiaries in which they hold a majority interest, whether domestic or foreign, are part of an independent audit testing programme that covers the effectiveness and adequacy of their internal AML/CFT polices, controls and procedures.

Some of the factors FIs should consider in determining the appropriate frequency and extent of audit testing of their AML/CFT programmes by their independent audit functions include but are not limited to:

- The results of the NRA and any topical risk assessment;
- The nature, size, complexity, and geographic scope of the FIs' businesses, and the results of their ML/TF business risk assessments;
- The risk profile associated with the products and services they offer and the markets and customer segments they serve;
- The frequency of supervision and inspection by, and the nature of the feedback (including the imposition of administrative sanctions) they receive from, Supervisory Authorities, relative to enhancing the effectiveness of their AML/CFT measures;
- Internal and external developments in relation to ML/FT risks, as well as developments pertaining to the management and operations of the FIs.

The scope of such audits should include but not be limited to:

- Examine the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity

8.5 Responsibilities of Senior Management

(AML-CFT Decision Articles 4.2(a), 4.2(b)(5), 8.1(a), 15.1(b) and 15.2, 17.3, 21.3, 25.1(d))

A cornerstone of any sound governance structure, including those related to AML/CFT compliance, is senior management involvement and accountability. The members of an FI's senior management (together with the members of the board of directors in those organisations that have one) are ultimately responsible for the quality, strength and effectiveness of the FI's AML/CFT framework, as well as for the robustness of its compliance culture. In this regard, an FI's senior management should set the ML/FT risk appetite and a proper "tone at the top," by demonstrating their commitment to ensuring an effective AML/CFT compliance programme is in place, and by clearly articulating their expectations with regard to the responsibilities and accountability of all staff members in relation to it.

Under the AML/CFT legal and regulatory framework of the UAE, the senior management of all FIs are responsible for performing certain functions related to the assessment, management and mitigation of the ML/FT risks to which their organisations are exposed. These responsibilities can be grouped broadly into categories which include:

- Implementation of governance, control, and operating systems. These include such elements as:

    - Appointing a qualified compliance officer in line with the requirements of the relevant Supervisory Authority;
    - Ensuring a robust and effective independent audit function is in place;
    - Putting in place and monitoring the implementation of adequate management and information systems, internal controls, and policies, procedures to mitigate risks.

- Approval of internal policies, procedures and controls. These include such elements as the FI's overall ML/FT risk appetite as well as the framework of AML/CFT policies, procedures and controls related to areas such as:

    - Identification, assessment, understanding, management and mitigation of ML/FT risks;
    - Performance, review and updating of CDD (including EDD and SDD) measures;
    - Identification and implementation of indictors to identify suspicious transactions;
    - Record retention and data protection;
    - Staff screening, training and development.

- Oversight of the AML/CFT compliance programme. This includes such elements as:

    - Reviewing and providing comments in relation to the compliance officer's semi-annual reports to the relevant Supervisory Authority;
    - Approving the establishment and continuance of High Risk Customer Business Relationships and their associated transactions, including those with PEPs;
    - Approving the establishment and continuance of Business Relationships involving high-risk countries;
    - Approving the establishment and continuance of relationships with correspondent institutions;
    - Ensuring the adequate application of the appropriate components of the AML/CFT compliance programme to all branches and majority-owned subsidiaries, including those operating in foreign jurisdictions.

- Application of the directives of Competent Authorities. This includes such elements as:

    - Applying the directives of Competent Authorities for implementing UN Security Council decisions under Chapter VII of the Charter of the United Nations, and other related directives, including Cabinet Decision (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions;
    - Implementing CDD measures defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, regarding High Risk Countries.

8.6 Governance Issues of Small Organisations

Some FIs may operate as small or mid-sized businesses, without large staff organisations or sophisticated IT infrastructures. In such cases, individual managers and employees may often be called upon to undertake multiple roles and responsibilities in the course of day-today business activities, and it may be difficult at times to maintain a clear separation of duties or functions. While an FI's small size does not in any way exempt it from fulfilling its obligations under the AML-CFT Law and AML-CFT Decision, and without prejudice to guidance provided in the previous sections, the following additional considerations are of particular importance to small and mid-sized FIs.

- In situations in which the responsibilities of the AML/CFT compliance officer are delegated to a manager or staff member who also has other responsibilities, FIs should undertake their best efforts to ensure that the designated AML/CFT compliance officer does not have day-to-day responsibility for sales and/or customer business relationship management.

- When an adequate separation of responsibilities is not possible due to the small size of an FI's organisation, FIs should take the necessary steps to ensure that operational and AML/CFT policies and procedures (particularly those pertaining to CDD, the identification and reporting of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and Sanctions Lists—see Sections 6, Customer Due Diligence (CDD), 6.4.3 Requirements for High-Risk Countries, and 10, International Financial Sanctions) are clearly formulated, documented, and adhered to during the establishment and ongoing monitoring of business relationships and the carrying out of transactions.

- In such cases, FIs should ensure that they clearly document the rationale for any policy and/or procedural exceptions they make, along with any additional AML/CFT risk mitigation measures they implement, and that these records are properly retained in accordance with the statutory record-keeping requirements (see Section 9, Record Keeping). FIs should also consider referring to any significant policy or procedural exceptions, along with their rationale, associated additional AML/CFT risk mitigation measures, and senior management comments, in the AML/CFT compliance officer's required semi-annual reports to the relevant Supervisory Authorities.

- FIs that are unable to ensure a clear and effective separation of AML/CFT responsibilities from those related to the day-to-day management of their businesses, including but not limited to sales and customer business relationship management functions, due to the small size of their organisation should also consider taking additional measures to enhance the application of their independent audit controls (see Section 8.4, Independent Audit Function). Examples of such measures include but are not limited to:

    - Incorporating the audit of policies, procedures (particularly those pertaining to CDD, the identification of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and Sanctions Lists), and records related to exceptions made to them, as part of their audit plans and/or their service-level agreements with their external providers of independent audit services;
    - Increasing the frequency of independent audits and random audit inspections;
    - Applying stricter criteria with regard to the review of past transactions, such as increasing the number of transactions reviewed for a given time period, reducing size threshold limits for transactions to be reviewed, or taking other reasonable measures in this regard.

9. Record Keeping

9.1 Obligations and Timeframe for the Retention and Availability of Records

(AML-CFT Law Articles 16.1(a),(f); AML-CFT Decision Articles 7.2, 24, 36, 37.3)

FIs are obliged to maintain detailed records, documents, data and statistics for all transactions, all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures, as specified in the relevant provisions of the AML-CFT Decision (see Section 9.2, Required Record Types). FIs are required to maintain the records in an organized fashion so as to permit data analysis and the tracking of financial transactions, and to make the records available to the Competent Authorities immediately upon request. They should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. All CDD information and transaction records should be available swiftly to Competent Authorities upon appropriate authority.

The statutory retention period for all records is at least five (5) years, depending on the circumstances, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account with the FI;
- Completion of an occasional transaction (in respect of a customer with whom no Business Relationship is established);
- Completion of an inspection of the records by the Supervisory Authorities;
- The issue date of a final judgment by the competent judicial authorities;
- Liquidation, dissolution, or other form of termination of a legal person or arrangement.

Without prejudice to the above, FIs should note that it is the prerogative of the Competent Authorities to require the retention of the records of any FI, whether data, statistics, or records pertaining to a specific customer or transaction or to general categories of customers or transactions which they deemed to be of interest, for a longer period of time at their own discretion.

In order to fulfil their record-keeping obligations, and commensurate with the nature and size of their businesses, FIs should determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records. The policies, procedures and controls should be documented, approved by senior management, and communicated to appropriate levels of the organisation. Examples of the factors which FIs should give consideration to when formulating the relevant policies, procedures and controls, include but are not limited to:

- Organisational roles and responsibilities in regard to the ML/TF business risk assessment, implementation, review and updating of AML/CFT policies, procedures and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures;
- Organisational roles and responsibilities in relation to record-keeping (including logging, cataloguing and organisation, archiving, handling and transferring of records and documents, as well as of the destruction of expired records) of CDD information and transactions;
- Physical and cyber security, and the protection of active and archived data and records from unauthorised access;
- Appropriate audit and quality assurance testing policies.

9.2 Required Record Types

(AML-CFT Law Articles 16.1(a),(b),(f); AML-CFT Decision Articles 7.2, 24)

The AML-CFT Law and AML-CFT Decision oblige FIs to retain several types of records, which can be classified broadly into the following categories:

- Transaction Records. This category relates to operational and statistical records, documents and information concerning all transactions executed or processed by the FI, whether domestic or international in nature.

- CDD Records. This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:

    - Customer Information, including account files and business correspondence, and results of any analysis undertaken
    - Company Information
    - Reliance on Third Parties to Undertake CDD
    - Ongoing Monitoring of Business Relationships
    - Suspicious Transaction Reports (STRs)

Additional guidance related to these record types is provided in the following sub-sections.

9.2.1 Transactions

(AML-CFT Law Articles 16.1(f); AML-CFT Decision Articles 24.1-3, 28.1-2, 29.4)

FIs are obliged to retain the operational and statistical records, documents and information concerning all transactions executed or processed by the FI, whether domestic or international in nature, and irrespective of the type of customer and whether or not a Business Relationship is maintained, for a minimum period of five (5) years. Some examples of the type of records, documents and information which must be retained include but are not limited to:

- Customer credit or debit advices, and transaction orders or applications (including those for cash deposits or withdrawals, currency exchange transactions);

- Credit-related documentation, including loan or guarantee applications, agreements, amendments and supporting documents, disbursement or repayment records, collateral pledges, letter of credit documentation, promissory notes;

- Deal tickets, trade blotters and ledgers, settlement and dividend payment records related to foreign exchange, securities dealing or investing transactions;

- Escrow or fiduciary account transaction records;

- Insurance policy premiums, pay-outs, and related transaction records and documents;

- Money transfer records, including book transfers orders, and domestic and cross-border wire transfer orders, and their related originator and beneficiary records;

- Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

In addition to the above, FIs should compile notes on any particularly large or unusual transactions, and keep these notes as part of their records. In particular, FIs licensed by the Central Bank must examine the background and purpose of all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or lawful purpose, and document their findings in writing. This includes transactions that are not considered necessary to be reported as suspicious. These findings must be maintained for inspection by the Central Bank for a period of at least five years.

9.2.2 Customer Information

(AML-CFT Law Articles 16.1(b); AML-CFT Decision Articles 24.2-4, 27.7, 28.1-2, 29.4, 37.1-3)

FIs are required to retain all customer records and documents obtained through the performance of CDD measures in relation to Business Relationships, including customers, Beneficial Owners, beneficiaries, or other controlling persons. Examples of such records include but are not limited to:

- Customer account information and files;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls);
- Copies of personal identification documents, CDD (including EDD and SDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries and investigations;
- Customer risk assessment and classification records.

9.2.3 Company Information

(AML-CFT Law Articles 16.1(b); AML-CFT Decision Articles 8.1(b), 9.1, 34-36)

The AML-CFT Decision provides that the administrators, liquidators, or any other stakeholders involved in the dissolution of a company are obliged to retain the records, documents and information specified in the relevant articles for a minimum period of five (5) years from the date of its dissolution, liquidation or termination. These records pertain to corporate documents as well as to information on Beneficial Owners, legal shareholders, and senior managers. Such records include but are not limited to documents and information concerning:

- Company formation, registration, deregistration, liquidation, dissolution or expiry, including documents such as share registers, memoranda and articles of association, deeds of settlement and foundation charters, or similar documents, along with any amendments to them (whether the organisation is for-profit or not-for-profit);
- Changes to company information, such as name, registered address, legal representatives and corporate officers (directors, company secretary), or legal form;
- Identification and identity verification documents related to Beneficial Owners, shareholders, nominee shareholders, directors and senior management officers and, in the case of Legal Arrangements, settlors or founders, protectors, beneficiaries, trustees or executors, governing council or committee members, or similar controlling persons.

In order to fulfil their statutory record-keeping obligations in this regard, FIs should determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records when they dissolve or liquidate companies in which they hold a controlling interest. The policies, procedures and controls should be documented, approved by senior management, and communicated to appropriate levels of the organisation (see Section 9.1, Obligations and Timeframe for the Retention and Availability of Records for additional

guidance concerning policies, procedures, controls and statutory retention periods related to record-keeping and data protection).

9.2.4 Reliance on Third Parties to Undertake CDD

(AML-CFT Law Article 16.1(b); AML-CFT Decision Articles 24.2-4, 19.1(b)-2(a))

FIs that rely on third parties, whether unaffiliated or members of their own financial groups, are obliged to ensure that copies of all the necessary documents collected through the performance of CDD measures can be obtained upon request and without delay, and that the third parties adhere to the record-keeping provisions of the AML-CFT Decision. See Section 9.2.2, Customer Information above for examples of such records.

In order to fulfil their statutory obligations, and commensurate with the nature and size of their businesses, FIs should determine the appropriate policies, procedures and controls related to the assessment, monitoring, and testing of third parties' record-retention frameworks. The policies, procedures and controls should be documented, approved by senior management, and communicated to appropriate levels of the organisation. Some of the factors to which FIs should give consideration when formulating relevant policies, procedures and controls include but are not limited to:

- Organisational roles and responsibilities in regard to the assessment, monitoring and testing of the third party's policies, procedures and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures;
- Organisational roles and responsibilities for the implementation of service-level agreements with third parties governing the provision of record-keeping services;
- Operational procedures related to request and transfer of records and documents, as well as their physical and cyber security, and the protection of active and archived data and records from unauthorised access;
- Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.

9.2.5 Ongoing Monitoring of Business Relationships

(AML-CFT Law Article 16.1(b),(f); AML-CFT Decision Article 24.2-4)

FIs are required to retain all customer records and documents obtained through the ongoing monitoring of Business Relationships. Examples of such records include but are not limited to:

- Transaction review, analysis, and investigation files, with their related correspondence;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to those transactions or their analysis and investigation;
- CDD records, documents, profiles or information gathered in the course of reviewing, analysing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;
- Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.

9.2.6 Suspicious Transaction Reports (STRs)

(AML-CFT Law Article 16.1(f); AML-CFT Decision Articles 24.2-4)

FIs are required to retain all records and documents pertaining to STRs and the results of all analysis or investigations performed. Such records relate to both internal STRs and those filed with the FIU, and include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
- Competent authority request for information, correspondent bank requests for assistance, and their related investigation files and correspondence;
- CDD and Business Relationship monitoring records, documents and information obtained in the course of analysing or investigating potentially suspicious transactions, and all internal or external correspondence or communication records associated with them;
- STRs (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence;
- Notes concerning feedback provided by the FIU with respect to reported STRs, as well as notes or records pertaining to any other actions taken by, or required by, the FIU.

10. International Financial Sanctions

The UAE is a member of several multinational and international organisations and governing bodies, including the United Nations. As such, the UAE is a party to many international agreements and conventions pertaining to the combating of money laundering and the financing of terrorism, as well as to the prevention and suppression of the proliferation of weapons of mass destruction. These conventions include, among others, the *International Convention for the Suppression of the Financing of Terrorism* and the *Treaty on the Non-Proliferation of Nuclear Weapons*.

FIs are obliged to comply with the directives of the Competent Authorities of the State in relation to the agreements and conventions referred to above, including but not limited to Cabinet Decision No. (74) of 2020 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions*.

Because it is outside of the scope of these Guidelines to provide detailed guidance on this, reference is made to the guidance on TFS issued by the Executive Office for the Import and Export of Goods. Due to the significance, complexity and extent of the subject matter of international financial sanctions, it is deemed appropriate that this material be covered in depth in separate guidance materials.

Part V—Appendices

11 Appendices

11.1 Glossary of Terms

Term	Definition

Beneficial Owner:	Natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement.
Beneficiary Financial Institution	The Financial Institution that receives a wire transfer from an Ordering Financial Institution directly or indirectly via an Intermediary Financial Institution and makes funds available to the beneficiary.
Business Relationship	Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them.
Committee:	National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations.
Competent Authorities:	The competent government authorities in the State entrusted with the implementation of any provision of the Decree-Law and the present Decision.
Correspondent Relationship:	Relationship between a correspondent financial institution and a respondent one through a current account or any other type of account or through a service related to such an account and includes a corresponding relationship established for the purpose of securities transactions or transfer of funds.
Crime:	Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organisations.
Customer Due Diligence (CDD):	Process of identifying or verifying the information of a Customer or Beneficial owner, whether a natural or legal person or a Legal Arrangement, and the nature of its activity and the purpose of the Business Relationship and the ownership structure and control over it for the purposes of the Decree-Law and this Decision.
Customer:	Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law (Articles 2 and 3 the Cabinet Resolution) with one of the Financial Institutions or Designated Non-Financial Businesses and Professions.
Decree-Law (or "AML-CFT Law"):	Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations.
Decision (or "AML-CFT Decision" or "Cabinet Decision"):	Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
Designated Nonfinancial Businesses and Professions (DNFBPs):	Anyone who conducts one or several of the commercial or professional activities defined in Article 3 of the Cabinet Decision, being anyone who is engaged in the following trade or business activities: 1. Brokers and real estate agents when they conclude operations for the benefit of their Customers with respect to the purchase and sale of real estate 2. Dealers in precious metals and precious stones in carrying out any single cash transaction or several transactions that appear to be interrelated or equal to more than AED 55,000. 3. Lawyers, notaries, and other independent legal professionals and independent accountants, when preparing, conducting or executing financial transactions for their Customers in respect of the following activities: (a) Purchase and sale of real estate. (b) Management of funds owned by the Customer. (c) Management of bank accounts, saving accounts or securities accounts. (d) Organising contributions for the establishment, operation or management of companies. (e) Creating, operating or managing legal persons or Legal Arrangements. (f) Selling and buying commercial entities.

	4. Providers of corporate services and trusts upon performing or executing a transaction on the behalf of their Customers in respect of the following activities: (a) Acting as an agent in the creation or establishment of legal persons. (b) Working as or equipping another person to serve as director or secretary of a company, as a partner or in a similar position in a legal person. (c) Providing a registered office, work address, residence, correspondence address or administrative address of a legal person or Legal Arrangement. (d) Performing work or equipping another person to act as a trustee for a direct Trust or to perform a similar function in favour of another form of Legal Arrangement. (e) Working or equipping another person to act as a nominal shareholder in favour of another person. 5. Other professions and activities which shall be determined by a decision of the Minister
Egmont Group:	The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/FT).
FATF:	The Financial Action Task Force is an intergovernmental body that sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.
FSRBs:	FATF-Style Regional Bodies are regional intergovernmental organisations which promote and assess the implementation of internationally accepted AML/CFT policies and regulations.
Financial Group:	A group of financial institutions that consists of holding companies or other legal persons exercising the control over the rest of the group and coordinating functions for the application of supervision on the group, branch, and subsidiary level, in accordance with the international core principles for financial supervision, and AML/CFT policies and procedures.
Financial Institution:	Anyone who conducts one or several of the financial activities or operations of /or on behalf of a Customer.
Financial Transactions or Activities:	Any activity or transaction defined in Article (2) of the Cabinet Decision.
Financing of Illegal Organisations:	Any physical or legal action aiming at providing funding to an illegal organisation, or any of its activities or members.
Financing of Terrorism:	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014 on combating terrorism offences.
FIU:	Financial Intelligence Unit.
Funds:	Assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.
High Risk Customer:	A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high

	risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority.
Illegal Organisations:	Organisations whose establishment is criminalised or which exercise a criminalised activity.
Intermediary Account:	Corresponding account used directly by a third party to conduct a transaction on its own behalf.
Intermediary Financial Institution:	The Financial Institution that receives and sends wire transfer between the Ordering Financial Institution and the Beneficiary Financial institution or another Intermediary Financial Institution.
Law Enforcement Authorities:	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidences on the crimes including AML/CFT crimes and financing illegal organisations.
Legal Arrangement:	A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as Trusts or other similar arrangements.
MENAFATF:	MENAFATF is a FATF-Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with international AML/CFT standards. The UAE is one of the founding members of MENAFATF.
Means:	Any means used or intended to be used for the commitment of an offence or felony.
Minister:	Minister of Finance
Money Laundering:	Any of the acts mentioned in Clause (1) of Article (2) of the Decree-Law.
Non-Profit Organisations (NPOs):	Any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit Legal Arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities.
Politically Exposed Persons (PEPs):	Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.
Predicate Offense:	Any act constituting an offense or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.
Proceeds:	Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
RBA:	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk.

Registrar:	Entity in charge of supervising the register of commercial names for all types of establishments registered in the State.
Sanctions Committee:	The UN Security Council Committee established as per resolution nos. 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.
Sanctions List:	A list wherein individuals and terrorist organizations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee are listed, along with their personal data and the reasons for Listing.
Settlor:	A natural or legal person who transfers the control of his funds to a Trustee under a document.
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
State:	United Arab Emirates
Supervised institutions:	Financial institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) which fall under the scope of Federal Decree-Law No. (20) of 2018 on Facing Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, and of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
Supervisory Authority:	Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and non-profit organisations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations.
Suspicious Transactions:	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanour or felony or related to the Financing of Terrorism or of illegal organisations, whether committed or attempted.
TFS:	Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.
Transaction:	Any business of either dealing, structuring, advising, drafting, appearing, arranging for funding or investing, preparing documentation or disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation.
Trust:	A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.
Trustee:	A natural or legal person who has the rights and powers conferred to him by the Settlor or the Trust, under which he administers, uses, and acts with the funds of the Settlor in accordance with the conditions imposed on him by either the Settlor or the Trust.
Wire Transfer:	Financial transaction conducted by a Financial Institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.

11.2 Useful Links

Institution	URL
Abu Dhabi Global Market	https://www.adgm.com/
Abu Dhabi Securities Exchange	http://www.adx.ae/
Basel Committee on Banking Supervision (BCBS)	http://www.bis.org/bcbs/index.htm
Central Bank of the UAE	https://www.centralbank.ae
Dubai Financial Market	http://www.dfm.ae/
Dubai Financial Services Authority (DFSA)	http://www.dfsa.ae/
Egmont Group	https://egmontgroup.org
FATF	http://www.fatf-gafi.org
Gulf Cooperation Council For The Arab States (GCC)	http://www.gcc-sg.org/
International Organisation of Securities Commissions (IOSCO)	http://www.iosco.org/
Interpol/Money Laundering	http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/default.asp
MENAFATF	http://www.menafatf.org/
Securities and Commodities Authority	http://www.sca.ae/
United Nations	http://www.un.org/
United Nations Office on Drugs & Crime – Global Programme Against Money Laundering	http://www.unodc.org/unodc/money-laundering/index.html
Wolfsberg Group	https://www.wolfsberg-principles.com/

Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting

Effective from 7/6/2021 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to assist the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

1.3. Legal Basis

(AML-CFT Law Articles 9.1, 15, 24, 25, 27; AML-CFT Decision Articles 16-18, 20.2, 21.2, 40-43)

The requirement to submit Suspicious Transaction Reports ("STRs") to the Financial Intelligence Unit ("FIU") is outlined in the (i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations and Federal Decree law No. (26) of 2021 To amend certain provisions of Federal Decree-law No. (20) of 2018, on anti-money laundering and combating the financing of terrorism and financing of illegal organisations (the "AML-CFT Law"); (ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations (the "AML-CFT Decision"); and (iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution.

Under the UAE AML-CFT legal and regulatory framework, all LFIs are obliged to promptly report to the FIU suspicious transactions and any additional information when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing, or benefitting from a crime. "Crime" is defined in Article 1 of the AML-CFT Law as "money laundering crime and related predicate offences, or financing of terrorism or illegal organisations." There is no minimum reporting threshold; all suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. LFIs are also required to put in place and update indicators that can be used to identify possible suspicious transactions.

Although the AML-CFT Law uses the term "STRs" to mean both suspicious transactions and activity, for the purposes of this Guidance document, suspicious activity involving transactions should be reported (in the first instance) to the FIU as STRs; suspicious activity that does not involve transactions, on the other hand, should be reported (in the first instance) to the FIU as Suspicious Activity Reports ("SARs"). Examples of scenarios that warrant a SAR filing include, but are not limited to: the customer is the subject of material adverse media; the customer alerts as a positive sanctions match; the prospective customer acts in a manner that is suspicious upon account opening (e.g., refusing to answer account opening questions; providing falsified or counterfeit documentation; exhibiting reluctance to provide detailed information about a business account, etc.); or the customer exhibits other suspicious behavior (e.g., inquiring about ways to circumvent certain reporting thresholds). STRs, SARs, and other report types

(referenced in greater detail in Section 3.2 ("Basic Structure of an STR or SAR")) align with the FIU's current reporting regime and utilization of the goAML system.

Under federal law and regulations, whether the LFIs operate in the mainland UAE or in a Financial or Commercial Free Zone, the designated competent authority for receiving report of suspicious transactions or activity is the FIU. The UAE's minimum statutory obligations that apply to LFIs are covered in the following requirements:

- To put in place indicators to identify suspicious transactions (AML-CFT Law Article 15, AML-CFT Decision Article 16).
- To report suspicious activity to the FIU and cooperate with relevant authorities, including to not disclose the information or data in an STR (AML-CFT Law Articles 9.1, 15, 24, 25, 27, AML-CFT Decision Articles 13.2, 17.1, 18.1, 20.2, 42.1/2).

1.3.1. Consequences for Failure to Disclose Suspicious Activity

Failure to report a suspicious transaction (STR, SAR, or other report types) without delay, whether intentionally or by gross negligence, is a federal crime in the UAE. The AML-CFT Law provides for the following sanctions against any person, including an LFI, or their managers and employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering and related predicate offences or the financing of terrorism or of illegal organisations:

- Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- Any of these two sanctions (i.e., imprisonment or fine of no less than AED100,000 and no more than AED1,000,000), according to Article 24 of the AML-CFT Law.

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a crime.

1.3.2. Protection for Individuals Disclosing Suspicious Activity

LFIs as well as their board members, employees, and authorized representatives, are protected by Article 15 of the AML-CFT Law and Article 17.3 of the AML-CFT Decision from any administrative, civil, or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. This is also the case even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. This covers cases when an employee files an STR, SAR, or other report types that its employer did not want to file.

However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

1.3.3. Meaning of Suspicious Transaction

Within the AML-CFT Law and its AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds for which an LFI has reasonable grounds to suspect as constituting—in whole or in part, and regardless of the amount or the timing - any of the following:

- The proceeds of crime (Money laundering and related predicate offenses, or financing of terrorism or illegal organisations);
- Being related to the crimes of money laundering and related predicate offences, the financing of terrorism or illegal organisations; and
- Being intended to be used in an activity related to such crimes.

The AML-CFT Law and its AML-CFT Decision define a predicate offence as "any act constituting an offense or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries."

It should be noted that the only requirement for a transaction to be considered as suspicious is "reasonable grounds" in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators; financial/transactional and behavioral patterns; Customer Due Diligence ("CDD") information; or adverse media information, and it is not dependent on obtaining evidence that a predicate offense has actually occurred or on proving the illicit source of the proceeds involved. LFIs do not need to have knowledge of the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; **reasonable grounds to suspect any such criminal activity are sufficient.**

LFIs should also note that suspicious transactions need not be completed, in progress, or pending completion. Attempted transactions, transactions that are not executed and past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

1.4. Acronyms

Terms	Description
AIF	Additional Information File without Transactions
AIFT	Additional Information File with Transactions
AML / CFT	Anti-Money Laundering / Combatting the Financing of Terrorism and Illegal Organisations
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
HRC	High Risk Country Transaction Report
HRCA	High Risk Country Activity Report
KYC	Know Your Customer
QC	Quality Control
Report	Any STR, SAR, AIF, AIFT, RFI, or RFIT based report
RFI	Request for Information without Transactions
RFIT	Request for Information with Transactions
RFR	Reason For Reporting
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report

2. Identification of Suspicious Transactions

2.1. Role of the First Line of Defens

Employees within the first line of defense (e.g., relationship managers, business executives, and backoffice operations functions) should understand the AML/CFT risks posed to the business in which they work. First line of defense employees are central to the management of customer and third-party risk and the timely escalation of potentially suspicious activity. LFIs should not rely solely on transaction monitoring systems to identify unusual and potentially suspicious activity in their customer population. First line of defense employees play a critical role in the detection and prevention of money laundering and the financing of terrorism and illegal organisations. Appropriately trained employees are in fact well-placed to identify suspicious transactions and assess that information once

deemed reasonable—collected through interactions with a customer—now appears suspicious. They should therefore be trained regarding potential risk and risk mitigation and reporting within their business area. Employees should understand the regulatory requirements within the scope of their role; red flags associated with their customers, products, services, delivery channels, and geographies; and the appropriate escalation procedure both to their management and to the second line of defense without compromising their responsibility to report suspicious transactions.

2.2. Role of the Second Line of Defense

The second line of defense (e.g., compliance employees) provides policy advice, guidance, assurance, oversight, and challenge to the first line of defense. While employees in Financial Crime Operations Units (possibly in the first line of defense) can investigate suspicious transactions and document the resultant investigation, the ultimate filing of the STR or SAR must be made by the Compliance Officer or the MLRO (in the second line of defense). To this end, the second line of defense is charged with overseeing the investigations programme comprised of both automated and manual monitoring processes. The second line of defense is also charged with monitoring risks facing the LFI, such as noncompliance with UAE laws and regulations, and reporting directly to senior management on the LFI's risk exposure, including through financial crime-related metrics. Specifically, the second line of defense and first line of defense (as applicable) should generate financial crime-related metrics (e.g., STRs or SARs filed, alert backlogs) to provide senior management with an adequate overview of the LFI's compliance program, including the timeliness and quality of the LFI's handling and resolution of transaction monitoring alerts and the STR or SAR filing process. The second line of defense should retain records of all information relating to transaction monitoring and suspicious activity reporting for a period of no less than five (5) years as provided in Article 24 of the AML-CFT Decision.

2.2.1. Role of the Compliance Officer / MLRO

According to Article 21 of the AML-CFT Decision, LFIs are required to appoint a Compliance Officer with the appropriate competencies and experience to perform the necessary tasks to:

- Detect transactions relating to any crime as defined in Article 1 of the AML-CFT Decision.
- Review, scrutinize, and study records; receive data concerning suspicious transactions; and make decisions to either notify the FIU or maintain the transaction with a documented rationale for maintaining the transaction while upholding confidentiality requirements.
- Review the internal rules and procedures relating to combating the crime and their consistency with relevant laws and regulations; assess the extent to which the LFI is committed to the application of these rules and procedures; propose what is needed to update and develop these rules and procedures; prepare and submit semi-annual reports on these points to senior management; and send a copy of that report to the relevant supervisory authority with senior management remarks and decisions.
- Prepare, execute, and document ongoing training and development programs and plans for the LFI's employees on money laundering and the financing of terrorism and financing of illegal organisations, and the means to combat them.
- Collaborate with the supervisory authority and FIU, provide them with all requested data, and allow their authorized employees to view the necessary records and documents that will allow them to perform their duties.

According to CBUAE's Guidelines, the Compliance Officer is the LFI's money laundering reporting officer ("MLRO") charged with reviewing, scrutinizing, and reporting STRs and other reports pertaining to suspicious activity. In this capacity, the Compliance Officer or MLRO is ultimately responsible for the detection of transactions related to money laundering and financing of terrorism and illegal organisations; for reporting suspicions to the FIU; implementing the appropriate actions following an STR, SAR, or other report filing (e.g., ensuring the STR or SAR subject is input into the relevant list for close monitoring or internal watchlists/blacklists; changing the customer risk rating; etc.); and for cooperating with the relevant authorities on AML/CFT matters. The Compliance Officer or MLRO is ultimately responsible to ensure that an appropriate programme exists in the LFI and that the LFI effectively deploys a risk-based approach to detect and report suspicious activity.

The Compliance Officer or MLRO should also act as the primary point of contact with law enforcement agencies for their requests and investigations. The Compliance Officer or MLRO is responsible for liaising with regulators and external bodies on financial crime issues in order to share knowledge, report cases, develop best practices, and where possible, to improve coordination within the financial sector.

2.3. Role of the Third Line of Defense

The independent testing function is responsible for evaluating the design and operational effectiveness of an LFI's compliance program controls, including technical compliance with AML/CFT policies and procedures. This function serves as a "third line of defense" to identify gaps, deficiencies, and weaknesses in operational controls owned or overseen by an LFI's business, operations, and compliance functions. Independent testing should be conducted by an internal audit department, outside auditors, consultants, and/or other qualified, independent third parties. At a minimum, employees responsible for conducting independent testing should not be involved in the function being tested or in other AML/CFT functions that could compromise their independence. Risk-based auditing assists an LFI's Board of Directors and senior management in identifying areas of weakness, prioritizing those areas for remediation, and ensuring the provision of adequate resources, oversight, and training for affected employees.

2.4. Purpose of Transaction Monitoring

The purpose of transaction monitoring is the ongoing, retrospective monitoring of customers' and prospective customers' transactions or activity to identify activity anomalous from normal behavior. This may, on further investigation, generate knowledge or reasonable suspicion of financial crime and thereby require reporting to the appropriate law enforcement and/or regulatory authority as an STR, SAR, or equivalent local report in line with AML/CFT regulatory and/or UAE FIU reporting requirements. LFIs may choose to use a combination of automated transaction monitoring scenarios and exception-based (manual) transaction reports to monitor for potentially suspicious activity. The aim of the alert review process is to identify and respond to potential indicators of money laundering, associated predicate offenses, financing of terrorism and illegal organisations , financing of proliferation, and any potentially unusual activity that does not align to a customer's or account's profile including by deploying a risk-based approach. An LFI's transaction monitoring systems and manual processes should be reviewed, assessed, and revised periodically—at least annually—and otherwise as appropriate, justified by the required circumstances. Additionally, this review should include both an evaluation of transaction monitoring system thresholds and a fine tuning of the LFI's transaction monitoring system as well as an evaluation of its effectiveness. The individuals responsible for the review should have a proper understanding of the LFI's framework-including the LFI's business and customer base—to generate a meaningful output.

2.5. Internal Organization

In order for an LFI's transaction monitoring and suspicious activity reporting program to be effective, it must be based on the foundation of a sound governance structure. Namely, an LFI's internal organization is important to appropriately identifying unusual or potentially suspicious activity. Internal organization comprises an LFI's policies, procedures, and processes designed to oversee and manage risks and to achieve compliance with UAE AML/CFT laws and regulations. In particular, an LFI's internal organization addresses the core organizational elements of an LFI's compliance program: governance and management oversight; policies and procedures; clear lines of responsibility and reporting; and ongoing training to account for changes in the UAE's legislative and regulatory frameworks.

- Governance and Management Oversight: Governance and management oversight helps to ensure that an LFI's compliance program is appropriately funded, staffed, and equipped with the requisite technology, including to identify and report suspicious activity. An LFI's Board of Directors also ensures that the compliance program has an appropriately prominent status within the organization and is operationally independent. In this capacity, senior management, inclusive of the Compliance Officer, within a compliance program should have the appropriate authority; independence; access to employees and information within

the organization; and appropriate resources to conduct their activities—including the identification and reporting of suspicious activity—effectively. The compliance program should have access to the Board of Directors or a designated board committee to raise any issues or risks; report on the status of ongoing compliance; and escalate any other pertinent AML/CFT-related information.

- As part of an LFI's risk management framework, senior management and an LFI's Board of Directors should oversee the design, implementation, and maintenance of a transaction monitoring and suspicious activity reporting program based on an LFI's AML/CFT risks and in accordance with all applicable laws and regulations. Senior management should likewise oversee a vendor selection process (as applicable) if a third-party vendor is used to acquire, install, implement, or test a transaction monitoring program or any aspect of identifying and reporting suspicious activity, among other responsibilities. The Compliance Officer (or MLRO) shall periodically update the Board of Directors (or a committee of the Board) on the overall capability framework (that includes technology and process aspects of suspicious activity identification, investigation and reporting aspects).
- Policies and Procedures: An LFI should have policies and procedures that govern changes to its transaction monitoring program which ensures that changes are defined, managed, controlled, reported, and audited. Namely, LFIs should have governance protocols surrounding the design and implementation of new detection scenarios; periodic assessment and validation of existing detection scenarios; and retiring of detection scenarios. In addition, an LFI should develop a procedure for the investigation and processing of transaction monitoring alerts in order to file an STR, SAR, or other report type promptly and qualitatively. These policies and procedures should cover the key processes for drafting and filing an STR, SAR, or other report type and other regulatory reports. More broadly, policies and procedures work to manage key AML/CFT risks and create processes for adherence across an LFI.
- Clear Lines of Responsibility and Reporting: In relation to suspicious transactions, an LFI should have clear roles, responsibilities, and reporting lines, including reporting and escalations to the Board of Directors and senior management. These roles, responsibilities, and reporting lines should be clearly documented across all three lines of defense. Clear lines of responsibility help with effectively identifying and reporting suspicious activity in a timely manner while ensuring that there is appropriate and effective oversight of employees who engage in activities which may pose greater AML/CFT risk. LFIs should also have a mechanism to inform senior management and the Board of Directors (or a committee of the Board) of compliance initiatives, compliance deficiencies, STRs or SARs (or other reports) filed, and corrective actions taken.
- Ongoing Training: Training should be provided on an ongoing basis to an LFI's employees and should include changes to the UAE's legislative and regulatory frameworks; internal policies or procedures; and understanding of evolving risk issues with respect to an LFI's transaction monitoring and suspicious activity reporting program. Training topics can include, but are not limited to, thematic analysis of STRs or SARs; regulatory requirements and best practices related to STR or SAR reporting; noteworthy STRs or SARs (or other reports) filed during the prior quarter; and controls related to emerging financial crime risks. Training should be customized to include any other internal data that would be beneficial to both the first line and second line of defense.

2.5.1. Considerations for Institutions with Foreign Branches and Subsidiaries

For LFIs operating in an international context, FATF Recommendation 18 recommends that financial groups are required to implement group-wide AML/CFT programs applicable to foreign branches and majority-owned subsidiaries. Recent major enforcement actions taken by supervisors in key jurisdictions have highlighted the need to ensure that systems and controls are aligned across a financial group and that foreign branches and majority-owned subsidiaries align AML/CFT measures with a financial group's home country requirements. As a result, LFIs have implemented global AML/CFT policies that outline a group risk appetite and are managed in each jurisdiction to align to local regulatory or legislative requirements. To support alignment of controls, LFIs operating across jurisdictions may seek to leverage the same control solutions for key processes, such as customer screening or

transaction monitoring, though there may be different rules for different jurisdictions. For example, if the LFI operates in an economy which is known to be more cash-based than another, the cash trigger rules in transaction monitoring may vary appropriately. Centralized controls with operational centers of excellence also provide a means of ensuring alignment across the group around systems and controls.

2.6. Transaction Monitoring Methods

The five key components to an effective transaction monitoring and reporting system are: (i) identification of unusual or suspicious activity; (ii) managing alerts with an alert risk scoring model; (iii) STR or SAR decision making; (iv) STR or SAR completion and filing; and (v) monitoring and STR or SAR filing on continuing activity. To effectively identify unusual or potentially suspicious activity, LFIs should first maintain a transaction monitoring program based on an underlying AML/CFT risk-based assessment. The transaction monitoring program should take into account the AML/CFT risks of the LFI's customers, prospective customers, counterparties, businesses, products, services, delivery channels, and geographic markets in addition to helping prioritize high-risk alerts. However, the sophistication of monitoring systems can differ based on an LFI's AML/CFT risks. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or a combination of these. Overall, LFIs must adopt monitoring processes and procedures to monitor customer activity that are commensurate with the size and nature of the line of business and the money laundering and the financing of terrorism and illegal organisations' risks posed by their relevant customer base. The monitoring system and/or manual processes must reasonably demonstrate that transactions that carry the highest risk of money laundering and financing of terrorism and illegal organisations are subject to enhanced scrutiny.

As part of a risk-based approach to AML/CFT, in the case of customers or Business Relationships identified as high-risk, LFIs are expected to investigate and obtain more information about the purpose of transactions, and to enhance ongoing monitoring and review of transactions in order to identify potentially unusual or suspicious activities. In the case of customers or Business Relationships that are identified as low-risk, LFIs may consider monitoring and reviewing transactions at a reduced frequency.

Examples of some of the methods that may be employed for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;
- Transaction-based rules, in which the transactions of a certain type are examined;
- Location-based rules, in which the transactions involving a specific location (either as origin or destination) are examined; and
- Customer-based rules, in which the transactions of particular customers are examined.

2.6.1. Manual Monitoring

An LFI may seek to utilize a manual transaction monitoring system, which typically targets specific categories of transactions (e.g., those involving large amounts of cash, those to or from certain geographies) and includes a manual review of various reports generated by the LFI's systems in order to identify unusual activity. The type and frequency of reviews and resulting reports used should be commensurate with the LFI's AML/CFT risk profile—including the nature, size, and complexity of its operations—and properly cover customers, counterparties, businesses, products, services, delivery channels, and geographic markets. System-generated reports typically use a certain currency threshold to detect unusual activity. An LFI's responsible senior employee should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process and periodically appraise Senior Management and where required, notify the Board of Directors (as part of periodic updates), on the appropriateness of design of manual monitoring reports. LFIs should be alert to the fact that complex and evolving financial crime risks can undermine the effectiveness of manual monitoring systems, and therefore, manual monitoring systems should also be independently reviewed for reasonable filtering criteria.

2.6.2. Automated Transaction Monitoring

Automated transaction monitoring systems can cover multiple types of transactions and use different rules to identify potentially suspicious activity. In addition, many systems can adapt over time based on historical activity, trends, or internal peer comparison. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps in coverage to address potential financial crime schemes that may not have been addressed. LFIs should also seek to have appropriate case management systems so that such funds or transactions are scrutinized in a timely manner and a determination is made as to whether the funds or transaction are suspicious.

Once established, the LFI should review and test system capabilities and thresholds on a periodic basis, commensurate to its risk profile. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured, and that the parameter or filter is appropriate for the LFI's particular risk profile, including the applicability of the detection scenarios, underlying rules, threshold values, and assumptions used. An LFI should also aim to review its transaction monitoring program at least annually to account for changes in the LFI's internal procedures; local laws and regulations; and best practices.

Relatedly, the authorization to establish or alter expected activity profiles should be clearly defined through policies and procedures. An LFI's internal controls should ensure limited access to the monitoring systems, and changes should require the approval of the Compliance Officer, MLRO, or senior management. The LFI should implement a robust end-to-end, pre- and post-implementation testing procedure of its transaction monitoring program with documentation detailing current detection scenarios and the underlying assumptions, parameters, and thresholds applied.

Employees appointed by the LFI should also be responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the transaction monitoring program, which may extend to assessing the timely review and decision-making of generated alerts and potential STR or SAR filings. Such employees should be responsible for independently validating an LFI's transaction monitoring system's programming methodology and effectiveness to ensure that the LFI's automated transaction monitoring system is effectively detecting potentially suspicious activity. These appointed employees should also ensure that customer segments, customer types, and transactions/transaction codes are mapped into the transaction monitoring system, and that the transaction monitoring system is integrated with the LFI's core banking and other relevant system. Independent validation should also take place of an LFI's policies with an aim to assess if employees are adhering to these policies. This is especially important to validate the proper use of automated tools and to ensure that the application of information technology instruments or algorithms—often leveraged by LFIs to reduce the number of false positives in their transaction monitoring programs—is not inadvertently suppressing instances of reportable suspicious activity. Where appropriate, the LFI, in lieu of maintaining full time employees to perform aforementioned functions, may hire qualified specialist consultants or external vendors to provide such review services.

2.6.3. Intelligence-led Transaction Monitoring Approach

LFIs have begun to invest in forming and developing their own intelligence units or capabilities. By establishing such units or capabilities, these units seek to maximize the use of data and information available both internally—within the LFI—and externally—across jurisdictions and businesses—in order to tackle money laundering, the financing of terrorism and illegal organisations, and fraud schemes, as well as to consolidate analytical capacity and remove any jurisdictional and business silos. This has led some LFIs to shift from a pure transaction-level monitoring approach towards adopting a "customer-level" or "network" monitoring approach. Under this approach, previous investigations can be applied to inform and refine risk models, which can then be used to customize monitoring for different business lines and customer types. These enhancements are focused on looking beyond single transactions or single customers to identify the wider network in which a customer operates—looking at the customer as an entity—enabling LFIs to manage networks of accounts and report on these networks, that in turn, increases opportunities to disrupt that network. This model moves reporting away from reports of single suspicious transactions towards suspicious entities and networks with a view on how the funds flow between them.

3. Procedures for the Reporting of Suspicious Transactions

All customers and accounts should be subject to monitoring under a risk-based approach in order to identify potentially suspicious transactions, patterns, as well as behavior that is inconsistent with past behavior on the account or with the anticipated activity on the account as determined at onboarding. Alerts on such behavior are risk relevant indicators of potentially suspicious activity. Upon identifying unusual or potentially suspicious activity, an LFI's employees must review and, as appropriate, escalate the activity for further investigation or immediate action.

Although the process for reviewing unusual or potentially suspicious activity for further investigation or immediate action is not outlined in this guidance, LFIs should establish a process to investigate such activity, including developing policies and procedures that document the process for deciding whether to close the alert or to promptly report the transaction as suspicious and should include guidance on capturing detailed descriptions for the manner in which the alerts were either disposed of by reporting or closure of the alerts. For the purposes of this guidance, best practices are discussed once activity is determined to meet one or more of the regulatory definitions of suspicious activity and when an LFI decides to report such activity to the FIU by filing an STR, SAR, or other report type.

3.1. Importance of Filing an STR and SAR

The information generated from an STR, SAR, and other report type is important for identifying and combatting financial crime. First, the quality of STRs, SARs, and other report types is imperative for increasing the FIU's analytical function to identify vulnerabilities and threats to the UAE financial system and develop an overall understanding of money laundering and the financing of terrorism and illegal organisations' risks based on emerging trends and patterns. Relatedly, STRs, SARs, and other report types also assist law enforcement in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system. Law enforcement uses the intelligence generated from STRs, SARs, and other report types to initiate and supplement money laundering or terrorist financing investigations and other criminal cases. As a result, it is critical that the information provided in all reports of suspicious activity be as accurate, timely, and complete as possible.

3.2. Basic Structure of an STR or SAR

The Compliance Officer or MLRO and other concerned employees responsible for using the goAML system must be aware of the different report types. As such, the LFI should select the correct report type when filing a report through the goAML system. The STR and SAR are the primary (or first instance) reports which must be used to report a new suspicion, whereas Additional Information File without Transactions ("AIF") and Additional Information File with Transactions ("AIFT") report types are supplementary reports which can be used to escalate additional information or transactions that correspond to a previously filed STR or SAR. When filing an AIF or AIFT, the LFI should input the Reference Number that corresponds to the STR or SAR.

- STR: If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or an occasional customer, an LFI suspects transactions are related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit an STR to the FIU within the timelines established in this guidance.
- SAR: If, during the establishment or course of the customer relationship, an LFI suspects any activity or an attempted transaction (i.e., a non-executed transaction) can be related to money laundering, related predicate offenses, or the financing of terrorism or illegal organisations, then the LFI should submit a SAR to the FIU within the timelines established in this guidance.
- Additional Information File ("AIF") without Transactions: Should the FIU require any further details while reviewing an STR or SAR, then the LFI that originally submitted the report may be solicited for further information by receiving an AIF request from the FIU through the Message Board. Should such a situation arise, the LFI is required to submit an AIF based report through the goAML platform. Please note that an AIF is a supplemental report that does not contain transactional details.

- Additional Information File with Transactions ("AIFT"): Should the FIU require any further details including transactions while processing an STR or SAR, then the LFI that originally submitted the said report may be solicited for further information including transactions by receiving an AIFT request from the FIU through the Message Board. Should such a situation arise, then the LFI is required to submit an AIFT report through the goAML. Please note that an AIFT is a supplemental report that contains transactional details.
- Request for Information ("RFI") without Transactions: Should the FIU require further information from multiple LFIs rather than just the entity responsible for submitting the STR or SAR, then an RFI request will be sent out to the concerned LFIs through the goAML Message Board. Should such a situation arise, then the LFI is required to submit an RFI report through the goAML portal.
- Request for Information with Transactions ("RFIT"): The 'RFI with Transaction(s)' report is similar to the structure of an RFI request, with the exception that this report type supports the use of transactions.
- High Risk Country Transaction Report ("HRC"): If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or a potential customer, an LFI identifies transactions related to high-risk countries as defined by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee[2], then the LFI should submit an HRC to the FIU. Such reported transaction(s) may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the transaction within the set period.
- High Risk Country Activity Report ("HRCA"): If, during the establishment or course of the customer relationship, or when conducting an activity on behalf of a customer or a potential customer, a reporting entity identifies activities related to high-risk countries as defined by the National Anti- Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee[3], then the entity should submit an HRC to the FIU. Such reported activity(ies) may only be executed three working days after reporting such to the FIU, and if the FIU does not object to conducting the activity within the set period.

When all applicable information is collected, analyzed, and documented and the LFI decides that an STR or SAR is required, the information should be described in the narrative within an investigative narrative report template in a concise and chronological format. The LFI should divide the narrative into three sections: an introduction, a body, and a conclusion. The investigative narrative report template is considered as an addition to the goAML report (due to the potential text limitation within the "goAML description of the report" field).

- Introduction

The introductory paragraph should provide:

- A brief statement addressing the purpose of the report with a general description of the known or alleged violation.
- The name(s) of the subject against whom the report is filed.
- Any linked/ previous STRs, SARs, or other reports, including the date of any STR(s) / SAR(s) filed (or other reports) previously on the suspect or related suspects and the reason why the previous STR(s) / SAR(s) (or other report) was filed.

Additional Guidance:

- Whether the activity is associated with any sanctioned countries or contained on government lists for individuals or organisations.
- A summary of the "red flags" and suspicious patterns of activity that initiated the report. (This information should be provided either in the introduction or conclusion of the narrative).

- Body

The next paragraph or paragraphs of the narrative can provide all pertinent information documenting why the STR, SAR, or other report was filed and might include:

- Details of parties facilitating the suspicious activity or transactions. If the subject is an entity, details of the subject can include the entity's trade license number, date established, line of business, licensing authority, and ownership structure.
- Involved suspected transactions (usually identified in chronological order by date and amount) [To be included only for an STR and supplementary reports involving transactions].
- The review period for the suspicious activity or transactions.
- The source of funds, destination of funds, and total of suspected amounts. This can include the transactor and beneficiary information, providing as much detail as possible, including the name and location of any involved domestic and/or international financial institution(s); names, addresses, account numbers, and any other available identifiers of originator and beneficiary transactor(s); and/or third parties or business entities on whose behalf the conductor was acting; the date(s) of the transaction(s); and amount(s).
- Explain in detail the reason for the suspicion, and why the activity or transaction is determined to be illegal or suspicious.
- Description of the method of operation (i.e., modus operandi).

Additional Guidance:

- A breakdown of larger volumes of financial activity into categories of credits and debits, and by date and amount. [To be included only for an STR and supplementary reports involving transactions].
- An explanation of any observed relationships among the transactors (e.g., shared accounts, addresses, employment, known or suspected business relationships and/or frequency of transactions occurring amongst them; appearing together at the LFI and/or counter). [To be included only for an STR and supplementary reports involving transactions].
- Specific details on cash transactions that identify the branch(es) where the transaction(s) occurred, the type of transaction(s), and how the transaction(s) occurred (e.g., night deposit, on-line banking, ATM, etc.). [To be included only for an STR and supplementary reports involving transactions].
- Any factual observations or incriminating statements made by the suspect.

- Conclusion

The final paragraph will be covered under "Action Taken by Reporting Entity" field. The final paragraph of the narrative can summarize the report and might also include:

- Any planned/initiated mitigating steps, including information about any follow-up actions conducted by the LFI (e.g., intent to close or closure of accounts, ongoing monitoring of activity, etc.).

Additional Guidance:

- Names and telephone numbers of other contacts at the LFI if different from the point of contact indicated in the report.
- A general description of any additional information related to the LFI that may be made available to law enforcement by the LFI.
- Names of any law enforcement or department/unit investigating the case who are not already identified in another section of the report.

---

[2] https://www.namlcftc.gov.ae/en/high-risk-countries.php

[3] Idem note

3.3. Best Practices for Drafting an STR or SAR

In general, a narrative should identify the five core components - who? what? when? where? and why? -of the suspicious activity being reported to the FIU. The method of operation/modus operandi (or how?) is also important and should be included in the report narrative. An LFI should ensure that the following five questions are answered prior to submitting an STR, SAR, or other report in the FIU's goAML system.

Who is conducting the suspicious activity or transaction?

- Describe the **subject of the STR, SAR, or other report,** otherwise known as the suspect(s), including the conductor, beneficiary, and accountholders involved in the transaction or activity.
- Provide **identifying information** on the parties involved in the transaction, such as the suspect's occupation and position or title within the business.
- List **beneficial owners, directors, officers, and those with signing authority,** if possible. If the transaction or activity involves an entity, include information on the ownership, control, and structure of the business.
- Provide **details about each individual or entity's** role in each of the financial transactions described. It is important to understand who is sending and receiving the funds. [To be included only for an STR and supplementary reports involving transactions].
- If more than one individual or entity is involved in the suspicious activity, **explain the relationships among the individuals or entities (if known).**

Even though information may not always be available, information should be included to the extent possible. For instance, addresses for suspects are important; filing LFIs should note not only the suspect's primary street addresses, but also, other known addresses. Any identification numbers associated with the suspect(s) such as passport and driver's license numbers are also important to document.

What instruments or mechanisms are being used to facilitate the suspicious activity or transaction(s)?

- Review the **instruments or mechanisms used in the suspicious activity** (e.g., wire transfers, foreign currency, Wages Protection System (WPS), letters of credit and other trade instruments, correspondent accounts, money orders, credit/debit cards, etc.).
- Understand the **number of different methods employed for initiating the negotiation of funds,** such as the Internet, phone access, mail, night deposit box, remote dial-up, couriers, or others.
- Describe the **source of the funds (as originator) or use of the funds (as beneficiary).** In documenting the movement of funds, **identify all account numbers at the LFI affected by the suspicious activity or transaction** and when possible, provide any account numbers held at other LFIs and the names/locations of the other LFIs involved in the reported activity.

When did the suspicious activity or transaction take place?

- If the activity takes place over a period of time, **provide the date** when the suspicious activity or transaction was first observed and describe the duration of the activity.
- To better understand the history and nature of the activity, and the flow of funds, LFIs should provide **information on each individual transaction** in a chronological order (e.g., individual dates and transaction amounts, rather than only the aggregated amount). [To be included only for an STR and supplementary reports involving transactions].
- Provide information on when **the transaction was completed or attempted.** If the transaction was not completed, the LFI should indicate this in the narrative. [To be included only for an STR and supplementary reports involving transactions].

Where did the suspicious activity or transaction take place?

- Explain if **multiple offices of a single LFI** were involved in the suspicious activity or transaction being reported. Provide the addresses of those locations.
- Specify if the **suspected activity or transaction(s) involves a foreign jurisdiction.** In this case, list the foreign jurisdiction, LFI, address, and any account numbers involved in, or affiliated with the suspected activity or

transaction(s).
- This information should include any location involved in the **full transaction chain,** including ultimate originators and beneficiaries to the extent this can be ascertained. [To be included only for an STR and supplementary reports involving transactions].

Why does the LFI think the activity or transaction is suspicious?

- Describe the **industry or business** and why **the activity or transaction is unusual** for the customer. Consider the **types of products and services involved** in the activity and the **expected activities** of similar customers.
- Assess **why the activity created a red flag** for the LFI or triggered an alert within the system.

These answers will vary based on the LFI type (for example, a depository institution versus an insurance company) and an LFI should also consider such factors as:

- The types of products and services the LFI offers;
- The types of accounts the customer has with the LFI;
- The normally expected business activity of the customer (if they are a customer of the LFI), and why this is not normal or expected activity;
- The purpose of the payment or transaction, to the extent known, reported, alleged, or questioned; and
- If the activity resulted from an automated alert, the scenario or rule that generated the alert.

How did the suspicious activity or transaction occur?

- Describe how the **transaction or pattern of transactions was committed** (i.e., the "modus operandi" or the method of operation). [To be included only for an STR and supplementary reports involving transactions].
- For example, if there appear to be multiple cheques deposited matched with outgoing wire transfers from the accounts, the narrative should include information about both the cheques and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

3.3.1. Defensive STR or SAR Filings4

Defensive filing is the practice of filing STRs or SARs on transactions or activity(ies) that LFIs do not deem truly suspicious in order to reduce the risk of regulatory penalties for non-filing of STRs or SARs.[5] Although there may be some aspect of the transaction or activity creating potential suspicion, defensive filings do not report on activity that the LFI truly considers suspicious. As such, defensive filings are generally discouraged given that such filings diminish the value of STRs and SARs, including by leading to an increase in non-valuable filings. An STR, SAR, and other report types should be of the best possible quality, including in that it should have a clearly written narrative with sufficient detail that comprehensively articulates the factors involving the reported suspicious transaction or activity. As a result, the CBUAE considers defensive STR or SARs as indicative of an inefficient transaction monitoring system and an LFI's weak system of internal controls. An LFI may be asked to correct such deficiencies as part of broader supervisory measures provided by applicable law, including administrative sanctions, temporary limitation to business activities, etc. If, for any reason, an LFI needs additional data to assess whether unusual activity is truly suspicious, the LFI should review other mechanisms—such as expanding the time period for reviewing alerted transactions (e.g., from 30 days to 90 days) or reviewing threshold-based reports—to make the determination that an STR or SAR is required.

---

[4] The UAE FIU has noted instances where SAR or STRs are reported due to the LFI not receiving supporting documents that would justify the transaction or activity. However, upon the FIU raising a request to the same LFI in the form of an AIF, supporting documents were subsequently provided for the same subjects and report. This documentation in some instances removed the suspicion of the transaction and in others, helped explain the transaction or action. Submitting reports to the FIU without first conducting a thorough investigation and looking at all available evidence creates a situation where non-suspicious transactions may be reported to the FIU. LFIs are

reminded that internal investigations into the suspicious transaction or activity should be conducted to the fullest extent possible prior to raising an STR or SAR and that related documentation, when available or easily retrievable, should be included with the STR or SAR.

[5] Egmont Group, Enterprise-wide STR Sharing: Issues and Approaches, Pg. 17

3.4. How to Submit an STR and Other Report Types

LFIs are required to submit suspicious transaction and activity reports directly to the FIU using the "goAML" portal, and registration in the system is mandatory for all entities under CBUAE's supervision. According to the Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions, the FIU has launched the goAML system for the purposes of facilitating the filing of STRs, SARs, and other report types by all LFIs. LFIs should register themselves on the goAML system by following the "GoAML Registration Guide" and maintaining their registration in an "active" status. An entity's Compliance Officer or MLRO can register as the user of the system. GoAML provides a secure link from each LFI to the FIU through their respective supervisory authorities. The system also has an .xml schema for filing batches of STRs. All newly licensed LFIs should register themselves immediately after obtaining their financial services license. Failure to register within the goAML system may result in a breach of the LFI's AML/CFT obligations and will be dealt with in accordance with the prevailing legal provisions related to non-compliance.

According to the "goAML XML Submission Guide," the goAML system reflects multiple mandatory fields, business rules, and various binding scenarios. Combined, the system only accepts reports that pass through the minimum requirements set by the FIU. Mandatory fields for submitting a report in the goAML system are noted below:

1. **Select the Report Type [4.2.1 GoAML XML Submission Guide]:** A Compliance Officer or MLRO should select a report type and populate all available details in the 'Report Cover' as depicted below:

▪ Reporting Entity ID - Entity name as per the registration (auto-generated) ▪ Internal STR/SAR # - Internal STR/SAR number ▪ Submission Date* - Date of escalating the Report to the FIU (auto-generated) ▪ Description/Summary of the Report* - Brief overview for the suspicion/reason for submitting this report to the FIU. This field is only mandatory for STR and SAR report types ▪ Reporting Entity Branch - Branch where the main subject(s) of the report were identified	▪ Report Type* - Report type relevant to the suspicion/reason for submission to the FIU ▪ FIU Reference - Only applicable in the case of AIF/RFI/ AIFT/RFIT type reports. Provide the corresponding case number as specified in the Message Board communication sent by the FIU Action Taken by Reporting Entity* - The action(s) taken by the reporting entity post- identifying the reason for suspicion/submission

2. **MLRO Details [4.2.2 GoAML XML Registration Guide]:** This section of the report includes details on the Compliance Officer, MLRO, or individual filing the report, which is automatically populated using the details provided during the registration phase.[6]
3. **Location of the Incident [4.2.3 GoAML XML Registration Guide]:** The location of the incident requires the location where the suspicious incident/transaction originated from. This is mandatory for STR and SAR report types.
4. **Reason for Reporting [4.2.4 GoAML XML Registration Guide]:** The LFI is expected to select the most appropriate reason for reporting available from the menu selection provided. If necessary, more than one reason may also be provided. It is imperative that the correct Reason for Reporting ("RFR") is chosen for STRs or SARs submitted in the goAML system.[7]
5. **Transactions [4.2.5 GoAML XML Registration Guide]:** If the reported activity involves transaction(s), the LFI should populate the following transaction details:

▪ Transaction Ref. Number* - Kindly use the auto-generate button to generate a unique identification number if the LFI is not a Bank/Exchange House	▪ Transaction Executed by (Staff Name) - Name of the staff member who executed the transaction

▪ Reporting Entity Internal Reference Number*- Reporting entity's internal transaction reference number ▪ Type of Transaction* - The mode used to conduct the transaction being reported ▪ Late Deposit - Does this transaction account as a late deposit? (Yes or No) ▪ Total Suspected Amount* (AED) - Suspected amount in AED ▪ Date* - Date when transaction was initiated ▪ Indemnified for Repatriation* - If the reporting entity has received an indemnity for repatriation	▪ Authorizer - Name of the staff member responsible for authorizing the transaction ▪ Branch executing the transaction* - Branch where the transaction was executed ▪ Date of receipt for recall request* (that field will only show if 'Yes' was selected for Indemnified for Repatriation) - The date when the reporting entity received the fund recall request ▪ Purpose of the Transaction* - Purpose for executing the transaction ▪ Transactions Comments - Comments (if any)

6. **Transaction Type, From Type / To Type, My Client / Not My Client, Foreign Currency, Conductor, [4.2.5.1-4.2.5.5 GoAML XML Registration Guide]:** Additional transaction details should be added according to the transaction type; transaction type (to/from) (i.e., my client, not my client); and foreign currency type (if applicable); and the amount. These fields should be populated by the LFI according to the GoAML XML Registration Guide's instructions. Please refer to Party Type: Person (below) to populate information on the conductor of the transaction for 4.2.5.6.
7. **Phone, Address, Identification, Email, and Employer Address and Employer Phone [4.2.5.7-4.2.5.11 GoAML XML Registration Guide]:** These fields should be populated by the LFI according to the GoAML XML Registration Guide's instructions.
8. **Party Type [4.2.5.12 GoAML XML Registration Guide]:** The Party Type' refers to the initiating source (source of funds) and beneficiary/destination party in relation to the report being filed. The initiating source and beneficiary/destination party can be either a Person, Account, or Entity.

    - **Party Type: Person [4.2.5.6, 4.2.5.13 GoAML XML Registration Guide]:** Where the subject initiating or receiving the transaction is a person, clicking the 'Person' radio button will generate the following form and fields.

▪ Title - e.g., Mr./Mrs./Dr. ▪ Prefix - Prefix Name e.g., Von, Jr. ▪ First Name* - First name of the person ▪ Middle Name - Middle name of the person ▪ Last Name* - Last name of the person ▪ Gender - Male / Female ▪ Birth Date - Date of birth of the subject person ▪ Birthplace - Location where the person was born ▪ Mother's Name - Name of the person's mother (if available) ▪ Alias - A known alias for the person (if applicable) ▪ Emirates ID - Emirates ID number; input the number without using any spaces/hyphens ▪ Nationality 1 - First nationality of the person ▪ Nationality 2 - Second nationality of the person ▪ Nationality 3 - Third nationality of the person ▪ ID Number - ID number; input the number without using any spaces/hyphens ▪ Tax Number - Tax number for outside UAE without hyphens/spaces (e.g., FATCA number for US citizens) ▪ Residence - Country of residence	▪ Occupation - Known occupation of the subject ▪ Employer Name - Name of the person's current employer ▪ PEP (Y/ N) - Specify if the person is a politically exposed person. Input "Y" or "N" accordingly ▪ Source of funds - Primary source of funds used for the reported transaction ▪ Passport* - Select if the passport details are available (Y/N) ▪ Passport Number* - Input the passport number without any spaces/hyphens only in the absence of an Emirates ID ▪ Passport Country* - Country of the passport provided ▪ Deceased - Is the person deceased? (Y/N) ▪ Date of Death - Date when the person died (applicable only if "Y" was provided in the 'Deceased' field)

- **Party Type: Account [4.2.5.14 GoAML XML Registration Guide]:** If the transaction was initiated or received through an Account, clicking the 'Account' radio button will generate the following form and fields:

▪ Account Number* - Account number without any spaces/ hyphens ▪ Status Code (is mandatory for My Client) - Account status when transaction was initiated ▪ Institution Name - Name of the institution where the account was created ▪ UBO* - Who is the beneficial owner of the account? ▪ Non-Banking Institution - Is the mentioned account held in a bank or otherwise (Y/N) ▪ Client Number - Client Number as per reporting entity's records ▪ Account Type - Drop-down menu for type of account ▪ Currency Code - Currency of the account ▪ I BAN - I BAN as per standard format (no spaces/hyphens) ▪ Opened* - Date of account opening	▪ Closed - Date of account closure ▪ Balance* (Y/N) - Input "Y" or "N" on whether there is a credit / debit in the account ▪ Balance (if the 'Yes' radio button is selected (above)) - The current balance of the account in AED ▪ Date of balance - Date when the balance was recorded

- Please note that LFIs should also add a 'Signatory(ies)' form for reports involving accounts that are classified as 'My Client.' When the accountholder is a person, the LFI is required to enter all involved signatories. If the accountholder is an entity, the LFI is required to populate the entity details. For instances where an account has multiple signatories, all of the signatory details need to be captured in the goAML system.
- **Party Type: [4.2.5.15 GoAML XML Registration Guide]:** If the transaction was initiated through an Entity, clicking the 'Entity radio button will generate the following form and fields.

▪ Name* - Legal name as per documentation ▪ Commercial Name - Commercial name as per documentation ▪ Business Activity - Business activity of entity (drop-down) ▪ Licensing Authority - Regulatory authority responsible for licensing the entity ▪ Trade License Number Authority ▪ Place of incorporation - Specify the city (Emirate in case of a UAE entity) ▪ Establishment Date - Date when entity was established ▪ Incorporation Country - Country where the entity was incorporated (drop-down) ▪ Email - Registered email for the entity (if any) ▪ Website - Website for the entity (if any) ▪ Tax Number - Tax number for outside UAE without hyphens/spaces (e.g., FATCA number for US citizens)	▪ Comments - Comments (if any) ▪ PEP (Y/ N) - Specify if the person is a politically exposed person. Input "Y" or "N" accordingly ▪ Latest date of trade license issuance/renewal - Date of trade license issuance/renewal ▪ Latest date of trade license issuance/renewal - Date of trade license issuance/renewal ▪ **Phones, Addresses, and Controlling Persons/Beneficial Owners can also be added. Addresses and Controlling Persons/Beneficial Owners section are mandatory only when the entity is classified as 'My Client.'

9. **Involved Parties [4.2.5.16 GoAML XML Registration Guide]:** If there are multiple parties involved in the reported activity, the 'Involved Parties' form should be populated with the following fields.

▪ Role* - Nature of association with the transaction ▪ Funds Code* - The type of funds ▪ Country* - Country of the involved party	▪ Funds comment - Comments on use of funds (if any) ▪ Comments - Comments (if any) ▪ **Foreign Currency can also be added

▪ Significance - Rate the significance of the concerned subject from 0 - 10 (0 being the lowest and 10 being the highest score	

10. **Good and Services [4.2.5.17 GoAML XML Registration Guide]:** This section corresponds to transactions involving the exchange of goods and services.

▪ Item Type* - The type of item (e.g., Vehicle) ▪ Description - Description of the item (e.g., Luxury Car) ▪ Manufacturer - Item maker (e.g., if the item is a car - BMW) ▪ Presently Registered To - Name of current owner ▪ Previously Registered To - Name of previous owner ▪ Status Code - Stats code (e.g., Bought, Hired) ▪ Estimated Value - Estimated value of the item ▪ Currency Code - Used to report service conducted in foreign currency	▪ Disposed Value - Effective value for property transfer (value must be in AED) ▪ Size UOM - Unit of measurement (e.g. square meters) ▪ Size - Size of the property ▪ Registration Number - Official registration number (e.g., Car VIN Number) ▪ Registration Date - Official registration date (in MM/DD/YYYY format) ▪ Identification Number - Any number that can identify the item (e.g., Car Plate Number) ▪ Comments - If applicable ▪ **Addresses can be added

11. **Activity [4.2.6 GoAML XML Registration Guide]:** If the report does not contain any transaction(s), then the activity details may be captured in the report. The activity details should include the significance of a concerned subject (scale of 0-10), the reason for reporting the party, and any comments. The 'Activity' tab will be shown only in the case the reporting entity is submitting an "SAR", "RFI without transaction(s)" or an "AIF without transaction(s)" based report file.

Upon completion of all the mandatory fields (noted above) and submission of the report in the goAML system, the report will be provided to the FIU. It is mandatory for the LFI's filer to attach **supplemental documents** to accompany the submission—including but not limited to—Know Your Customer ("KYC") documentation, copies of identification documentation, account opening forms, transaction receipts, financial statements, and other documents relevant to the investigation. In the instance that the LFI conducted due diligence or internal investigations, the corresponding documents must also be attached. This will assist the FIU in reviewing the report with all the appropriate documentation to support its review and analysis.

---

[6] The UAE FIU has noted that there have been instances of reports being received whereby upon review, the LFI's MLRO and related team members' contact details were not updated in the goAML system, which included email addresses and phone numbers. Keeping contact information updated helps with the two-way communication between LFIs and the FIU while helping to shorten the turnaround time of report analysis. It also enhances the ability of the FIU to analyze and subsequently process reports in a timely manner. The contact information should be kept updated at all times.

[7] The UAE FIU has noted that in some cases LFIs file reports while choosing RFRs that, upon closer examination, are not linked to the actual suspicions of the report. As an example, reports have been received with RFRs related to the financing of terrorism and illegal organisations with no evidence of any activity connected to the financing of terrorism and illegal organisations. Selecting incorrect RFRs hinders the FIU's analysis, and the LFI should expect multiple requests by the FIU for further clarification in these cases. LFIs should be prudent and diligent when choosing RFRs and submitting reports to the UAE FIU. RFRs should be chosen correctly and in relation to the actual suspicions of the STR or SAR being submitted.

3.5. Amendments to Submitted Reports

Once a report is submitted and accepted in the system, neither the Compliance Officer, MLRO, nor FIU employees can apply any changes and amendments to the report for missing or incorrect information. However, LFIs may be requested to file a corresponding AIF, AIFT, RFI, or RFIT, and mention in the "Description of the Report" field the reason of filing. LFIs should ensure that the filer uses the correct web reference number of the initial report. In order to avoid such incident(s) and in order to safeguard the system data integrity, LFIs should adopt a maker and checker process/concept to verify the quality and accuracy of uploaded information.

4. Timing of Alert Reviews and STR or SAR Filings

4.1. Alert Review, Case Investigation, and STR or SAR Decision Making

An efficient alert management and dispositioning process is essential to safeguarding the financial integrity of LFIs, assisting law enforcement in the identification and investigation of criminal activity, and satisfying regulatory expectations concerning timely suspicious activity reporting. The alert management and dispositioning process should be adequately staffed and free of bottlenecks and should include a process for the expedited filing of urgent reports in appropriate cases. For purposes of this guidance, "alerts" shall be understood to include automated transaction monitoring alerts, employee referrals, and law enforcement requests. The LFI should apply a risk-based approach to the alert review process by prioritizing alerts based on their risk category. For instance, alerts generated on suspicious transactions of higher-risk customers should be risk-scored higher and prioritized for review.

Alert Review: An LFI's employees should review an alert and determine whether further investigation is warranted. The underlying basis for the determination should be documented in accordance with an LFI's investigations procedures. An LFI may choose to have alert review decisions subject to Quality Control ("QC") review, prior to final dispositioning.

Where the facts available at the alert review stage are or may be sufficient to warrant an STR or SAR filing without further investigation, or where the transaction may otherwise require immediate attention (per criteria set forth below in 4.4 Activity Requiring Immediate Attention), employees should immediately escalate the alerted activity to the designated STR or SAR decision authority for expedited review.

Case Investigation: For any alerted activity determined to require further investigation, employees should conduct and complete (at least preliminarily) an investigation of the alerted activity, document the results of any research or analysis performed, and make a recommendation as to whether an STR or SAR should be filed.

Where a case investigator becomes aware of activity that requires immediate attention (per criteria set forth below in 4.4 Activity Requiring Immediate Attention), employees should immediately escalate the activity to the designated STR or SAR decision authority for expedited review.

If, in the case investigator's judgment, the facts available at the filing recommendation deadline meet one or more of the UAE regulatory definitions of suspicious activity, the case investigator should submit a recommendation to file an STR or SAR, even if certain aspects of the activity remain unexplained. Unanswered requests for information (RFIs) made in the course of a case investigation should not delay the timely submission of recommendations with respect to an STR or SAR filing. LFIs should define the reasonable RFI timeframe to allow the customer to respond to quires raised during a case investigation as part of the RFI process.

In the event of escalation for expedited review, the Compliance Officer or MLRO should review the activity and make a determination as to whether it is suspicious within 24 hours of the date of escalation. Where appropriate, the Compliance Officer or MLRO also should escalate the activity for potential exit and account closure.

4.2. STR/SAR Decision Making and Filing

In the absence of escalation for expedited review, LFIs are expected to file an STR/SAR within a maximum of 35 business days from the date of automated alert generation. The establishment of adequate grounds of suspicion may involve the investigation procedures as per the LFIs' AML and/or Financial Crime Compliance policies and procedures. LFIs are expected to complete the required investigative procedures as expeditiously as possible. LFIs must maintain adequately detailed records of investigative procedures performed against alerts and when filing an STR/SAR, must include a summary justifying the time taken to establish grounds of suspicion.

In the event of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 24 hours of the determination. All prospective STRs or SARs should be reviewed for accuracy and completeness prior to filing, in accordance with applicable procedures.

LFIs are ultimately responsible under UAE's AML-CFT Law to report suspicious activity without delay and should seek to file STRs and SARs ahead of the prescribed timeline.

4.3. Monitoring and Reporting of Continuing Suspicious Activity

Upon filing an STR/SAR pertaining to an account holder, LFIs are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against said account holder, LFIs are expected to expeditiously file an STR/SAR with the FIU.

4.4. Activity Requiring Immediate Attention

Situations requiring immediate attention include reportable violations that are ongoing (e.g., part of an ongoing money laundering scheme as indicated by an appropriate law enforcement authority) and transactions that the LFI suspects are related to the financing of terrorism and illegal organisations.

4.5. Exceptions for Complex Investigations

There may be instances when the LFI encounters potentially unusual or suspicious activity that is of a "complex" nature. The following is a non-exhaustive list of factors that should be considered to determine whether investigated activity qualifies as a complex investigation: employee-related investigations; significant investigations involving multiple customers, multiple jurisdictions, multiple accounts, multiple transactions, and/or multiple subpoena requests; and legal referred investigations.

If the LFI designates an investigation as "complex", the LFI should submit an initial STR or SAR to the FIU within 15 business days of the alert generation. The initial STR/SAR should be labelled as a "Complex investigation" to the FIU. Following the initial STR or SAR filing, the LFI has an additional 30 business days to obtain all necessary information related to the complex investigation and submit a follow-up STR or SAR to the FIU.

4.6. Summary of Review, Investigation, and Reporting Timelines

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the absence of escalation for expedited review. Please note – the following table captures the maximum timeline by which LFIs should identify and report suspicious activity and transactions. LFIs are ultimately responsible under UAE's AML-CFT Law to report suspicious activity without delay and should seek to file STRs and SARs ahead of the below timelines.

Action	Maximum Timeline in Calendar Days
Dispositioning of alert; recommendation on whether to file an STR or SAR; and decision on whether to file an STR or SAR	LFIs are expected to file an STR/SAR within a maximum of 35 business days from the date

	of automated alert generation.
Filing of a follow-up STR or SAR for a "complex investigation"	If an LFI designates an investigation as "complex", the LFI should submit an initial STR within 15 business days of alert generation – SAR/STR to be labelled "Complex investigation". Follow-up SAR/STR to be submitted within 30 business days of filing the initial STR.
Filing of STR or SAR on continuing activity	Upon filing an STR/SAR pertaining to an account holder, LFIs are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against said account holder, LFIs are expected to expeditiously file an STR/SAR continuing activity with the FIU.

4.7. Escalation for Expedited Review

In certain cases, an alert or case may need to be dispositioned and an STR or SAR filed more rapidly than usual processes allow. In such cases, the alert will be dispositioned and the STR or SAR filed according to the expedited review timeline as laid out below.

Circumstances where expedited review is expected include:

- The activity requires immediate attention (as defined above); and
- The facts available at the alert review stage are or may be sufficient to warrant an STR or SAR filing without further investigation.

The following table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the event of escalation for expedited review.

Action	Maximum Timeline in Calendar Days
Decision on whether to file an STR or SAR and filing of first STR or SAR	24 hours from decision to file
Filing of STR or SAR on continuing activity	Upon filing an STR/SAR pertaining to an account holder, LFIs are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against said account holder, LFIs are expected to expeditiously file an STR/SAR with the FIU.

5. Confidentiality and Prohibition against "Tipping Off"

According to Article 18 of the AML-CFT Decision, when reporting suspicious activity or transactions to the FIU, LFIs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure that the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, LFIs and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs, SARs, and other report types. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organization.

LFIs must ensure that all relevant information relating to STRs, SARs, and other report types is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. LFIs should ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used for case management and notifications, secure information flows and guidance/training to all employees involved. This guidance and training are particularly important for the first line of defense employees who have contact with customers. It is essential that these employees know when there may be cases of suspicious transactions, what questions they have to ask the customer and which information they must not under any circumstances disclose to the customer.

It should be noted that the confidentiality requirement **does not pertain** to communication within the LFIs or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to money laundering and the financing of terrorism and illegal organisations, according to the Article 39.1 of the AML-CFT Decision.

It is a federal crime for LFIs or their managers, employees, or representatives, to inform a customer or any other person, whether directly or indirectly, that a report has been filed or will be filed, or of any information or data contained in the report, or that an investigation is under way concerning the transaction, otherwise known as "tipping off." Any person violating this prohibition is liable to a penalty of no less than AED100,000 and no more than AED500,000 and imprisonment for a term of not less one year, according to the Article 25 of the AML-CFT Law.

6. Handling of Transactions and Business Relationships after Filing STRs or SARs

6.1. Requirements for Corresponding with the FIU

As a standard practice and as specified in Article 9.1 of the AML-CFT Law, the FIU can reach out to LFIs to provide additional requested information pertaining to an STR or SAR. Therefore, when responding to the FIU's inquiries, details should be provided in a way that is precise and outlined as per the request. LFIs should maintain clarity on the presented information and provide it in the required format (e.g., tabular format, pdf, etc.). Moreover, LFIs should avoid adding unnecessary codes and abbreviations or any raw information extracted directly from the core databases, which are unknown to the FIU. It is important to understand that the details pertaining to the source and destination of funds are essential for investigating the reported activity. Therefore, names; account numbers; country of origin and destination; currencies; dates; source and purpose of transactions; and other related information should be detailed in LFI's response. Once the report is filed, LFI should send the report web reference number and inform the FIU via the goAML Message Board.

6.2. Post STR and SAR Process

Following an STR or SAR filing, the FIU may or may not revert to the LFI with specific instructions, requests for additional information, feedback or further guidance related to the STR or SAR, or to the business relationship in general. In such cases, these communications will generally be directed to the Compliance Officer or MLRO of the LFI. However, LFIs may not receive instructions, additional information requests, or other feedback from the FIU regarding STRs or SARs that have been filed; or the receipt of such communications may be delayed beyond what they consider to be a reasonable time period. In such instances, LFIs must follow their internal policies in relation to

such customers and should determine the appropriate handling of the STR or SAR and of the business relationship in general, taking into consideration all of the risk factors involved.

Specifically, once a suspicious transaction or other suspicious information related to a customer or business relationship has been reported to the FIU, the LFI should take the following immediate responses:

- LFIs should follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general.
- LFIs should identify all related/associated accounts or relationship of STR or SAR customers and conduct a review on those accounts/relationship to check whether any suspicious transaction(s) has taken place. If yes, appropriate risk-based Enhanced Due Diligence ("EDD") and ongoing monitoring procedures should be implemented.
- The customer or business relationship, including the related/associated accounts and relationship to the STR or SAR customers, should immediately be classified as a high-risk customer and appropriate risk-based EDD and ongoing monitoring procedures should be implemented in order to mitigate the associated money laundering and the financing of terrorism and illegal organisations risks.

Unless specifically instructed by the FIU to do so, LFIs are under no obligation to carry out transactions they suspect, or have reasonable grounds to suspect, of being related to a crime. Furthermore, unless specifically instructed by the FIU to maintain the business relationship (for example, so that the competent authorities may monitor the customer's activity), it should be the LFI's responsibility to take appropriate steps in order to decide whether or not to maintain the business relationship based on their risk appetite. However, LFIs should consider the risk of tipping off a customer when taking these restrictive measures on the account. These steps may include, but are not limited to:

- Reassessing the business relationship risk and re-evaluating the customer's risk profile, where necessary.
- Initiating an enhanced customer due diligence review.
- Considering the performance of an enhanced background investigation (including, if appropriate, the use of a third-party investigation service).
- Any other reasonable steps, commensurate with the nature and size of their businesses, and bearing in mind the obligation to avoid "tipping off" the customer.

LFIs that determine to maintain the business relationship should, commensurate with the nature and size of their businesses:

- Document the process by which the decision was made to maintain the business relationship, along with the rationale for, and any conditions related to, the decision; and
- Implement adequate EDD measures to manage and mitigate the money laundering/the financing of terrorism and illegal organisations risks associated with the business relationship.

In such cases, beyond EDD measures, LFIs should also implement additional control measures such as, but not limited to:

- Requiring additional data, information or documents from the customer in order to carry out transactions (for example, evidence of relevant licenses or authorizations, customs documents, additional identification documents, bank or other references).
- Restricting the customer's use of certain products or services. Placing restrictions and/or additional approval requirements on the processing of the customer's transactions (for example, transaction size and/or volume limits, or limits to the number of transactions of certain types that can be executed during a given time period).

LFIs should also document the specific EDD, ongoing monitoring, and additional control measures to be taken. In this regard, LFIs should obtain senior management approval for the plan, including its specific conditions, duration and any requirements for its removal, as well as the roles and responsibilities for its implementation, monitoring and

reporting, commensurate with the nature and degree of the money laundering and the financing of terrorism and illegal organisations risks associated with the business relationship.

Thus, retaining a customer relationship, exiting the relationship, restricting an account, or any other actions taken by an LFI following the filing of an STR, SAR, or other report is a decision based on the LFI's internal policies and procedures, including its risk appetite, to safeguard the LFI from relevant risks. This is unless the entity receives instructions from the FIU or any other competent authority that should be immediately implemented without delay. In cases where the LFI decides to reject a new customer or to exit an existing relationship due to an STR or SAR filing (or other report), the LFI should ensure that the subject of the filing is added to internal watch lists, (e.g., a list of individuals and entities that have been exited for financial crime-related reasons and that should be screened by the LFI to avoid future on-boarding).

While individual STRs, SARs, or other reports that pose particular risk may require escalation and review for potential exit, repeated filings on a single account or group of related accounts should trigger consideration of customer exit. Repeat filings should also prompt a review of risks associated with accounts of a similar type and of whether internal controls are effectively mitigating risk. An LFI should determine a threshold for which an account that has been subject to a certain amount of STR or SAR filings (or other report) will be escalated to senior management for consideration of account closure, possible restrictions on the account, and/or enhanced monitoring.

LFIs should also maintain a customer exit policy that outlines the process for reviewing the overall customer relationship and deciding on next steps, including ending the relationship and notifying law enforcement and/or other group affiliates, as appropriate. Customer exit policies should include criteria for when these actions are appropriate and outline how the LFI should monitor the activity of a customer it decides to retain. The LFI should contact law enforcement before closing an account if the entity has knowledge of an ongoing law enforcement investigation involving that account or customer, or the LFI has filed an STR(s), SAR(s), or other report types on the customer or account due to continuing suspicious activity. LFIs should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that an LFI keep a particular account open, the LFI should ask for a written request. The written request should indicate that the agency has requested that the LFI maintain the account along with the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by an LFI in accordance with its own standards and guidelines.

6.3. Governance and Reporting to Senior Management

LFIs should have mechanisms to inform the Board of Directors (or a committee of the Board) and senior management of compliance initiatives, compliance deficiencies, STRs, SARs, or other regulatory reports filed, and corrective actions taken. LFIs should also develop and maintain a system of reporting that provides accurate and timely information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created, and STRs, SARs, or other report types filed.

Employees should report the number and types of STRs, SARs, or other regulatory reports filed to the Board of Directors or a Board-designated committee. While employees are not required to provide actual copies of STRs, SARs, or other regulatory reports to the Board (or a committee of the Board), such notifications should contain sufficient information to enable the Board or its committee to provide appropriate oversight over the LFI's AML/CFT program. Where an individual filing documents activity that poses a particular risk, management may provide a copy of the report to the Board or Board-designated committee. Where appropriate, the suspicious activity or transaction underlying the filing of an STR, SAR, or other regulatory reports should be communicated to those individuals responsible for managing the risk associated with the customer and/or activity that is the subject of the STR, SAR, or other regulatory reports in order to permit such employees to respond appropriately to the AML/CFT risks identified. Although all such communications are subject to the confidentiality restrictions, it should be noted that the confidentiality requirement does not pertain to communication within the LFIs or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention, or reporting of suspicious transactions and/or crimes related to money laundering and the

financing of terrorism and illegal organisations, according to Article 39.1 of the AML-CFT Decision (also referenced in Section 5. Confidentiality and Prohibition against "Tipping Off").

6.4. Record Retention

According to Article 24 of the AML-CFT Decision, LFIs are required to retain all records and documents pertaining to STRs and the results of all analysis or investigations performed for at least five (5) years from the date of completion of the transaction or termination of the business relationship. Such records relate to both internal STRs and those filed with the FIU, and should include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
- Competent authority request for information, correspondent bank requests for assistance, and their related investigation files and correspondence;
- CDD and Business Relationship monitoring records, documents, and information obtained in the course of analyzing or investigating potentially suspicious transactions, requests for assistance by LFIs, and all internal or external correspondence or communication records associated with them;
- STRs, SARs, and other report types (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence; and
- Notes concerning feedback provided by the FIU with respect to reported STRs, SARs, and other report types, as well as notes or records pertaining to any other actions taken by, or requested by, the FIU.

Annex 1. Indicative Examples of Insufficient STR and SAR Narratives

Example 1:

- Reason for reporting: Statements show large payments to luxury car companies. High amounts of funds transfers continue over several months.

Comments: The narrative lacks identifying information on the STR subject (name, occupation, address, account number, etc.), and no explanation is given as to why the LFI considers this activity suspicious. The narrative lacks specific transaction data that identifies the dates and amounts of the large payments and specific details on the destination of the funds (the name, location, bank, and account number of the beneficiary car companies, if identifiable).

Example 2:

- Money orders were purchased on 03-28-21 to ABC Corporation in the amount of AED30,000.

Comments: No explanation is given as to why the MVTS considers this activity suspicious. The LFI does not indicate if money orders were purchased with cash. The LFI does not provide any information about the purchaser or nature of the business (ABC Corporation) and if this activity was normal or unusual for the purchaser or the business.

Example 3:

- Mr. X was the originator of 12 wires totaling AED400,000. All of the wires were remitted to a Hong Kong based company. During the same period of time, Mr. X deposited cash into his account.

Comments: The narrative lacks specific details on the destination of the funds (the name of the Hong Kong based company, bank, and account number of the beneficiary, if identifiable). The depository LFI fails to include any information concerning the relationship, if any, between the LFI and the customer. Also, no specific transaction data is provided that identifies the dates and amounts of each wire transfer and the cash deposit.

Example 4:

- The reason for the suspicion is due to multiple third-party transfers being paid into Mr. Y account that were soon followed by multiple cash withdrawals. Funds sent from the account to multiple third parties.

Comments: The narrative lacks specific details on the source of the funds (the individual/entity sending the multiple third-party transfers). The STR does not provide a timeframe of when the transfers were made, the number and value of the third-party transfers, the number and value of the cash withdrawals, and the timeframe (how soon) the cash withdrawals were made following the third-party transfers. The depository LFI fails to include any information concerning the relationship, if any, between the individual/entity sending the multiple third-party transfers and the customer.

Example 5:

- Information has come to our attention that the Mrs. Y has been convicted of a drug trafficking offense.

Comments: The narrative fails to describe the depository LFI's relationship with the subject and include additional identifying details about the subject (name, occupation, address, account number, etc.). The narrative does not describe any suspicious activity aside from the conviction and fails to state if the suspicion is related to money laundering or if there are possible links to the financing of terrorism and illegal organisations.

Example 6:

- Mrs. Y came into the bank and asked questions during the account opening process that were suspicious.

Comments: The narrative does not describe the suspicious activity in detail as a basis for filing the SAR (e.g., the customer refusing to answer account opening questions; providing falsified or counterfeit documentation; exhibiting reluctance to provide detailed information about the customer's business). The narrative template also fails to describe information that the LFI was able to gather on the prospective customer during account opening (occupation, address, etc.).

Example 7:

- Mr. LMN was the subject of adverse media involving his association with a terrorist group.

Comments: The narrative fails to describe the depository LFI's relationship with the subject and include additional identifying details about the subject (name, occupation, address, account number, etc.). The narrative template also does not identify the terrorist group, describe the customer's relationship with the terrorist group, the timeframe for the customer's involvement with the terrorist group, and how the LFI became aware of this association, such as a hyperlink to the adverse media report.

Example 8:

- Mrs. ABC purchased an insurance product using unusual payment methods. Mrs. ABC is a teacher at Happy Day Elementary School in Dubai and resides at 11111 Street Name, Dubai, UAE. Mrs. ABC also has two motor vehicles insured with the LFI since April 2019.

Comments: The narrative fails to describe the type of insurance product purchased, on what date, with what payment method, and why the institution considers this payment method unusual. The institution also does not indicate the customer's stated purpose for purchasing the insurance product and if this is line with what the LFI knows about the customer.

Example 9:

- Mr. XYZ requests to increase payments on his life insurance policy during the period from 02-01- 21 to 05-01-21, and the payments appear to be excessive, given Mr. XYZ's prior history.

Comments: The narrative fails to include additional identifying details about the subject (name, occupation, address, etc.). The narrative lacks specific transaction data that identifies the dates, amounts, and method of payment on the life insurance policy. The narrative also does not describe why the institution considers these payments to be excessive based on the customer's prior history of payments. The narrative does not indicate how long the subject has been in possession of the life insurance policy.

Annex 2. Red Flag Indicators in the Context of the UAE

The FIU published the following typologies and indicators in their Biannual Financial Crime Trends and Typologies Report (January - June 2020). These typologies and indicators, as well as any future ones the FIU may determine, should be incorporated into an LFI's AML/CFT program with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.

B.1 General indicators

According to the FIU, the following indicators are present in many of the typologies used in money laundering and the financing of terrorism and illegal organisations.

- Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.
- Significant and/or frequent transactions in contrast to known or expected business activity.
- Significant and/or frequent transactions in contrast to known employment status.
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds.
- Where relevant, nervous or uncooperative behavior exhibited by the LFI's employees and/or customers.

B.2 Wire transfers to and from bank accounts

- **How it works:** Transferring proceeds of crime from one person to another via money remittance services.
- **Possible indicators**
  - Significant and/or frequent cash payments for transfers.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers to high-risk countries or known tax havens.
  - Transfers to numerous offshore jurisdictions with no business rationale.
  - Same home address provided by multiple remitters.
  - Reluctant to provide the LFI with identification details.

B.3 Purchase of valuable commodities

- **How it works:** Laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.
- **Possible indicators**
  - Significant and/or frequent cash purchases of valuable commodities.
  - Regularly buying and selling of valuable commodities that is not supported with a business purpose and/or does not make economic sense.

B.4 Purchase of valuable assets

- **How it works:** Laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.
- **Possible indicators**
  - Purchase/sale of real estate above/below market value irrespective of economic disadvantage.
  - Cash purchases of valuable assets with cash and/or cash deposits for valuable assets.
  - Low value property purchased with improvements paid for in cash before reselling.

- Rapid repayment of loans/mortgages with cash or funds from an unlikely source.

B.5 Offshore companies

- **How it works:** The process of registering companies in the UAE, especially in the free zones, with foreign directors and/or shareholders in order to open bank accounts to facilitate money laundering and/or the financing of terrorism and illegal organisations by unverified beneficiaries.
- **Possible indicators**
  - Large numbers of companies registered with the same office address.
  - Address on file is for a 'Virtual office'.
  - Accounts/facilities are opened/operated by company formation agents.
  - Lack of information regarding overseas directors/beneficiaries.
  - Complex ownership structures.
  - Companies where there is no apparent business purpose.
- **Additional indicators:**
  - The same natural person is the director for a large number of single director companies.
  - The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies.
  - Use of a small number of local 'agents' who undertake transactions with the companies' register.

B.6 Nominees, trustees, family members or third parties

- **How it works:** Utilizing other people to carry out transactions in order to conceal the true identity of the individual ultimately controlling the proceeds of crime.
- **Possible indicators**
  - Customers using family members or third parties, including the use of children's accounts.
  - Transactions where third parties seem to be retaining a portion of funds, which would indicate the use of mules.
  - Accounts operated by someone other than the account holder.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Significant and/or frequent transactions made over a short period of time.

B.7 Trade-based money laundering

- **How it works:** Manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- **Possible indicators**
  - Invoice value greater than value of goods.
  - Discrepancies in domestic and foreign import/export data.
  - Suspicious cargo movements.
  - Suspicious domestic import data.
  - Discrepancies in information regarding the origin, description, and value of the goods.
  - Discrepancies with tax declarations on export declarations.
  - Sudden increase in online auction sales by particular vendors (online auction sites).
  - Frequent purchases between same buyers and vendors (online auction sites).

B.8 Cancellation of credits or overpayments

- **How it works:** Laundering proceeds of crime by overpaying then requesting refund cheques for the balance.
- **Possible indicators**
  - Frequent cheque deposits issued by car dealers, dealers in jewelry, etc.
  - Significant and/or frequent payments to utility companies, for example, prepaid cards for fuel, telecom e-wallets etc.

- Frequent cheque deposits issued by utility companies (i.e., electricity providers).
- Significant and/or frequent payments for purchases from online auction sites.
- Frequent personal cheque deposits issued by third parties.

B.9 Electronic transfers to and from bank accounts

- **How it works:** Transferring proceeds of crime from one bank account to another via LFIs.
- **Possible indicators**
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers involving accounts located in high-risk countries or known tax havens.
  - Transfers to offshore jurisdictions with no business rationale.
  - Multiple transfers sent to the same person overseas by different people.
  - Departure from the UAE shortly after transferring funds.
  - Transfers of funds between various accounts that show no economic purpose (i.e., multiple transfers incurring bank fees where one single transfer would have been sufficient).

B.10 Co-Mingling

- **How it works:** Combining proceeds of crime with legitimate business takings.
- **Possible indicators**
  - Significant and/or frequent cash deposits when business has electronic funds transfer at point-of-sale facilities.
  - Large number of accounts held by a customer with the same LFI.
  - Accounts operated by someone other than the account holder.
  - Merging businesses to create layers.
  - Complex ownership structures.
  - Regular use of third-party accounts.

B.11 Gatekeepers/professional services

- **How it works:** Utilizing 'Professionals' to establish seemingly legitimate business activities, for example, Lawyers, Accountants, Brokers, Company Formation Agents.
- **Possible indicators**
  - Accounts and/or facilities opened and/or operated by company formation agents.
  - Gatekeepers that appear to have full control.
  - Known or suspected corrupt professionals offering services to criminal entities.
  - Accounts operated by someone other than the account holder.

B.12 Cash deposits

- **How it works:** Placement of cash into the financial system.
- **Possible indicators**
  - Large cash deposits followed immediately by withdrawals or electronic transfers.

B.13 Structuring

- **How it works:** Separating large transactions into small transactions to avoid scrutiny and detection from LFIs.
- **Possible indicators**
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Small/frequent cash deposits, withdrawals, electronic transfers made over a short time period.
  - Multiple low value domestic or international transfer.

B.14 Smurfing

- **How it works:** Utilizing third parties or groups of people to carry out structuring.
- **Possible indicators**
  - Third parties conducting numerous transactions on behalf of other individuals.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Accounts operated by someone other than the account holder.

B.15 Credit Cards/Cheques/Promissory Notes

- **How it works:** Instruments used to access funds held in an LFI, often in another jurisdiction.
- **Possible indicators**
  - Frequent cheque deposits in contrast to known or expected business activity.
  - Multiple cash advances on credit card facilities.
  - Credit cards with large credit balances.

B.16 Transactions inconsistent with intended purpose of the account

- **How it works:** Transactions that are out of the ordinary for the individual or conducted without a clear rationale.
- **Possible indicators**
  - Transactions to or from unrelated parties.
  - Transaction amounts that are inconsistent with the account's expected volumes or frequencies.
  - Transactions that are out of the ordinary for the customer's profession or business activity.

B.17 Cash couriers

- **How it works:** Concealing the movement of currency from one jurisdiction to another using people, luggage, mail, or any other mode of shipment, without declaration.
- **Possible indicators**
  - Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.
  - Customers originating from locations with poor AML/CFT regimes/high exposure to corruption.
  - Significant and/or frequent cash deposits made over a short period of time.
  - Significant and/or frequent currency exchanges made over a short period of time.

B.18 Other payment technologies

- **How it works:** Utilizing emerging or new payment technologies such as virtual currencies/crypto- currencies, peer-to-peer (P2P) lending etc. to facilitate money laundering and/or the financing of terrorism and illegal organisations.
- **Possible indicators**
  - Excessive use of stored value cards.
  - Significant and/or frequent transactions using mobile telephone services.
  - Unjustified transactions to and from Cryptocurrency platforms and digital assets exchanges.

B.19 Underground banking/alternative remittance services

- **How it works:** Transferring proceeds of crime from one person to another via informal banking mechanisms such as unregistered Hawaladars.
- **Possible indicators**
  - Mostly prevalent under the auspices of a general trading company license.
  - Significant and/or frequent cash payments for transfers in which the cash deposits could be from many different individuals using the cash deposit machines.
  - Cash volumes and transfers in excess of average income of migrant account holders.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Large transfers from accounts to potential cash pooling accounts.

- Significant and/or frequent transfers recorded informally using unconventional bookkeeping.
- Significant and/or frequent transfers requested by unknown or intermittent customers.
- Numerous deposits to one account followed by numerous payments made to various people.
- Vague invoices and documentation which may deliberately be made to appear complex.

B.20 Cash exchanges

- **How it works:** Exchanging low denomination notes for high denomination notes (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **Possible indicators**
  - Significant and/or frequent cash exchanges from small to large denominations.

B.21 Currency conversion

- **How it works:** Converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- **Possible indicators**
  - Significant and/or frequent local or foreign currency exchanges.
  - Opening of foreign currency accounts with no apparent business or economic purpose.

Annex 3. Red Flag Indicators for the UAE Insurance Sector

The UAE Insurance Authority has issued the following list of red flag indicators when handling life and general insurance products. The indicators, as well as any future ones the UAE Insurance Authority may determine, should be incorporated into an LFI's AML/CFT program with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity related to life and general insurance products.

1. The purchase of an insurance product does not reflect a customer's known needs (e.g., purpose of the account).
2. The early surrender of an insurance product is taken at a cost to the customer.
3. The surrender of an insurance product is initiated with the refund directed to a third party.
4. The customer exhibits no concern for the investment performance of a purchased insurance product and instead exhibits significant concern for its early surrender terms.
5. The customer purchases insurance products using unusual payment methods, such as cash or cash equivalents, or with monetary instruments in structured amounts.
6. The customer demonstrates reluctance to provide identifying information when purchasing an insurance product.
7. The customer borrows the maximum amount available from their insurance product shortly after purchase.
8. The customer used to purchase low-premium insurance and pay premiums by making regular payments but suddenly purchases insurance that requires a large lump-sum premium payment, for which no reasonable explanations are provided.
9. The customer purchases an insurance product without concern for the coverage or benefits, or the customer only cares about the procedures for the policy loan, cancellation of insurance policy, or changing beneficiary when purchasing an insurance policy that has a high cash value or requires a high lump-sum premium payment.
10. The customer usually pays a premium by making regular payments but suddenly requests to purchase a large-sum policy by paying off premium all at once.
11. The customer purchases insurance products with high cash value successively over a short period of time, and the insurance products purchased do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
12. The customer pays premiums in cash and in several payments marginally below the threshold for declaration but cannot reasonably explain the source of funds. In addition, the transactions do not appear to be

commensurate with the customer's status and income or are unrelated to the nature of the customer's business.

13. The customer, after making a large premium payment for a policy purchased, applies for a large policy loan or cancels the policy in a short period of time, for which no reasonable explanations are provided.
14. The customer is a policyholder of several motor vehicles which is inconsistent with their profile.
15. The theft of a motor vehicle is not reported by the customer/policyholder.
16. The customer attempts to insure a motor vehicle that was reported as stolen or as a total loss.

Annex 4. Overarching Rules and Principles for the goAML System

The FIU published the goAML XML Submission Guide (please see Section 3.4) with additional detail on the rules that an LFI should consider when submitting an STR, SAR, or other report type in the goAML system:

- All LFIs transactions should be reported as bi-party transactions on the goAML system.
- Reporting entities should submit only suspicious transactions in a report. Any additional transactions can be submitted via an AIFT (upon request only).
- For AIFT submissions where the number of transactions exceed 10,000, reporting entities are advised to split them into more than one AIFT; however, the AIFT should use the same "Internal Reference Number".
- A deposit is composed of a bi-party transaction occurring from a person who may be a conductor to an account.
- A withdrawal is composed of a bi-party transaction occurring from an account to a person.
- A remittance is composed of a bi-party transaction occurring from one person/account/entity to another.
- A wire transfer is composed of a bi-party transaction occurring from an account to another account.
- In case a LFI is acting as a correspondent bank within a reported transaction, then the transaction is occurring from one account to another, in which both accounts should be classified as 'Not My Client' by the LFI/Compliance Officer/MLRO.
- In the case of Exchange Houses, where a currency exchange transaction is being reported, it should be reported as a bi-party transaction, where the "from" and "to" parties are the same Person.
- The conductor field is mandatory when the transaction is conducted from an entity.
- If the date of birth for a subject (person) is unknown, then the user may enter the 1st of January 1900 in the 'Birth Date' field.
- In case the expiration date of a registered ID is unknown, then the user may enter the 31st of December 2100 in the 'Expiry Date' field.
- When reporting a transaction that involves an account, it is imperative that the LFI also provide details for the person or entity associated with the said account.

Annex 5. Synopsis of the Guidance

Introduction	Purpose	The purpose of the Guidance is to assist the understanding and effective performance by the United Arab Emirates Central Bank's (CBUAE) licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	This guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories: •National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and •Insurance companies, agencies, and brokers.

	Legal Basis	The legal basis of STR reporting is based on the (i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering (AML) and Combatting the Financing of Terrorism (CFT) and Financing Illegal Organisations and Federal Decree law No. (26) of 2021 To amend certain provisions of Federal Decree-law No. (20) of 2018, on anti-money laundering and combating the financing of terrorism and financing of illegal organisations; (ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations; and (iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution. The legal basis addresses (i) the consequences for failure to disclose suspicious activity, (ii) protection for individuals disclosing suspicious activity, and (iii) the meaning of suspicious transactions.
Identification of Suspicious Transactions	Role of the First Line of Defense	The first line of defense plays a critical role in the management of customer and third-party risk and the timely escalation of potentially suspicious activity. The first line of defense is well-placed to identify suspicious transactions and assess that information once deemed reasonable—collected through interactions with a customer—now appears suspicious. Employees within the first line of defense include relationship managers, business executives, and back-office operations functions.
	Role of the Second Line of Defense	The second line of defense (e.g., compliance employees) provides policy, advice, guidance, assurance, oversight, and challenge to the first line of defense. While employees in Financial Crime Operations Units (possibly in the first line of defense) can investigate suspicious transactions and document the resultant investigation, the ultimate filing of the STR or SAR should be made by the Compliance Officer or the money laundering reporting officer (MLRO) (in the second line of defense). The second line of defense is charged with overseeing the investigations programme.
	Role of the Third Line of Defense	The third line of defense identifies gaps, deficiencies, and weaknesses in operational controls owned or overseen by an LFI's business, operations, and compliance functions.
	Purpose of Transaction Monitoring	The purpose of transaction monitoring is the ongoing, retrospective monitoring of customers' and prospective customers' transactions or activity to identify activity anomalous from normal behavior. This may, on further investigation, generate knowledge or reasonable suspicion of financial crime and thereby require reporting to the appropriate law enforcement and/or regulatory authority as an STR, SAR, or equivalent local report in line with AML/CFT regulatory and/or UAE FIU reporting requirements.
	Internal Organization	An LFI's internal organization is important to appropriately identify unusual or potentially suspicious activity. Internal organization comprises an LFI's governance and management oversight; policies and procedures; clear lines of responsibility and reporting; and ongoing training to account for changes in the UAE's legislative and regulatory frameworks. There are also specific considerations for institutions with foreign branches and subsidiaries.

	Transaction Monitoring Methods	A transaction monitoring program should take into account the AML/CFT risks of the LFI's customers, prospective customers, counterparties, businesses, products, services, delivery channels, and geographic markets in addition to helping prioritize high-risk alerts. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or a combination of these, including an intelligence-led transaction monitoring approach.
Procedures for the Reporting of Suspicious Transactions	Importance of Filing an STR or SAR	Information generated from an STR, SAR, and other report type is important for law enforcement and the FIU to effectively identify and combat financial crime. Specifically, the quality of STRs, SARs, and other report types is imperative for increasing the FIU's analytical function to identify vulnerabilities and threats to the UAE financial system and develop an overall understanding of money laundering and the financing of terrorism and illegal organisations risks
	Basic Structure of an STR or SAR	Different report types can be filed in the FIU's "goAML" portal (i.e., STR, SAR, AIF, AIFT, RFI, RFIT, HRC, HRCA). In addition, an LFI should divide a narrative into three sections (introduction, body, and conclusion).
	Best Practices for Drafting an STR or SAR	A narrative should identify and answer the five questions – who? what? when? where? and why? – of the suspicious activity being reported to the FIU in addition to the operation/modus operandi (or how?). The Guidance also addresses how defensive STR or SAR filings are generally discouraged.
	How to Submit an STR or SAR	LFIs are required to submit suspicious transaction and activity reports directly to the FIU using the "goAML" portal. There are certain mandatory fields that an LFI should populate when submitting a report in the goAML portal in addition to providing certain supplemental documents.
	Amendments to Submitted Reports	Once a report is submitted and accepted in the goAML system, changes cannot be applied, including amendments for missing or incorrect information. However, LFIs may file a corresponding AIF, AIFT, RFI, or RFIT.
Timing of Alert Reviews and STR Filings	Alert Review, Case Investigation, and STR/SAR Decision Making and Filing	In the absence of escalation for expedited review, LFIs are expected to file an STR/SAR within a maximum of 35 business days from the date of automated alert generation. The establishment of adequate grounds of suspicion may involve the investigation procedures as per the LFIs' AML and/or Financial Crime Compliance policies and procedures. LFIs are expected to complete the required investigative procedures as expeditiously as possible. LFIs must maintain adequately detailed records of investigative procedures performed against alerts and when filing an STR/SAR, must include a summary justifying the time taken to establish grounds of suspicion. In the event of escalation for expedited review, the Compliance Officer or MLRO should file an STR or SAR to the FIU within 24 hours of the determination. All prospective STRs or SARs should be reviewed for accuracy and completeness prior to filing, in accordance with applicable procedures.
	Monitoring and Reporting of Continuing Suspicious Activity	Upon filing an STR/SAR pertaining to an account holder, LFIs are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against

		said account holder, LFIs are expected to expeditiously file an STR/SAR with the FIU.
	Activity Requiring Immediate Attention	Situations requiring immediate attention include reportable violations that are ongoing (e.g., part of an ongoing money laundering scheme as indicated by an appropriate law enforcement authority) and transactions that the LFI suspects are related to the financing of terrorism and illegal organisations.
	Exceptions for Complex Investigations	If the LFI designates an investigation as "complex", the LFI should submit an initial STR or SAR to the FIU within 15 business days of the alert generation. The initial STR/SAR should be labelled as a "Complex investigation" to the FIU. Following the initial STR or SAR filing, the LFI has an additional 30 business days to obtain all necessary information related to the complex investigation and submit a follow-up STR or SAR to the FIU.
	Summary of Review, Investigation, and Reporting Timelines	There are recommended timelines for the review, investigation, and reporting of suspicious activity in the absence of an escalation for expedited review.
	Escalation for Expedited Review	In certain cases, an alert or case may need to be dispositioned and an STR or SAR filed more rapidly than usual processes allow. In such cases, the alert will be dispositioned and the STR or SAR filed within 24 hours.
Confidentiality and Prohibition against "Tipping Off"	Confidentiality and Prohibition against "Tipping Off"	When reporting suspicious activity or transactions to the FIU, LFIs are obliged to maintain confidentiality regarding both the information being reported and specific to the act of reporting itself, and to make reasonable efforts to ensure that the information and data reported are protected from access by any unauthorized person.
Handling of Transactions and Business Relationships after Filing STRs	Requirements for Corresponding with the FIU	If the FIU reaches out to an LFI for additional information pertaining to an STR or SAR, details should be provided in a way that is precise and outlined as per the request. LFIs should maintain clarity on the presented information and provide it in the expected format.
	Post STR or SAR Process	Following the filing of an STR or SAR filing, LFIs are obliged to follow the instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general. LFIs may decide to retain a customer relationship, exit the relationship, or restrict an account, among others. Any actions taken by an LFI following the filing of an STR or SAR is a decision based on the LFI's internal policies and procedures, including its risk appetite, although LFIs should consider the risk of tipping off a customer when implementing such restrictive measures.
	Governance and Reporting to Senior Management	LFIs should have mechanisms to inform the Board of Directors (or a committee of the Board) and senior management on the status of its AML/CFT program, including reporting on the number and types of STRs or SARs.
	Record Retention	LFIs are required to retain all records and documents pertaining to STRs or SARs and the results of all analysis or investigations performed for a period of no less than five (5) years from the date of completion of the transaction or termination of the business relationship.
Annexes	Annex 1: Indicative Examples of Insufficient STR or SAR Narratives	Examples of insufficient STR or SAR narratives are provided with an explanation on why these STR or SAR narratives are not sufficient and comprehensive.

	Annex 2. Red Flag Indicators in the Context of the UAE	The FIU published typologies and indicators of suspicious activity that an LFI should consider with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.
	Annex 3. Red Flag Indicators for the UAE Insurance Sector	The UAE Insurance Authority issued a list of red flag indicators that an LFI should consider with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.
	Annex 4. Overarching Rules and Principles for the goAML System	The goAML XML Submission Guide provides additional detail on the rules that an LFI should consider when submitting an STR, SAR, or other report type in the goAML system.
	Annex 5	Synopsis of the Guidance

Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions

Effective from 4/7/2021 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations*[1] (issued by Notice No. 74/2019 dated 19/06/2019) and the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control's ("Executive Office") *Guidance on Targeted Financial Sanctions for Financial Institutions and Designated Non-financial Business and Professions*[2] (circulated by CBUAE Notice No. 2893 dated 02/06/2021) and any amendments or updates thereof. As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.
[2] Available at: https://www.uaeiec.gov.ae/en-us/un-page#

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementation Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions ("Cabinet Decision 74").

The AML-CFT Law and the AML-CFT Decision require LFIs to promptly apply directives issued by the competent authorities of the UAE for implementing the decisions issued by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision 74 sets out the legislative and regulatory framework regarding the Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List.

The Executive Office[3] acts as a national lead to coordinate and liaison implementation of TFS with all the federal and local government stakeholders including financial institutions (FIs) and designated non-financial business and professions (DNFBPs) and has issued the *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*". The Executive office is mainly responsible for:

- Receiving and processing grievances against Listing in UN and Local Lists decisions;
- Receiving and processing applications to use frozen funds as per sanctions lists;
- Working closely with the Supreme Council with regards to the local Listing;
- Circulating updates to the local and UN lists to the government and private sector; and
- Coordinating and exchanging information between Government Agencies.

This Guidance issued by the CBUAE is supplementary to the above mentioned "*Guidance on Targeted Financial Sanctions for Financial Institutions and Designated Non-financial Business and Professions*" issued by the Executive Office.

[3] Website: Home | Committee for goods & material subjected to import & export (uaeiec.gov.ae)

1.4. Definitions

Controlling Shareholder: A shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the board of directors, or the decisions made by the board or by the general assembly of the entity, through the ownership of a percentage of the shares or stocks or under an agreement or other arrangement providing for such influence.

Direct Relationship: A relationship between two parties that knowingly provide the other material, technological, logistical, or financial support and both parties are directly impacted by the other party.

Funds: Assets of all types, in whatever form and however acquired, whether corporeal or incorporeal, tangible or intangible, movable or immovable, electronic, digital or encrypted, including national currency, foreign currencies, documents and legal instruments establishing ownership of such assets or any associated rights, in whatever form, including electronic or digital forms, as well as economic resources considered as assets of any kind, including oil and natural resources, and bank credits, cheques, money orders, shares, securities, bonds, drafts, and letters of credit and any interest, dividends, or other income accruing from or generated by such assets, and that may be used to obtain any other funds, goods or services including internet posting services or related services.

Indirect Relationship: A relationship between two parties that affect each other through a third-party source or one or more intermediaries.

Listed Person: Individuals, legal entities and groups listed by the UN Security Council on the UN Consolidated List, or listed by the UAE Cabinet on the Local Terrorist List, as the case may be.

Listing: Identifying the individuals, legal entities and groups subject to sanctions imposed pursuant to relevant UNSC Resolutions ("UNSCRs"), decisions of the Sanctions Committee, or relevant decisions of the UAE Cabinet, as the case may be, and implementing relevant sanctions against such individuals, legal entities and groups, with a statement of the reasons for Listing.

Local Terrorist List: Terrorism lists issued by the UAE Cabinet pursuant to the provisions of Article (63) paragraph (1) of Federal Law No. (7) of 2014 on Combating Terrorism Offences.

Other Measures: Sanction measures other than freezing that must be enforced, and which may be included in Relevant UNSCRs or UAE Cabinet decisions regarding the issuance of Local Terrorist List, such as prohibitions relating to travel, weapons, imports, or provision of fuel supplies and other.

Previous Customer: A customer with whom the relationship was terminated and the LFI maintains relevant records according to record keeping and other requirements.

Relevant UNSCRs: All current and future UNSCRs relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1373 (2001), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.

Sanctions Committee: Any of the UN Security Council Committees established as per its resolutions, including UNSCRs 1267 (1999) and 1989 (2011) relating to ISIL and Al-Qaida, 1988 (2011) relating to the Security and Stability of Afghanistan, and 1718 (2006) relating to the suppression and combating of proliferation of weapons of mass destruction for the DPRK.

Subsidiary: An entity owned by another entity by more than 50% of its capital or under full control of that entity regarding appointment of the Board of Directors.

Targeted Financial Sanctions (TFS): The term Targeted Financial Sanctions means that such sanctions are against certain individuals, entities, groups, or undertakings. The term Targeted Financial Sanctions includes both asset

freezing and prohibitions to prevent funds or other assets from being made available, directly, or indirectly, for the benefit of individuals, entities, groups, or organization who are sanctioned.

The Executive Office: The Executive Office of the Committee for Goods and Materials Subject to Import and Export Control.

UN Consolidated List: A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their Listing.

Without Delay: Within 24 hours of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

2. Sanctions Compliance Program

LFIs should take appropriate steps to develop, implement and regularly update an appropriate Sanctions Compliance Program (SCP) in order to fulfil their obligation to comply with the provisions of the Cabinet Decision 74 as well as with the directives of the relevant competent authorities and supervisory authorities in regard to sanctions issued by the UNSC. An appropriate SCP also assists LFIs to manage their exposure to the risks associated with international financial sanctions programs and restrictive measures implemented by other countries.

LFIs should design and update their SCP so that its scope is proportionate to the level of their risk profile, tailored to their nature, scale, and complexity, appropriate for the products and services they offer, the customers, clients, and partner relationships they maintain, and the geographic regions in which they operate. LFIs should ensure the SCP includes the eight (8) essential components: senior management commitment, risk assessment, sanctions risk appetite, internal controls, policies and procedures, training, independent audit and testing of processes and systems, and record keeping.

2.1. Senior Management Commitment

Senior management is defined broadly to include senior leadership, executives, and the board of directors. Senior management's commitment to, and support of, the LFI's SCP is one of the most important factors in determining its success. In order to facilitate effective senior management commitment, an LFI should:

- Ensure that senior management has reviewed and approved the organization's SCP.
- Ensure that senior management has reviewed and approved the methodology used for undertaking the risk assessment and reviewed and approved the LFI's risk assessments at least on an annual basis.
- Clearly designate the personnel responsible for ensuring proper implementation of the SCP, including day-to-day operations, and compliance with statutory obligations. This personnel should have the appropriate competencies and experience, or be appropriately trained, to perform the duties and responsibilities associated with this role, has sufficient seniority, and is delegated sufficient authority and autonomy in order to discharge the LFI's responsibilities. The personnel may have other responsibilities in the LFI, provided that these responsibilities do not conflict with their role in implementing the SCP. For example, large LFIs may choose to hire a dedicated sanctions compliance officer, while smaller LFIs may choose a specific officer or manager currently working at the LFI to be responsible for the SCP in addition to their other duties.
- Ensure the existence of direct reporting lines between the personnel responsible for the SCP and senior management to facilitate the escalation of financial sanctions issues, including regular and periodic meetings.
- Ensure that the SCP is fully integrated into the organization's daily operations and allocated adequate resources in the form of human capital, expertise, information technology, and other resources as appropriate.

- Recognize compliance failings and implement necessary measures to reduce future incidents, including through addressing root causes and implementing systemic solutions.

2.2. Risk Assessment

LFIs should take appropriate steps to conduct a regular and updated risk assessment to identify, understand, assess, monitor, and manage their risks in line with their business nature and size. While there is no "one-size-fits all" risk assessment, the assessment exercise should generally consist of a holistic review of the LFI from top-to-bottom and assess its touchpoints to the outside world where the LFI may potentially, directly or indirectly, be exposed to sanctioned parties or transactions. In most cases, LFIs should consider performing such risk assessments annually; however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. These may include a change to the LFI risk profile, regulatory or law enforcement advisories, or global trends in terrorism financing ("TF") and the financing of proliferation of weapons of mass of mass destruction ("PF").

- In determining potential risks, LFIs should take into account, to the extent relevant, any vulnerabilities relating to:
  - its customers, supply chain, intermediaries, and counterparties;
  - its products and services, including how and where such items fit into other financial or commercial products, services, networks, or systems;
  - the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counterparties;
  - its distribution channels and business partners;
  - the complexity and volume of its transactions;
  - the development of new products and business practices including new delivery mechanisms, channels, and partners; and
  - the use of new or developing technologies for both new and pre-existing products and services.
- LFIs should document risk assessment operations, maintain them up-to-date on an on-going basis, and make them available upon request.
- The results of a risk assessment are integral to informing the SCP's policies, procedures, internal controls, and training in order to effectively mitigate risks.
- LFIs should develop and thoroughly document their risk assessment methodologies to identify, analyze, and address relevant risks. The methodologies should reflect the conduct and root cause of any violations or systemic deficiencies identified.

2.3. Sanctions Risk Appetite

LFIs should develop and maintain a comprehensive written sanctions risk appetite approved by the LFI's senior management and embedded through policies, procedures, and screening systems parameterization.

- The sanctions risk appetite should specify which sanctions regimes are applicable to the LFI (for example UNSCR, OFAC, EU, UK etc.).
- LFIs should specify their policy on treating of interests, properties, assets, or entities that are owned or controlled 50% or more by a Listed Person.
- LFIs should specify their approach on mitigating the risk of breaching of unilateral sanctions, especially in the context of sanctions that may have extra-territorial implications or the Listed Persons may or may not have a presence in UAE (for example secondary sanctions by OFAC).
- LFIs should specify their approach on screening of alias names such as one word synonyms, vessel names or paper based instruments.
- LFIs should identify and document any exceptions to sanctions risk appetite or deviations from their policies and procedures; these should be approved by senior management.

For more details and information, please refer to Annex 2 for related Lessons learned from CBUAE Supervision.

2.4. Internal Controls

Internal controls are the mechanisms, rules, and procedures implemented to help ensure the integrity and effectiveness of an LFI's SCP. As required by Cabinet Decision 74, LFIs must have appropriate internal controls in place, including the most recent publication of Targeted Financial Sanctions of the UN Consolidated List and the Local Terrorist List. Accordingly, LFIs must maintain strong and clear internal controls that ensure the effective implementation of their SCP, including policies, procedures, processes, and systems.

- LFIs should document how their processes and systems are configured in order to demonstrate that their configuration is reasonably expected to detect and manage the specific sanctions risks to which the LFI is exposed to and ensure transparency of any system limitations or risk-based decisions that the screening controls are not designed to detect.[4]
- LFIs should establish a mechanism to ensure that, upon learning of a weakness pertaining to its SPC compliance, immediate and effective action is taken to identify compliance gaps and their root causes, including all program-related software, systems, and other technology, and remediate them by implementing systemic solutions to reduce the chances of future failures.

[4] See https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf

2.5. Policies and Procedures

LFIs should develop and maintain clear and comprehensive written policies and procedures to enable them to manage and mitigate the sanctions risks they have identified, commensurate with the nature and size of their business.

- LFIs should ensure that policies and procedures are approved by senior management and that they:
  - Enable the LFI to clearly and effectively identify, prevent, escalate, and report suspicious transactions and activities;
  - Are tailored to the organization and capture the organization's day-to-day operations and processes;
  - Are easy to follow and designed to prevent employees from engaging in misconduct;
  - Prohibit employees from, directly or indirectly, informing the customer or any third party that freezing or any Other Measures shall be implemented;
  - Require enhanced due diligence to be conducted on all customers and transactions that are assessed to be high-risk for TF and PF; and
  - Contain sufficient detail of their record keeping obligations.
- LFIs should ensure the effective and consistent implementation of the policies and procedures related to the SCP across their organizations, including branches, Subsidiaries, and other entities in which LFIs hold a majority interest.
- LFIs should clearly communicate the SCP's policies and procedures, including for record keeping, to all relevant employees and external or outsourced service providers.
- LFIs should review and update policies and procedures in a timely manner in response to events or emerging risks and ensure that such updates are communicated to employees on a timely basis.
- LFIs should implement a formal review process at least annually of the policies and procedures at appropriate levels subject to approval where changes are material.
- LFIs should identify and document any exceptions or deviations from the policies and procedures related to the SCP; these should be approved by senior management.

2.6. Training

The maintenance and implementation of an effective SCP requires that all relevant employees and management understand requirements and obligations, policies and procedures, internal control mechanisms, and threats, risks, and vulnerabilities. A robust training program is an integral component of an effective SCP. A training program should:

- Be of a scope and nature proportionate to the LFI's overall risk profile;
- Be specific to the role carried out by the employee, with tailored training for employees engaged in sensitive roles;
- Provide training to all appropriate employees and personnel upon onboarding in a timely manner and at least annually thereafter;
- Hold employees accountable for training through assessments;
- Include measures to take immediate and effective action to provide corrective training or other corrective actions to relevant personnel upon learning of a confirmed negative risk assessment result or audit finding, or other deficiency pertaining to the SPC.

2.7. Independent Audit and Testing of Processes and Systems

Independent audit helps the LFI assess the effectiveness of current processes, including by assessing the sufficiency of the program and by checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify SCP weaknesses and deficiencies. Independent audits should:

- Be undertaken regularly to review and assess the effectiveness of the financial sanctions policies, procedures, systems and controls, and their compliance with the LFI's obligations;
- Be undertaken by the internal audit function, or by a competent independent external auditor, or both, and resourced with skilled and competent staff that understand the SCP of the LFI; and
- Be commensurate to the level and sophistication of the SCP and updated to account for changing risk assessments or sanctions environments.

LFIs should ensure that the audit function is independent of the audited activities and functions, and has sufficient authority, skills, expertise, and resources within the organization. LFIs should immediately address negative audit findings and take the necessary steps to identify and implement compensating controls until the root cause is remediated.

In addition, LFIs should deploy an independent risk-based testing regime to regularly test their processes' and systems' adequacy and expected outcomes, as well as to assess their effectiveness in managing the specific risks articulated in the risk assessment. Regular testing of processes and systems ensures that the screening application generates expected alerts, threshold settings and/or screening rules to forego or suppress undesirable alerts in accordance with the LFI's risk appetite. Regular testing should be supported by metrics, analysis, and reporting, and be reviewed by the personnel responsible for the SPC to determine whether risk acceptance or remediation is appropriate with respect to any relevant findings. Regular testing could be undertaken by the internal audit function, or by a competent external provider, or both.

2.8. Record Keeping

According to the AML-CFT Law and the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed. LFIs must maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so

as to provide, if necessary, evidence for prosecution of criminal activity. LFIs must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.

3. Screening Operations

Under Article 21.2 of Cabinet Decision 74, **LFIs must regularly screen their databases and transactions against names on the UN Consolidated List and the Local Terrorist List, and also immediately when notified of any changes to any of such lists,** provided that such screening includes the following:

- Searching their customer databases
- Search for the names of parties to any transactions.
- Search for the names of potential customers.
- Search for the names of beneficial owners.
- Search for names of persons and organizations with which they have a direct or indirect relationship.
- Continuously search their customer database before conducting any transaction, or entering into a serious business relationship with any person, to ensure that their name is not listed on the UN Consolidated List or the Local Terrorist List.

3.1. Sanctions Evasion

Illicit actors targeted by sanctions are likely to utilize a range of tactics to evade the prohibitions, which can be difficult to identify. LFIs should remain vigilant in order to identify attempts to evade, avoid, or circumvent sanctioned activities. Frequent tactics employed for sanctions evasion include renaming, using intermediaries, creating front companies, and using alternative financial networks. LFIs should monitor not only for sanctions violations but also for red flags of potential evasion risks. LFIs also a need to remain vigilant for new methods of evading sanctions. Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") play a critical role, in combination with sanctions screening, to identify and prevent more complicated forms of sanctions evasion.

LFIs should also prohibit activity that aims to evade or circumvent sanctions prohibitions. Accordingly, LFIs must not engage in activities that could be part of a sanctions evasion scheme, including but not limited to:

- Tipping off customers or counterparties;
- Omitting, withholding, altering, misstating, or removing any information about customers or transactions;
- Accepting incomplete (when the customer deliberately does not provide an identifier to obscure being matched with the sanctions lists, such as a date of birth or address) or false information (when the customer provides a false identifier that would not match with the sanctions lists listed details, such as a wrong date of birth);
- Providing false or incomplete information to counterparties or sanctions-imposing authorities; or
- Any other activities that would cause a conflict with or failure to comply with this Guidance.

For more details and information, please refer to the Executive Office's "*Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction*" (circulated by CBUAE Notice No. 2893 dated 02/06/2021).

3.2. Maintenance of UN Consolidated List and Local Terrorist List

LFIs should rely on the official website of the UNSC for the most updated UN Consolidated List:

https://www.un.org/securitycouncil/content/un-sc-consolidated-list

LFIs should rely on the official website of the Executive Office to obtain the most recent publication of the Local Terrorist List issued by the UAE Cabinet:

https://www.uaeiec.gov.ae/en-us/
https://www.uaeiec.gov.ae/ar-ae/

In addition, under Article 21 of Cabinet Decision 74, LFIs must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the Listing and de-Listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.

When LFIs utilize external vendors' lists for their Sanctions List and Local Lists, it is the LFI's responsibility to undertake due diligence on these vendors and ensure that the vendors' lists contain all names listed by the UN Consolidated List and UAE Local Terrorist List.

3.3. Customer Screening

Screening processes should be conducted at various stages of the customer lifecycle to include:

- Periodic name screening: A change to either the customer identifying information or UN Consolidated List /Local Terrorist List should trigger an automatic rescreening.
- Ad hoc name screening: Such screening is triggered by a specific business need or in order to comply with a request by a competent authority, or in the case of feedback from a downstream financial institution.
- Re-screening: A specific scenario in the transaction monitoring system identifies a high-risk jurisdiction in updated customer information.

3.4. Name Screening

In addition to the regular screening utilizing the UN Consolidated List and Local Terrorist List indicated above, LFIs should maintain the following sanctions compliance procedures to prevent and detect sanctions breaches:

1. **Ownership/Control Rule:** Individuals or legal entities that are directly or indirectly owned or controlled mainly or fully by one or more Listed Person are subject to the same prohibitions as the Listed Person, even if such individuals or legal entities are not specifically named by the competent authority on the respective UN Consolidated List or Local Terrorist List.

The criterion to be taken into account when assessing whether an individual or legal entity is mainly **owned** by a Listed Person is the possession of more than 50% of the proprietary rights of an entity or having majority interest in it. If this criterion is satisfied, it is considered that the individual or legal entity is owned by a Listed Person.

The criteria to be taken into account when assessing whether an individual or legal entity or arrangement is mainly **controlled** by a Listed Person, alone or pursuant to an agreement with another shareholder or other third party, include the following:

- Having the right to appoint or remove a majority of the members of the administrative or management body of such a legal person, entity, group or arrangement;

- Having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative or management body of a legal person, entity, group or arrangement who have held office during the present and previous financial year;

- Controlling alone, pursuant to an agreement with other shareholders in or members of a legal person, group or entity, a majority of shareholders' or members' voting rights in that legal person, entity, group or arrangement;

- Having the right to exercise a dominant influence over a legal person, group or entity, pursuant to an agreement entered into with that legal person, entity, group or arrangement, or to a provision in its Memorandum or Articles of Association, where the law governing that legal person, entity, group or arrangement permits its being subject to such agreement or provision;

- Having the power to exercise the right to exercise a dominant influence referred to in the previous point, without being the holder of that right;

- Having the right to use all or part of the assets of that legal person, entity, group or arrangement;

- Managing the business of that legal person, entity, group or arrangement on a unified basis, while publishing consolidated accounts; or

- Sharing jointly and severally the financial liabilities of legal person, entity, group or arrangement, or guaranteeing them.

2. Fuzzy Matching: An algorithm-based technique to match one data point, where the contents of the information being screened is not identical, but its spelling, pattern or sound is a close match to the contents contained on a list used for screening.

3. Weak or Low-quality Aliases: Relatively broad or generic alias may generate a large volume of false hits when such names are run through a computer-based screening system. LFIs should perform their own assessments on whether to screen for weak aliases based on their understanding of their own risk profile.

3.5. Verification of False Positives

Because many names may be common, various potential matches may be found. A potential match is when there is any match between data in the sanctions lists with any information in the LFI's databases. However, it does not necessarily mean that the individual or entity the LFI is dealing with is subject to sanctions. **When identifying the potential match, LFIs should suspend any transaction until they are satisfied it is not a Listed Person.**

LFIs should compare potential matches with the UN Consolidated List and the Local Terrorist List in order to confirm whether they are true matches and to eliminate "false positives." LFIs should compare information that is known about the party in question, such as date of birth and address, with other information provided in the designation order. Furthermore, LFIs should undertake efforts to obtain additional information and identification documents, which may have previously not been obtained from the customer or a counterparty to ascertain whether the customer is the actual designated person in the case of similar or common names. If the LFI establishes that the match is a false positive, then the LFI does not need to freezing or apply Other Measures related to sanctions. Therefore, the LFI may allow the transaction or relationship to continue its normal course, provided that the transaction or relationship is not suspicious and does not trigger any other concerns. LFIs are required to maintain evidence of the false positive verification process in their records and make them available to the competent authorities immediately upon request.

LFIs may create a "white list" (or a "good customer list") of names of customers that have been flagged as potential matches to the UN Consolidated List and the Local Terrorist List but subsequently cleared through thorough due diligence by the LFI. Those "white lists" may be used to improve the process related to screening by leveraging the results of past due diligences and reducing the number of false positives. While an LFI should not overly rely on such a list and must diligently and continuously screen customers and transactions in case they are implicated in updated UN Consolidated List and Local Terrorist List, the use of such a "white list" may assist the LFI in expediting the

dispositioning in case of repeated false positive matches. LFIs should have documented procedures to managing and periodically reviewing and updating those "white lists".

For more details and information, please refer to Annex 2 for related Lessons learned from CBUAE Supervision.

3.6. Payments Screening

LFIs should also screen information regarding counterparties of all incoming and outgoing transfers in order to identify any potential match to Listed Persons. The information to be screened includes:

- The parties involved in a transaction, including the sender and the receiver;
- Third parties and intermediaries;
- Bank Names, Bank Identifier Code ("BIC") and other routing codes;
- Free text fields;
- International Securities Identification Number ("ISINs") or other risk relevant product identifiers (there are multiple fields in the identifier information section for sanctions lists. An ISIN number can be screened as an identifier number similar to a date of birth/passport number, and towns/regions can be screened as jurisdictions operating in);
- Geography, including addresses, countries, cities, towns, regions.

3.7. Confirmed match

Under Articles 15 and 21 of Cabinet Decision 74, when a match is found through the screening process, LFIs must immediately, without delay and without prior notice, freeze all Funds. Without delay, as defined by Article 1 of Cabinet Decision 74, means **within 24 hours** of the Listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.

For more details and information, please refer to the Executive Office's *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*.

4. Notification to Cbuae and Executive Office

Under Article 21(5) of Cabinet Decision 74, **LFIs must immediately notify the CBUAE** in the following cases:

- Identification of funds and actions that have been taken as per requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Terrorist List (including but not limited to freezing), including attempted transactions.
- Detection of any match with Listed Persons or entities, details of the matched data, and actions that have been taken as per the requirements of Relevant UNSCRs and Local Terrorist Lists, including attempted transactions.
- Identification of a previous customer or an occasional customer listed on the UN Consolidated List or Local Terrorist List.
- Suspicion that a current or previous customer, or a person with whom they have a business relationship, is a Listed Person or has a direct or indirect relationship with a Listed Person.
- No action has been taken due to a false positive and the inability to dismiss a false positive through available or accessible information (i.e. given insufficient information, such as matching identifier information, address, DOB, or nationality). Please see also section 3.5 above.
- Unfreezing of Funds, identifying the information relating to funds that have been unfrozen, including their status, nature, value and measures that were taken in respect thereof, and any other information relevant to such decisions.

Under Article 15(2) of Cabinet Decision, **LFIs must also notify the Executive Office** of any freezing measures and/or attempted transactions.

According to the Executive Office's *Guidance on Targeted Financial Sanctions for FIs and DNFBPs*, LFIs should notify the CBUAE and the Executive Office within two (2) business days from taking any freezing measure and/or attempted transactions. For the reporting mechanism and form(s), please consult the CBUAE's and the Executive Office's websites as updated from time to time.

Annex 1. Red Flag Indicators for TF and PF

Accurately identifying and assessing the TF and PF risks of a customer or business relationship is critical for appropriately managing these risks. A single indicator on its own may seem insignificant, but when combined with others it could provide reasonable grounds to suspect that the transaction is related to TF or PF activity.

1. Red Flag Indicators for TF7

Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual[5]

Activity Inconsistent with the Customer's Business:

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).
- The stated occupation of the customer is not commensurate with the type or level of activity.
- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
- Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

Funds Transfers:

- A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
- Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

Other Transactions That Appear Unusual or Suspicious:

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.

- Banks from higher-risk locations open accounts.
- Funds are sent or received via international transfers from or to higher-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Terrorist Financing Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)[6]

- Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.
- An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
- The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
- Raising donations in an unofficial or unregistered manner.
- Client identified by media or law enforcement as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.
- Law enforcement information provided which indicates individual(s) or entity(ies) may be linked to a terrorist organization or terrorist activities.
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
- Individual or entity's online presence supports violent extremism or radicalization.
- Client donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).

---

[5] Available at: https://bsaaml.ffiec.gov/manual/Appendices/07

[6] Available at: https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/fin_mltf-eng

2. Red Flag Indicators for PF

Indicators of Possible Proliferation Financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing[7]

(i) Transaction involves person or entity in foreign country of proliferation concern.
(ii) Transaction involves person or entity in foreign country of diversion concern.
(iii) The customer or counterparty or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
(iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.
(v) A freight forwarding firm is listed as the product's final destination.
(vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
(viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).
(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.
(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.

(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
(xiii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).
(xiv) Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
(xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
(xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
(xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
(xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
(xix) New customer requests letter of credit transaction awaiting approval of new account.
(xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
(xxi) Involvement of items controlled under WMD export control regimes or national control regimes.
(xxii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
(xxiii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.
(xxiv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
(xxv) Involvement of a customer or counterparty, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
(xxvi) Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
(xxvii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).
(xxviii) Involvement of a university in a country of proliferation concern.
(xxix) Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.
(xxx) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.
(xxxi) Use of personal account to purchase industrial items.

---

[7] Available at: fatf guidance on proliferation financing (fatf-gafi.org)

3. Red Flag Indicators for Potential Sanctions Circumventions

Some Red Flags or Situations to Identify Potential Sanctions Circumventions Published in the Executive Office's "Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction" [8]

The following are some red flags or situations that could be looked at more closely or monitored by financial institutions and designated non-financial businesses or professions to identify potential sanctions circumventions of your clients, their business, or their transactions.

- Dealings in sectors vulnerable for terrorist financing and/or proliferation of weapons of mass destructions, for example
  - Financial sector
  - Hawalas or other money transfer services providers

    - Oil and gas sector
    - Non-profit organizations
    - International trade
- Dealings, directly or through a client of your client, with high-risk countries for terrorism financing.
- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
- Dealings with sanctioned goods or under embargo. For example:
    - Weapons
    - Oil or other commodities
    - Luxury goods (for DPRK sanctions)
- Dealings with dual-used goods.
- Dealings with controlled substances.
- Identifying documents that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- Use of intermediaries.
- When the flows of funds exceed those of normal business (revenues or turnover).
- The activity developed or financed does not relate to the original or intended purpose of the company o entity. For example:
- For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
- For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.
- Carrying out of multiple ATM cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or in the border of sanctioned countries.
- Irregularities during the CDD process which could include, but is not limited to:
    - Inaccurate information about the source of funds and/or the relationship with the counterparty.
    - Refusal to honor requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.
    - Suspicion of forged identity documents

[8] Available at https://www.uaeiec.gov.ae/en-us/un-page#

Annex 2. Lessons learned from CBUAE Supervision

In 2020 the CBUAE's AML/CFT Supervision Department conducted a thematic review of 30 LFIs' sanctions screening systems. The aim of the review was to assess the LFIs' compliance with these provisions and their sanctions screening systems' effectiveness and efficiency levels.

For more details and information, please refer to the CBUAE's "*Sanctions Screening Testing Thematic Review – Lessons Learned and Expectations".*[9]

[9] Available at https://www.centralbank.ae/en/cbuae-amlcft.

Annex 3. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by the CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE related to targeted financial sanctions, screening and reporting requirements as well as the development of an appropriate sanctions compliance program.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: ▪ national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and ▪ insurance companies, agencies, and brokers.
Sanctions Compliance Program	Senior Management Commitment	LFI senior management's commitment to, and support of, the Sanctions Compliance Program (SCP) is one of the most important factors in determining its success. In order to facilitate effective senior management commitment, an LFI should, among other things: ▪ Ensure that senior management has reviewed and approved the organization's SCP; ▪ Clearly designate the personnel responsible for ensuring proper implementation of the SCP; and ▪ Ensure that the SCP is fully integrated into the organization's daily operations and allocating adequate resources to it.
	Risk Assessment	LFIs should take appropriate steps to conduct a regular and updated sanctions risk assessment to identify, understand, assess, monitor and manage their risks in line with their business nature and size.
	Sanctions Risk appetite	LFIs should develop and maintain a comprehensive written sanctions risk appetite approved by the LFI's senior management and embedded through policies, procedures, and screening systems parameterization.
	Internal Controls	Internal controls are the mechanisms, rules, and procedures implemented to help ensure the integrity and effectiveness of an LFI's SCP. LFIs must have and maintain strong and clear internal controls to ensure compliance with their statutory sanctions obligations and ensure the effective implementation of their SCP.
	Policies and Procedures	LFIs should develop and maintain clear and comprehensive written policies and procedures that should, among other things: ▪ Be approved by senior management; and ▪ Enable the LFI to clearly and effectively identify, prevent, escalate, and report potentially prohibited transactions and activities. LFIs should ensure the effective and consistent implementation of the policies and procedures related to the SCP across their organizations, including branches, subsidiaries, and other entities in which LFIs hold a majority interest. LFIs should implement a formal review process, at least annually, of the policies and procedures at appropriate levels subject to approval where changes are material.
	Training	A robust training program is an integral component of an effective SCP and should, among other things:

		▪ Be of a scope and nature proportionate to the LFI's overall risk profile; ▪ Be specific to the role carried out by the employee, with tailored training for employees engaged in sensitive roles; and ▪ Provide training to all appropriate employees and personnel upon onboarding in a timely manner and at least annually thereafter.
	Independent Audit and Testing of Processes and Systems	Independent audit helps the LFI assess the effectiveness of current processes, including by assessing the sufficiency of the program and by checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify SCP weaknesses and deficiencies. In addition, LFIs should deploy an independent risk-based testing regime to regularly test their processes' and systems' adequacy and expected outcomes, as well as to assess their effectiveness in managing the specific risks articulated in the risk assessment.
	Record keeping	LFIs must maintain, at least for five years, detailed records associated with their ML/FT risk assessment and mitigation measures as well as all records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed; and make them available to authorities on request.
Screening Operations	Sanctions Evasion	LFIs should remain vigilant in order to identify attempts to evade, avoid, or circumvent sanctioned activities. LFIs should monitor not only for sanctions violations but also for red flags of potential evasion risks. LFI's should also prohibit activity that aims to evade or circumvent sanctions prohibitions.
	Maintenance of Sanctions List and Local Lists	LFIs should rely on the official websites of the UNSC and the Executive Office of the Committee for Goods & Materials Subject to Import & Export Control (Executive Office) respectively for the most updated UN Consolidated List and Local Terrorist List. LFIs must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.
	Customer Screening	Screening should be conduct at various stages of the customer lifecycle, to include periodic name screening, ad hoc name screening, and re- screening.
	Name Screening	In addition to the regular screening utilizing the lists indicated above, LFIs should maintain additional sanctions compliance procedures relating to name screening to prevent and detect sanctions breaches. These procedures should address the ownership/control rule, fuzzy matching, and weak or low-quality aliases.
	Verification of False Positives	LFIs should compare potential matches with the sanctions lists indicated above in order to confirm whether they are true matches and to eliminate "false positives." If the LFI establishes that the match is a false positive, then the LFI does not need to freezing or apply other measures related to sanctions. The LFI may allow the transaction or relationship to continue its normal course, provided that the transaction or relationship is not suspicious and does not trigger any other concerns. LFIs are required to maintain evidence of

		the false positive verification process in their records and make them available to the competent authorities immediately upon request.
	Payments Screening	LFIs should also screen information regarding counterparties of all incoming and outgoing transfers in order to identify any potential match to Listed Persons.
	Confirmed Match	When a match is found through the screening process, LFIs must immediately, without delay and without prior notice, freeze all Funds. Without delay, as defined by Cabinet Decision 74, means within 24 hours of the listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be.
Notifications	Notifications to the CBUAE and Executive Office	LFIs must immediately notify the CBUAE, as well as the Executive Office, of any freezing measures and/or attempted transactions. LFIs should notify the CBUAE and the Executive Office within two (2) business days from taking any freezing measures and/or attempted transactions. For the reporting mechanism and form(s), please consult the CBUAE's and the Executive Office's websites as updated from time to time.
Annexes	Annex 1	Red flag indicators for TF and PF
	Annex 2	Lessons learned from CBUAE Supervision
	Annex 3	Synopsis of the Guidance

Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening

Effective from 8/9/2021 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework

currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies and other LFIs; and
- Insurance companies.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations ('AML-CFT Law");

(ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision"); and

(iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74").

With respect to transaction monitoring ("TM"), and as per Articles 4.2 (a) and 20 of AML-CFT Decision, LFIs are obliged to develop internal policies, controls, and procedures that are commensurate with the nature and size of their business and are approved by senior management to enable them to manage the crime risks that have been identified. They must also continuously update them. Furthermore, under Article 16 of AML-CFT Decision, LFIs must put in place indicators that can be used to identify suspicious transactions and other activity in order to file suspicious transaction reports ("STR"), suspicious activity reports ("SAR") or other report types to the UAE's Financial Intelligence Unit ("FIU). LFIs must update these indicators on an ongoing basis, in line with all applicable instructions from the UAE's supervisory authorities and FIU.

With respect to sanctions screening, and as per Article 21.2 of Cabinet Decision 74, LFIs are obliged to regularly screen their databases and transactions against names on lists issued by the UNSC and its relevant Committees (UN Consolidated List) or by the UAE Cabinet (Local Terrorist List), and also immediately when notified of any changes to any of such lists. Such screening must include regular searches of their customer databases, parties to any transactions, potential customers, beneficial owners, and persons and organizations with which the LFI has a direct or indirect relationship. LFIs must also screen their customer database before conducting any transaction, or entering into a business relationship with any person, to ensure that their name is not listed on the UN Consolidated List or the Local Terrorist List.

For more details and information, please refer to the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control's ("Executive Office") *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions*[2], the CBUAE's *Guidance for Licensed Financial Institutions on*

the Implementation of TFS, and the CBUAE's Guidance for Licensed Financial Institutions on STR[3]. LFIs should consult the CBUAE's and the Executive Office's websites as updated from time to time.

[2] Available at: https://www.uaeiec.gov.ae/en-us/un-page.
[3] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
FATF	Financial Action Task Force
FIU	Financial intelligence unit
ISIN	International Securities Identification Numbers
KYC	Know your customer
LFI	Licensed financial institution
MIS	Management information systems
ML	Money laundering
OCR	Optical character recognition
PF	Proliferation financing
SAR	Suspicious activity report
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TF	Terrorist financing
TM	Transaction monitoring
TFS	Targeted financial sanctions

2. Transaction Monitoring

An effective TM program enables LFIs to detect, investigate, and report suspicious transactions, in compliance with the UAE's legal and regulatory framework, and to ensure that the institutions' customers and transactions remain within their risk appetite. Effective TM therefore depends critically on information obtained through the application of customer due diligence ("CDD")/know your customer ("KYC") measures, including but not limited to information regarding the types of transactions in which the customer would normally be expected to engage.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship, together with the ongoing analysis of actual customer behavior and the behavior of relevant peer groups, allows the LFI to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. TM compliance personnel should escalate for priority remediation any identified omissions or inaccuracies in relevant customer or beneficial ownership information or gaps or data quality issues in required transaction or payment message fields.

An effective TM program consists of the following core elements:

- **A well-calibrated risk-based framework:** The risks LFIs face are dynamic and the transactions they carry out may be varied and high in volume. LFIs should therefore review and enhance their TM frameworks regularly and upon the occurrence of specified "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment, to ensure that they remain tailored to the institution's financial crime risks. Incorporating feedback from the personnel handling the alerts to the TM system also helps in

better calibration and tuning.

- **Robust training and risk awareness:** To ensure proper functioning and implementation of their TM programs, LFIs should ensure that personnel with TM responsibilities have adequate experience and expertise and receive role-specific training on the institution's TM policies, procedures, and risks.

- **Meaningful integration into the AML/CFT program:** LFIs should ensure that their TM systems and frameworks reinforce, and are reinforced by, the wider AML/CFT control environment of which they are a part. An effective TM program depends on the quality and completeness of data drawn from the LFI's customer and transactional systems and databases. In tandem, the outcomes of TM should inform the LFI's understanding and management of its financial crime risks, including by prompting off-cycle customer reviews and the application of enhanced scrutiny or additional controls to higher-risk customers or transactions.

- **Active oversight:** The LFIs' board and senior management should take an active role in overseeing the performance of their TM programs and the ongoing enhancement of TM systems on the basis of the institution's risks. Where the outcomes of TM are compromised by factors such as inappropriate calibration, process inefficiencies, staff issues, or system failures, it is necessary that the board (or a board-designated committee) and senior management be made aware of these issues in a timely manner so as to ensure that they are promptly and adequately remediated. The board and senior management should also communicate clear risk appetites within their institutions and set a strong tone from the top that the prevention, detection, and reporting of illegal or suspicious transactions are a priority. A quality assurance process should also play a crucial part in the TM program, by validating the review from accuracy and detail perspective. Any changes in the transaction codes or changes in the core banking system should be approved by senior management.

2.1. Risk Assessment

The design of an LFI's TM program should be informed by the LFI's risk assessment, so that TM controls are applied across the full range of risks to which the institution is exposed and enhanced scrutiny is applied to the areas of highest risk. An LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographic exposure presenting the greatest money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") risks, as well as the strength of the controls currently in place to mitigate these risks. The risk assessment serves a range of critical purposes, including but not limited to enabling an LFI to:

- understand the type of level of risk associated with its business relationships and transactions;

- develop risk-based policies, procedures and controls;

- make informed decisions with respect to resourcing and staffing;

- apply additional controls to areas of heightened risk; and

- ensure that the LFI's residual risks are within its risk appetite.

With respect to transaction monitoring specifically, the risk assessment can be used to ensure that each mode of transacting with or through the institution—domestically or internationally—is subject to a form of TM that is commensurate with its risks and is operating effectively to mitigate those risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or the legal and regulatory environment.

2.2. Risk-Based Deployment of Transaction Monitoring Controls

TM can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/TF/PF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. **LFIs with a larger scale of operations are expected to have in place automated systems** capable of handling the risks from an increased volume and variance of transactions. LFIs utilizing automated systems should perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. While **smaller LFIs may rely on TM systems that are less automated**, they should still ensure that these are appropriately executed to address the risks from their day-to-day transactional activity.

Examples of automated tools include rule- or scenario-based automated suspicious activity monitoring systems (which typically perform post-execution batch screening of transactions on a daily, weekly, monthly, and/or ad hoc schedule), automated fraud detection systems, trade surveillance systems, and automated negative news screening tools. Examples of manual tools include unusual activity or unusual transaction reporting by business-line employees (including especially, but not limited to, customer relationship managers or those otherwise in customer-facing roles), reporting of potentially suspicious activity by LFI employees (including internal whistleblower reporting), manual reviews of document-based transactions (such as documentary trade finance transactions or loans), manual negative news screening, and periodic or event-based CDD reviews.

Particularly where purely manual processes are employed, LFIs should implement appropriate training on TM policies and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. LFIs should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research. Regardless of whether automated or manual processes (or a combination of the two) are used to perform TM, it is the LFI's responsibility to demonstrate that the monitoring program is effective and appropriately risk based.

Where practicable and on a risk basis, LFIs should monitor transactions at the customer or relationship level, including across financial groups, and not only on an individual account basis, so as to obtain a complete view of a customer's transaction profile at the institution. Holistic monitoring of customers with multiple accounts is especially important for customers assessed to be politically exposed persons or as belonging to other high-risk categories.

2.3. Data Identification and Management

LFIs should have in place adequate processes to ensure that customer and transactional data feeding into their TM program (whether using manual or automated processes, or both) meets established data quality standards, that data is subject to testing and validation at risk-based intervals, and that identified data quality and completeness issues are remediated in a timely manner.

As an initial matter, LFIs should identify and document all data sources that serve as inputs into their TM program. TM data sources may include both internal customer databases, core banking or other transaction processing systems, and applicable "flat-file" databases, as well as external sources such as Society for Worldwide Interbank Financial Telecommunication ("SWIFT") message data. Source system documentation should include the identification of a system owner or primary party responsible for overseeing the quality of source data and addressing identified data issues. Where automated TM systems are used, LFIs should institute data extraction and loading processes to ensure a complete, accurate, and fully traceable transfer of data from its source to TM systems. LFIs should also ensure that staff's access rights to both source systems and TM systems are commensurate with their roles and responsibilities, so as to ensure that relevant staff can perform their duties effectively and that access is not extended to unauthorized persons or those no longer requiring system access.

Both prior to the initial deployment of a TM system or process and at risk-based intervals thereafter, LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their TM program. Data testing and validation should typically occur at minimum every 12 to 18 months, as appropriate based on the LFI's risk profile, and the frequency of such activities should be clearly mandated and documented in the LFI's policies and procedures. Such testing can include data integrity checks to ensure that data is being completely and accurately captured in source systems and transmitted to TM systems, as well as the reconciliation of transaction codes across core banking and TM systems. Testing may also utilize quantitative data quality standards or benchmarks to track data quality over time and specify a threshold or range beyond which data irregularities or other data quality issues shall require corrective action.

In addition, LFIs should put in place appropriate detection controls, such as the analysis of trends observable through management information system ("MIS") data and the generation of exception reports, to identify abnormally functioning TM rules or scenarios and ensure that any such irregularities caused by data integrity or other data quality issues are appropriately diagnosed and remediated. Where appropriate, a root cause analysis should be performed, and any findings and recommended remedial actions should be escalated to senior management to address the underlying issue in a timely manner.

2.4. Rule Definition and Pre-Implementation Testing

LFIs should employ TM detection scenarios (or "rules") that are designed to identify potentially suspicious or illegal transactions and elevate them for further review and investigation, as warranted. LFIs utilizing automated systems should perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. Transactions may be suspicious simply in virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries) or because, together with other transactions, they form a pattern that diverges from expected or historical transactional activity or may otherwise be indicative of illicit activity, including the evasion of reporting or recordkeeping requirements.

TM rules may be automated or manual and should employ value and other thresholds and parameters that take into account the specific risks and contexts of the institution, as identified in the financial crimes risk assessment, and the specific product or service and customer type involved in the transaction. To this end, LFIs should perform risk-based customer and product segmentation, so that rule parameters and thresholds are appropriately calibrated to the type of activity subject to TM. LFIs with larger transaction volumes should consider employing the use of statistical tools or methods such as above-the-line and below-the-line testing, which involves increasing and decreasing the predetermined thresholds of TM rules in a testing environment and measuring the resulting output, to better fine-tune their calibrations and reduce the volume of false-positive alerts.

In order to identify patterns of potentially suspicious or illegal activity spanning multiple transactions, LFIs should group individual TM parameters and thresholds into multi-factor risk scenarios in order to more precisely target transaction patterns and behaviors consistent with known illicit financing typologies. Key typologies and associated indicators of relevance in the context of the UAE published by the FIU are included in the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting*.[4] The use of scenarios should not be limited to LFIs with automated transaction monitoring systems, as smaller institutions with less-automated systems can and should apply the same logic in training and guiding their staff to detect these more complex risks. However, LFIs with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. In all cases, LFIs should maintain documentation that articulates the institution's current detection scenarios and their underlying assumptions, parameters, and thresholds.

Where automated systems are employed, LFIs should perform pre-implementation testing of TM rules and systems, using historical transaction data as appropriate. Such testing should include system integration testing to ensure compatibility of the TM system with source systems and other AML/CFT compliance infrastructure and user acceptance testing to ensure that the system performs as anticipated in the operating environment. Material data mapping, transaction coding, and other data quality issues, as well as irregularities in TM model performance and outputs, identified through pre-implementation testing should be prioritized for remediation and subject to re-testing prior to the deployment of a TM system.

[4] Available at https://www.centralbank.ae/en/cbuae-amlcft.

2.5. Alert Scoring and Prioritization

Consistent with a risk-based approach, LFIs may consider assigning risk-weighted scores to TM alerts in order to prioritize higher-risk alerts for expedited review. LFIs may opt to assign a higher risk score, and thus to prioritize for review and investigations, transactions that violate individual TM rules corresponding with especially heightened risks (based on the risk profile and risk appetite of the institution) as well as transactions identified as violating multiple TM rules. LFIs with larger TM alert review and investigation teams may likewise opt to allocate higher-scoring alerts to more senior investigators or those with specialized expertise in certain risk areas. In such a scenario, non-high scoring alerts could then be allocated to the staff using a "round robin" or any other technique in order to ensure a balanced and efficient distribution of alerts among staff. Although alert scoring may be used to achieve a risk-based prioritization and allocation of manually generated TM alerts, such processes may be especially useful for LFIs faced with a high volume of alerts produced by automated TM systems.

2.6. Outcomes Analysis and Management Information Systems Reporting

LFIs should document and track TM outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. Irregularities in TM system performance, including significant changes in the productivity of TM rules over time, may be indicative of underlying data quality or data integrity issues or of the need to recalibrate rule thresholds or parameters. Identified data quality or integrity issues should be reported back to designated data or owners, and apparent rule calibration issues (such as unproductive rules or those producing excessive volumes of false positive alerts) should be reported back to model owners for tuning and optimization. Where TM outcomes analysis reveals that certain transaction types or patterns are repeatedly flagged by the TM system and then consistently cleared as false positives by TM investigators, the LFI may consider employing a risk-based suppression logic or other "whitelisting" process to prevent the generation of alerts on activity repeatedly deemed not to be suspicious. Such methods, however, should not be applied to higher-risk customer or transaction types and should be carefully monitored and subject to periodic and event-driven testing, tuning, and validation, as described below.

In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their TM program, including through the provision of metrics, trends, and other MIS reporting generated by TM systems or produced by TM alert review and investigation teams. Such reporting may include an analysis of the number of alerts produced by each TM rule and the proportion of such alerts that are cleared as false positives, that require further investigation, and that ultimately result in the filing of an STR/SAR. TM-related reporting and analysis should feed back into an LFI's financial crimes risk assessment, and LFI management should use this information to ensure that the institution's customers and transaction remain within the LFI's risk appetite and that activity exceeding its risk appetite is addressed through appropriate risk mitigation measures, including but not limited to the use of account- or customer-based risk markers and/or activity, product, or service restrictions.

2.7. Post-Implementation Testing, Tuning, and Validation

On a periodic basis and in the event of material system output or operational irregularities, LFIs should reassess the functionality of TM systems and processes, including the continued relevancy of detection scenarios and assumptions and the calibration of rule threshold values and parameters. As with pre-implementation testing, post-implementation testing should include checks for system integration, data quality, and operational functionality, and should additionally include back-testing of TM rules to ensure that they remain current and effective in targeting riskier transactions and activity. Any proposed tuning or adjustment to TM rules, particularly material adjustments, should be subject to pre-implementation testing using sample or historical data to ensure the proper functioning of the new or revised rules, and should be reflected in updated TM documentation.

TM model testing and validation should be performed by individuals with sufficient expertise and appropriate level of independence from the model's development and implementation. Generally, validation should be done by people who are not responsible for the development or use of the TM model and do not have a stake in whether a model is determined to be valid. Independence may be supported by the separation of reporting lines (as where model validation is performed by an internal audit department as part of independent testing of the AML/CFT program) or by the engagement of an external party not responsible for model development or use. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

3. Sanctions Screening

As per Article 21.2 of Cabinet Decision 74, LFIs are required to perform regular searches against applicable sanctions lists of their customer databases, parties to any transactions, potential customers, beneficial owners, and persons and organizations with which the LFI has a direct or indirect relationship, as well as continuous searches of their customer database before conducting any transaction or entering into a business relationship with any person. Sanctions screening systems and processes are essential, but are also only as effective as the customer and transactional information used when comparing against applicable sanctions lists. Therefore, effectiveness depends critically on the completeness and accuracy of information obtained through the application of CDD/KYC measures and contained in payment instructions and other transactional data fields.

Sanctions compliance personnel should escalate for priority remediation identified omissions or inaccuracies in relevant customer or beneficial ownership information, as well as gaps or data quality issues in required transaction or payment message fields. On a risk basis, LFIs should perform sample testing of payment messages to ensure proper usage of message types and compliance with payment transparency requirements.

An effective sanctions screening program consists of the following core elements:

- **A well-calibrated risk-based framework:** The risks LFIs face are dynamic and the transactions they carry out may be varied and high in volume. LFIs should therefore review and enhance their sanctions screening frameworks regularly and upon the occurrence of specified "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment, to ensure that they remain tailored to the institution's financial crime risks.

- **Robust training and risk awareness:** To ensure proper functioning and implementation of their sanctions screening programs, LFIs should ensure that personnel with sanctions screening responsibilities have adequate experience and expertise and receive role-specific training on the institution's sanctions screening policies, procedures, and risks.

- **Meaningful integration into the sanctions program:** LFIs should ensure that their sanctions screening systems and frameworks reinforce, and are reinforced by, the wider sanctions control environment of which they are a part. An effective sanctions screening program depends on the quality and completeness of data drawn from the LFI's customer and transactional systems and databases. In tandem, the outcomes of sanctions screening should inform the LFI's understanding and management of its financial crime risks, including by prompting off-cycle customer reviews and the application of enhanced scrutiny or additional controls to higher-risk customers or transactions, as warranted.

- **Active oversight:** The LFIs' board and senior management should take an active role in overseeing the performance of their sanctions screening programs and driving the ongoing enhancement of sanctions screening systems on the basis of the institution's risks. Where the outcomes of sanctions screening are compromised by factors such as inappropriate calibration, process inefficiencies, staff issues, or system failures, it is necessary that the board (or a board-designated committee) and senior management be made

aware of these issues in a timely manner so as to ensure that they are promptly and adequately remediated. The board and senior management should also communicate clear risk appetites within their institutions and set a strong tone from the top that the implementation of targeted financial sanctions is a priority. A quality assurance process should also play a crucial part in the sanctions screening program, by validating the review from accuracy and detail perspective.

3.1. Risk Assessment

An LFI's risk assessment is a critical tool for ensuring that the institution has a complete, accurate, and up-to-date understanding of the sanctions risks to which their institution may be exposed, and for facilitating a risk-based approach to sanctions compliance. In the context of targeted financial sanctions, the risk-based approach cannot provide a justification for failing to apply sanctions-related controls, including sanctions screening, to *all* customer relationships and transactions, as defined below, which is a minimum legal requirement for all LFIs. Rather, the risk-based approach should be utilized by LFIs to apply additional or more rigorous controls—above the minimum legal requirement—to areas of heightened sanctions risk.

The LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographies through which the LFI is most likely to engage, directly or indirectly, with sanctioned persons, parties, countries, or regions, as well as the strength of the controls currently in place to mitigate sanctions risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment.

3.2. Risk-Based Deployment of Sanctions Screening Controls

Sanctions screening can include the manual review of customers and transactions against applicable sanctions lists, as well as the use of automated screening and interdiction software and systems. In all cases, the appropriate method of sanctions screening and the screening criteria employed should be appropriately calibrated to the sanctions risks presented by the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. Areas of heightened risk may require additional sanctions-related due diligence, more frequent or more intensive manual reviews of customers, counterparties, and their transactions, enhanced monitoring for transactions or behavior designed to evade sanctions controls, or the specialized training for sanctions compliance personnel in high-risk roles.

Sanctions screening controls should also be calibrated to the size, nature, and complexity of each institution. **LFIs with a larger scale of operations are expected to have in place automated systems** capable of handling the risks from an increased volume and variance of transactions. While **smaller LFIs may rely on sanctions screening systems that are less automated,** they should also still ensure that these are appropriately executed to address the risks from their day-to-day transactional activity, as well as fully automated for the **update of any changes to the UN Consolidated List and the Local Terrorist List**.

Examples of automated tools include automated name screening tools that compare customer databases against applicable sanctions lists, live payment and other transaction filtering tools that screen payment message and transaction data against applicable sanctions lists prior to execution, and text analytics tools that automatically convert paper documentation into electronic data that can then be screened against applicable sanctions lists.

Examples of manual tools include manual reporting and escalations of potentially sanctions-related activity by LFI employees (including especially customer relationship managers and other business-line personnel), manual reviews of document-based transactions (such as documentary trade finance transactions or loans), and periodic or event-based CDD reviews.

Particularly where purely manual processes are employed, LFIs should implement appropriate training on sanctions screening policies and procedures to ensure that personnel adhere to the internal processes for identification and

referral of potentially sanctions-related activity. LFIs should be aware of all methods of identification and should ensure that their sanctions screening program includes processes to facilitate the transfer of internal referrals to appropriate personnel for searches against applicable lists. Regardless of whether automated or manual processes (or a combination of the two) are used to perform sanctions screening, the onus is on the LFI to demonstrate that the screening program is effective and appropriately risk based.

3.3. Data Identification and Management

LFIs should have in place adequate processes to ensure that customer and transactional data feeding into their sanctions screening program (whether using manual or automated processes, or both) meets established data quality standards, that data is subject to testing and validation at risk-based intervals, and that identified data quality issues are remediated in a timely manner.

As an initial matter, LFIs should identify and document all data sources that serve as inputs into their sanctions screening program, including applicable customer databases and core banking or other transaction processing systems. Source system documentation should include the identification of a system owner or primary party responsible for overseeing the quality of source data and addressing identified data issues. Where automated sanctions screening systems are used, LFIs should institute data extraction and loading processes to ensure a complete and accurate transfer of data from its source to sanctions screening systems. LFIs should also ensure that staff's access rights to both source systems and sanctions screening systems are commensurate with their roles and responsibilities, so as to ensure that relevant staff can perform their duties effectively and that access is not extended to unauthorized persons or those no longer requiring system access.

Both prior to the initial deployment of a sanctions screening system or process and at risk-based intervals thereafter, LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their sanctions screening program. Data testing and validation should typically occur at minimum every 12 to 18 months, as appropriate based on the LFI's risk profile, and the frequency of such activities should be clearly mandated and documented in the LFI's policies and procedures. Such testing can include data integrity checks to ensure that data is being completely and accurately captured in source systems and transmitted to sanctions screening systems, as well as the reconciliation of transaction codes across core banking and sanctions screening systems. Testing may also utilize quantitative data quality standards or benchmarks to track data quality over time and specify a threshold or range beyond which data irregularities or other data quality issues shall require corrective action.

In addition, LFIs should put in place appropriate detection controls, such as the analysis of trends observable through MIS data and the generation of exception reports, to identify abnormally functioning sanctions screening logic and ensure that any such irregularities caused by data integrity or other data quality issues are appropriately diagnosed and remediated. Where appropriate, a root cause analysis should be performed, and any findings and recommended remedial actions should be escalated to appropriate senior management to address the underlying issue in a timely manner.

3.4. Screening Program Design and Pre-Implementation Testing

The process of screening information collected and maintained by an LFI on the parties it does business with and their related parties is referred to as "name screening". The concept encompasses any data set within the LFI's operations, separate from its transaction records, that may present a relevant sanctions risk indicator or be conducive to detection through screening on a periodic basis and prior to entering into a customer relationship. The process of screening a movement of value—including funds, goods, or assets— out of, into, or through the LFI between parties or accounts is referred to as "transaction screening".

Where automated systems are employed, LFIs should perform pre-implementation testing of sanctions screening systems, using historical transaction data as appropriate. Such testing should include system integration testing to ensure compatibility of the sanctions screening system with source systems and other sanctions compliance infrastructure and user acceptance testing to ensure that the system performs as anticipated in the operating

environment. Material data mapping, transaction coding, and other data quality issues, as well as irregularities in sanctions screening model performance and outputs, identified through pre-implementation testing should be prioritized for remediation and subject to re-testing prior to the deployment of a sanctions screening system.

The following sections provide additional detail about system design and pre-implementation testing as these relate specifically to name screening and transaction screening processes respectively.

3.4.1. Name Screening

As per the Executive Office's *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions*,[5] **name screening (whether automated or manual) must be performed prior to the onboarding of a customer and/or the facilitation of an occasional transaction and on an ongoing basis (at least daily) thereafter**. As indicated above, name screening encompasses any data set within the LFI's operations, separate from its transaction records, that may present a relevant sanctions risk indicator or be conducive to detection through screening on a periodic basis and prior to entering into a customer relationship.

Data relevant for name screening may include:

- Customer data, including the names and addresses of existing or prospective customers, their beneficial owners, and other related or connected parties whose information is collected pursuant to risk-based due diligence procedures;
- Employee data, including employee names and addresses;
- Third-party service provider data, including the names, addresses, and beneficial owners of an LFI's vendors, landlords, and tenants, as applicable;
- International Securities Identification Numbers ("ISINs") and other sanctions-relevant identifying features of assets held in custody by the LFI; and
- Recipients of the LFI's corporate donations or sponsorship.

Not all data elements within an LFI's records are relevant for sanctions screening. When determining what reference data should be screened, an LFI should identify the data within its operations and records that is relevant to sanctions risk, determine how it is relevant, ensure it is conducive to effective screening, and differentiate it from data that is not relevant or suitable to screening. For example, the names of individuals and entities with whom the LFI has a relationship are relevant for screening against name-based sanctions lists but not for geographic (region- or country-based) sanctions programs. Likewise, while the data contained in the addresses of such individuals and entities may not be directly relevant for *screening* against name-based sanctions lists, this data may assist in differentiating a true name match from a false name match when *reviewing* apparent name screening hits.

An LFI should also define other data elements (such as date of birth, nationality, and place of birth) that may be relevant for sanctions screening in some situations but not others. Date of birth, for example, is relevant as a distinguishing factor to assess a potential or a true match from a false match on an individual and might be used for screening in combination with another attribute, such as a name. In each case, LFIs should weigh up the relative incremental value of screening the data element against the reliability of the data and whether an alert against the data will meaningfully assist in detecting or preventing a sanctions risk that would not be reasonably detected through other controls, or by screening different data attributes. The screening criteria used by LFIs to identify name variations and misspellings should be based on the level of sanctions risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high volume of transactions, the LFI's interdiction software should be able to identify close name derivations for review.

An LFI's reference data is typically maintained in electronic files and is most effective when screened through an automated process and repeated at defined intervals. The use of manual screening can be considered when the risk

is sufficiently low and where the reference data cannot be sourced reliably, either electronically or in a format necessary for automated screening. For example, if an LFI has identified only a small population of names requiring screening, it may choose to forego investing in an automated screening system and instead manually input these names into an online screening filter.

[5] Available at: https://www.uaeiec.gov.ae/en-us/un-page#.

3.4.2. Transaction Screening

LFIs should screen all payments prior to completing the transaction (also referred to as "real-time" screening), utilizing all transaction records necessary to the movement of value between parties and at a point in the transaction where detection of a sanctions risk is actionable to prevent a violation. The LFI should then identify which attributes within those records are relevant for sanctions screening and the context in which they become relevant. As with name screening, names of parties involved in a transaction are relevant for list-based sanctions programs, whereas addresses are more relevant to screening against geographic sanctions programs but can be used as identifying information to help distinguish a potential or true match from a false match under a list-based program. Other data elements, such as bank identification codes, may be relevant for both list-based and geographic sanctions programs.

Some data elements are more relevant for sanctions screening purposes when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. Where automated controls alone may not be capable of detecting both factors simultaneously, manual review of the associated activity may be required alongside review to confirm a true match to applicable sanctions lists. In addition, certain data elements offer little or no risk mitigation through screening, for example, amounts, dates, and transaction reference numbers have no relevance from a screening perspective, although they may be relevant for TM or other risk management purposes.

Data relevant for transaction screening may include:

- The parties involved in a transaction, including the originator and beneficiary;
- Agents, intermediaries, and financial institutions involved in a transaction;
- Bank names, Bank Identifier Codes ("BICs"), and other routing codes;
- Free text fields, such as payment reference information or the stated purpose of the payment in Field 70 of a SWIFT message;
- ISINs or other risk-relevant product identifiers, including those that relate to sectoral sanctions identifications within securities-related transactions, as applicable;
- Trade finance documentation, including any:
    - Importers and exporters, manufacturers, drawees, drawers, notify parties, and signatories;
    - Shipping companies, vessel names and International Maritime Organization (IMO) numbers, names of parties associated with the vessel (including ship owners, charterers, and captains), and freight forwarders;
    - Facilitators, such as insurance companies, agents, and brokers; and

- Financial institutions, including issuing, advising, confirming, negotiating, claiming, collecting, reimbursing, and guarantor banks.

- Geographic details, including:
  - Addresses, countries, cities, towns, regions, ports, and airports (e.g., as contained within SWIFT Fields 50 and 59 or acquired through vessel tracking inquiries);
  - Phone or fax numbers and web addresses, insofar as these contain geographic or other relevant details;
  - Place of taking in charge, receipt, dispatch, delivery, or final destination;
  - Country of origin, destination, and transshipment of goods or services; and
  - Airport of departure or destination.

Transaction screening should be performed at a point in time where a transaction can be stopped and before a potential violation occurs. This typically occurs at a number of points in the lifecycle of a transaction, but certainly prior to executing any commitment to move funds. Particular attention should be directed to any points within the transactional process where relevant information could be changed, modified, or removed in order to undermine screening controls.

Transactional records are typically found in large volumes and within business processes predicated on speed of execution. These transaction types are generally in electronic form and conducive to systemic, automated screening. Some transaction types, however, still rely on documentation in various formats and varying methods of presentation. LFIs may employ text analytics tools such as optical character recognition ("OCR") that automatically convert paper documentation into electronic data that can then be screened against applicable sanctions lists, but some paper-based transactions, such as documentary trade finance transactions, may require manual screening processes, where relevant information is physically added into a system for screening. OCR requires quality assurance validation to ensure the information has been captured fully and accurately. Certain paper-based transactions, such as paper cheque clearing, where the volumes can be high and the manual screening process creates high rates of errors, may rely on controls other than screening, such as CDD/KYC processes, where the sanctions risks for the product are assessed as being low.

3.5. List Management

Under Article 21.2 of Cabinet Decision 74, LFIs' sanctions screening lists must include all names on lists issued by the UNSC and its relevant Committees (UN Consolidated List) or by the UAE Cabinet (Local Terrorist List). LFIs' sanctions screening processes should also include searches for entities that are not themselves listed but that are owned or controlled mainly or fully by a listed person (also referred to as "shadow listed persons"). LFIs cannot conduct transactions with shadow listed persons and must freeze any funds or assets of a shadow listed person that they may hold as per Article 15 of Cabinet Decision 74. Although shadow designated persons, by their very nature, are not listed by government authorities, LFIs should develop internal lists of such persons based on their own due diligence and consideration of external sources, such as adverse media reporting. LFIs should include such a list, together with any other internal lists (such as lists of customers exited for financial crime concerns) in its sanctions screening systems and processes.

Given the dynamic nature of targeted financial sanctions, LFIs should establish and implement sanctions list management procedures that enable the institution's sanctions screening program to adjust rapidly to changes published by sanctions authorities. The following considerations are relevant to effective list management, and each should be documented and reviewed on a regular basis, to ensure that the LFI's chosen approach remains in line with its risk appetite and in compliance with applicable legal requirements:

- **List selection:** The LFI should determine which sanctions lists are relevant for screening. Lists must include, at a minimum, all names on the UN Consolidated List and the Local Terrorist List, but may also include other jurisdictional lists as well as internal lists of persons known to have a sanctions nexus, lists of geographic terms (such as cities, regions, and ports), banking terms (such as BICs), and lists of prohibited goods or prohibited securities, where applicable. Although lists issues by the UNSC or by the UAE Cabinet must be employed in the screening of all customers and transactions, as outlined above, other lists may be employed on a risk basis. For example, screening against lists of prohibited goods may be limited to the context of trade finance transactions, whereas such transactions likely would not need to be screened against sanctioned securities.

- **Sourcing of lists:** The LFI should determine which lists are to be generated internally and which lists are best sourced from external vendors, and the processes for generating and implementing such lists.

- **List maintenance:** The LFI should determine the processes for adding and removing lists or entries on internal lists, where screening is no longer required or where the result is within the institution's risk appetite. The LFI should identify and implement appropriate controls to ensure that lists remain up to date and that only appropriate individuals can add or remove lists or list entries.

- **Data enhancement:** The LFI should determine whether certain list entries should be modified or enhanced based on additional information.

- **Whitelisting:** The LFI may consider establishing and maintaining a "white list" of customer names or other data elements that have already been flagged and cleared through thorough due diligence by the LFI as false positives. These "white lists" may be used to improve the process related to screening by leveraging the results of past due diligence and reducing the number of false positives. While the LFI should not overly rely on such a list, and must diligently and continuously screen customers and transactions in case they are implicated in the updated UN Consolidated List and Local Terrorist List, the use of such a "white list" may assist the LFI in expediting the dispositioning in case of repeated false positive matches. LFIs should have documented procedures to managing and periodically reviewing and updating those "white lists" to account for the possibility that persons on a whitelist may later become sanctioned persons. Where automated screening tools are employed, the LFI should determine the management of rules for automatically eliminating potential hits caused by the interaction of certain list terms and frequently encountered data. Where manual screening processes are employed, the LFI should establish a process for manually reviewing potential hits against the whitelist.

- **Geographic scope of application:** Where the LFI has operations in multiple jurisdictions, the LFI should determine which lists should be screened in all jurisdictions of an LFI's operations and which, if any, could be screened only within a certain jurisdiction or several jurisdictions.

- **Exact matching versus "fuzzy logic":** The LFI should determine which lists should be deployed within the screening filter on an exact match basis, and which should use fuzzy matching (i.e., an algorithm-based technique to match one name or other string of words where the content of the information being screened is not identical—but its spelling, pattern, or sound is a close match—to the contents on a list used for screening).

- **Frequency of screening:** The LFI should determine the frequency or the triggers for static data screening, so as to account for additions to lists and changes in customer data.

List management procedures should be documented and subject to periodic review to ensure that list management practices remain aligned to the LFI's risk profile and risk appetite.

3.6. Outcomes Analysis and Management Information Systems Reporting

LFIs should document and track sanctions screening outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. Irregularities in sanctions screening system performance, including significant changes in the volume of apparent matches to sanctions lists over time, may be indicative of underlying data quality or data integrity issues or of the need to recalibrate sanctions screening search logic. Identified data quality or integrity issues should be reported back to designated data owners, and apparent screening logic issues should be reported back to model owners for tuning and optimization.

In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their sanctions screening program, including through the provision of metrics, trends, and other MIS reporting generated by sanctions screening systems or produced by sanctions screening alert review and investigation teams. Such reporting may include an analysis of the number and type of screening hits and the proportion of apparent matches that are cleared as false positives compared to those that are confirmed as potential or true matches. Sanctions screening-related reporting and analysis should feed back into an LFI's financial crimes risk assessment, and LFI management should use this information to ensure that the institution's customers and transaction remain within the LFI's risk appetite and that activity exceeding its risk appetite is addressed through appropriate risk mitigation measures, up to and including account activity restrictions and customer exit.

3.7. Post-Implementation Testing, Tuning, and Validation

On a periodic basis and in the event of material system output or operational irregularities, LFIs should reassess the functionality of sanctions screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process. Any proposed material adjustments to sanctions screening search logic should be subject to pre-implementation testing using sample or historical data to ensure the proper functioning of the new or revised logic, and reflected in updated sanctions screening documentation.

Sanctions screening model testing and validation should be performed by individuals with sufficient expertise and appropriate level of independence from the model's development and implementation. Generally, validation should be done by people who are not responsible for the development or use of the sanctions screening model and do not have a stake in whether a model is determined to be valid. Independence may be supported by the separation of reporting lines (as where model validation is performed by an internal audit department as part of independent testing of the sanctions compliance program) or by the engagement of an external party not responsible for model development or use. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.

4. Program Governance and Oversight

The following sections outline program governance expectations relating to TM and sanctions screening systems and processes.

4.1. Oversight, Management Reporting, and Auditing

The LFI's board of directors and senior management should exercise active oversight of the institution's key financial crimes risks and the controls in place to mitigate those risks. The board (or a board-designated committee) and senior management should receive regular reports on the institution's key risks and trends and the overall performance of AML/CFT and sanctions controls, and should review the institution's financial crimes risk assessment, any AML/CFT and sanctions audit and regulatory reports, and the institution's written AML/CFT and

sanctions program. The AML/CFT and sanctions program should be subject to senior management approval, and the board and senior management should ensure that clear, current, and appropriate policies and procedures are put in place and that there are effective TM and sanctions screening systems supported by adequate internal expertise and resources.

TM and sanctions screening functions should be given clear and distinct responsibilities for their respective tasks in the TM and sanctions screening process chain (e.g., for alert handling and the filing of STRs/SARs). Additionally, as detailed above, LFIs are expected to implement effective reporting systems, to include quantitative MIS report as well as qualitative analysis of key risks and trends as appropriate, to ensure that their board and senior management are updated on key financial crimes risks in a timely manner. Any data quality or system functionality or output issues should be documented and tracked, and the status of remedial actions should be reported regularly to senior management.

TM and sanctions screening programs should be subject to independent testing by internal or external auditors with sufficient technological expertise and understanding of ML/TF/PF and sanctions risks and requirements. The LFI's independent testing function (whether internal or external) should ensure adequate TM and sanctions screening coverage of the LFI's customers, products, services, delivery channels, and geographies and may perform model testing and validation, as detailed above, as part of its AML/CFT and sanctions independent testing plan and methodology; otherwise, model testing and validation should be performed at periodic, risk-based intervals by a qualified and independent third party.

4.2. Use of Vendors and Other Third Parties

LFIs may use externally provided TM or sanctions screening services and other third-party providers to fulfil their legal and regulatory obligations to monitor and screen their customers and transactions. However, LFIs are ultimately responsible for complying with AML/CFT and sanctions requirements, even if they choose to use third-party models to assist with their compliance obligations.

The selection of third-party system or service should be guided by the LFI's size, geographic footprint, business and technology environments, and financial crimes risks, as well as functional requirements, such as the volume of data to be screened, the degree to which TM and sanctions screening processes will be centralized across business lines within the LFI, the nature of existing data integrity processes, and the ability of the application to integrate effectively within an LFI's technological infrastructure. When selecting a vendor, LFIs should require the vendor to provide developmental evidence explaining the product components, design, and intended use, so as to determine whether the model is appropriate for the LFI's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic. LFIs should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

LFIs are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the LFI may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by an LFI for its particular circumstances. An LFI's customization choices should be documented and justified as part of validation. If vendors provide input data or assumptions, or use them to build models, their relevance for the LFI's situation should be assessed. LFIs should obtain information regarding the data used to develop the model and assess the extent to which that data is representative of the LFI's situation. The LFI also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the LFI's own outcomes. Systematic procedures for validation help the LFI to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of an LFI's operations. It is also very important for the LFI to have as much knowledge in-house as possible, in case the vendor or the LFI terminates the contract for any reason, or if the vendor is no longer in business. LFIs should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

4.3. Role-Specific Training

LFIs should ensure that personnel responsible for performing TM and sanctions screening roles receive training that covers key financial crimes risks faced by the institution (such as common ML/TF/PF or sanctions evasion typologies), complex and higher-risk customer and transaction types relevant to TM and sanctions screening processes, applicable legal and regulatory requirements, and internal policies, procedures, and processes. Training should be tailored to each individual's specific responsibilities and include desktop procedures or instructions for the use of any TM or sanctions screening systems or other technology relevant to the individual's role.

An LFI's TM and sanctions screening training should be based on an assessment of the institution's training needs, incorporated into wider AML/CFT and sanctions training plans and programs, and subject to completion tracking and escalation procedures to ensure timely completion of mandatory training by all relevant personnel. Mandatory training should also be extended to any staff located abroad whose responsibilities cover accounts booked in or activity flowing into, out of, or through the UAE.

4.4. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, copies of personal identification documents, including STRs/SARs and results of any analysis performed. LFIs must maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions.

Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guide is to assist the understanding and effective performance by CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE relating to the design, implementation, and maintenance of effective transaction monitoring and sanctions screening programs.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies and other LFIs as well as insurance companies.
Transaction Monitoring	Risk Assessment	An LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographic exposure presenting the greatest money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") risks, as well as the strength of the controls currently in place to mitigate these risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the

		occurrence of "trigger events" such as material changes in the LFI's business or risk profile or the legal and regulatory environment.
	Risk-Based Deployment of TM Controls	In all cases, the type and degree of monitoring should appropriately match the ML/TF/PF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. Where practicable and on a risk basis, LFIs should monitor transactions at the customer or relationship level, including across financial groups, and not only on an individual account basis, so as to obtain a complete view of a customer's transaction profile.
	Data Identification and Management	LFIs should identify and document all data sources that serve as inputs into their TM program. LFIs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into their TM program. In addition, LFIs should put in place appropriate detection controls, such as the analysis of trends through management information systems (MIS) data and the generation of exception reports, to identify abnormally functioning TM rules or scenarios and ensure they are appropriately diagnosed and remediated.
	Rule Definition and Pre-Implementation Testing	LFIs should employ TM detection rules or scenarios that are designed to identify potentially suspicious or illegal transactions and elevate them for further review and investigation, as warranted. To this end, LFIs should: ▪ Perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes; ▪ Perform risk-based customer and product segmentation, so that rule parameters and thresholds are appropriately calibrated; ▪ Consider employ statistical tools or methods such as above-the-line and below-the-line testing, to better fine-tune their calibrations and reduce the volume of false-positive alerts; and ▪ Perform pre-implementation testing of TM rules and systems to ensure compatibility of the TM system with source systems and other AML/CFT compliance infrastructure to ensure that it performs as anticipated in the operating environment.
	Alert Scoring and Prioritization	LFIs may consider assigning risk-weighted scores to TM alerts in order to prioritize higher-risk alerts for expedited review. LFIs with larger TM alert review and investigation teams may likewise opt to allocate higher-scoring alerts to more senior investigators or those with specialized expertise in certain risk areas.
	Outcomes Analysis and MIS Reporting	LFIs should document and track TM outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. In addition, LFIs should ensure that senior management is regularly updated on the performance and output of their TM program, including through the provision of metrics, trends, and other MIS reporting.
	Post-Implementation Testing, Tuning, and Validation	On a periodic and event-driven basis, LFIs should reassess the functionality of TM systems and processes, including the continued relevancy of detection scenarios and assumptions and the calibration of rule threshold values and parameters. TM model testing and validation should be performed by individuals with sufficient

		expertise and appropriate level of independence from the model's development and implementation. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.
Sanctions Screening	Risk Assessment	The LFI's risk assessment should include, at a minimum, an assessment of the customers, products and services, delivery channels, and geographies presenting the greatest sanctions risks, as well as the strength of the controls in place to mitigate these risks. The risk assessment should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the LFI's business or risk profile or its legal and regulatory environment.
	Risk-Based Deployment of Sanctions Screening Controls	Sanctions screening programs should be appropriately calibrated to the sanctions risks presented by the institution's customers, products and services, delivery channels, and geographic exposure and may vary across an LFI's business lines or units, where applicable. Sanctions screening controls should also be calibrated to the size, nature, and complexity of each institution. LFIs should apply additional or more rigorous sanctions controls—such as enhanced customer or transactional due diligence, increased monitoring for sanctions evasion, and specialized training for personnel in high-risk roles—to areas of heightened sanctions risk.
	Data Identification and Management	LFIs should identify and document all data sources that serve as inputs into their sanctions screening program and test and validate the integrity, accuracy, and quality of data flowing into their sanctions screening program. In addition, LFIs should put in place appropriate detection controls, such as MIS trends analysis and exception reports, to identify abnormally functioning screening logic to ensure such irregularities are appropriately diagnosed and remediated.
	Screening Program Design and Pre-Implementation Testing	LFIs should perform pre-implementation testing of screening systems to ensure compatibility with source systems and other sanctions compliance infrastructure to ensure it performs as anticipated in the operating environment. Name screening (whether automated or manual) must be performed prior to the onboarding of a customer and/or the facilitation of an occasional transaction and on an ongoing basis (at least daily) thereafter. LFIs should screen all payments prior to completing the transaction (also referred to as "real-time" screening), utilizing all transaction records necessary to the movement of value between parties. Transaction screening should be performed at a point in time where a transaction can be stopped and before a potential violation occurs.
	List Management	LFIs should establish and implement sanctions list management procedures that enable the institution's sanctions screening program to adjust rapidly to changes published by sanctions authorities. List management procedures should be documented and subject to periodic review to ensure that list management practices remain aligned to the LFI's risk profile and risk appetite.
	Outcomes Analysis and MIS Reporting	LFIs should document and track screening outputs in order to identify and address any technical or operational issues and understand key risks or trends over time. In addition, LFIs should ensure that senior management is regularly updated on the

		performance and output of their screening program, including through the provision of metrics, trends, and other MIS reporting.
	Post-Implementation Testing, Tuning, and Validation	On a periodic and event-driven basis, LFIs should reassess the functionality of sanctions screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process. Sanctions screening model testing and validation should be performed by individuals with sufficient expertise and level of independence. All model validation activities and identified issues should be clearly documented, and management should take prompt action to address model issues.
Program Governance and Oversight	Oversight, Management Reporting, and Auditing	LFIs'board (or board-designated committee) and senior management should receive regular reports on the key risks and trends and overall performance of the AML/CFT and sanctions controls. TM and sanctions screening functions should be given clear and distinct responsibilities for their tasks. TM and sanctions screening programs should be subject to independent testing by internal or external auditors.
	Use of Vendors and Other Third Parties	LFIs may use externally provided TM or sanctions screening services. However, LFIs are ultimately responsible for complying with AML/CFT and sanctions requirements. Systematic procedures for validation help the LFI to understand the vendor product and its capabilities, applicability, and limitations.
	Role-Specific Training	LFIs should ensure that TM and sanctions screening personnel receive role-specific training that covers key financial crimes risks, complex and higher-risk customer and transaction types, applicable legal and regulatory requirements, internal policies, procedures, and processes.

Guidance for Licensed Financial Institutions Providing Services to Cash-intensive Businesses

Effective from 27/9/2021 **Status:** In-Force

1. Introduction

1.1 Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or

supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.2 Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

1.3 Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations ("AML-CFT Law").

- Cabinet Decision No. (10) of 2019 Concerning the Implementation Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations ("AML-CFT Decision").

1.4 Definitions

Bearer Negotiable Instruments: Financial instruments of whatever form, whether in the form of a bearer document, such as: traveler's cheques; promissory notes and cheques, payment orders, or others. These instruments may either be in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; or may be incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee's name omitted.

CBUAE Regulations: Any resolution, regulation, circular, rule, instruction, standard or notice issued by the Central Bank.

Cash Couriers: Natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another.

Cash or Currency: Banknotes and coins that are legal tender in circulation as a medium of exchange.

Cross-Border Transportation of Currency or Bearer Negotiable Instruments: Any in-bound or outbound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (1) physical transportation by a natural person, or in that person's accompanying luggage or vehicle; (2) shipment of currency through containerized cargo; or (3) the mailing of currency or bearer negotiable instruments by a natural or legal person.

Predicate Offense: Any act constituting a felony or misdemeanor under the applicable laws of the UAE whether this act is committed inside or outside the UAE when such act is punishable in both countries.

2. Understanding Risks

2.1 Vulnerabilities of Cash

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that, as the UAE is a cash-intensive economy and plays an important part in global trade, there are significant risks associated with the cross-border movement of cash and bearer negotiable instruments, including bulk-cash smuggling that is associated with third-party money laundering risks.

As a major medium of exchange in the UAE, cash is particularly vulnerable to abuse by illicit actors to conduct money laundering activities and finance criminal activities. The specific characteristics of cash-anonymity, interchangeability, and transportability—make it an attractive method by illicit actors seeking to conceal the proceeds of crime. Unlike other monetary instruments, such as credit cards or wire transfers, cash holds no record of its source or owner, and can be easily concealed in large quantities upon which it is difficult to trace once spent. Cash transactions are also instantaneous and widely accepted across jurisdictions.

Criminal activity—or a predicate offense—is often cash based. A predicate offense for money laundering is the underlying criminal activity that generates proceeds. Criminals then seek to "launder" these illicit proceeds, which leads to the offense of money laundering. The FATF Recommendations identify "designated categories of offenses"[2] as the following:

- Participation in an organized criminal group and racketeering;
- Terrorism, including financing of terrorism and illegal organisations;
- Trafficking in human beings and migrant smuggling;
- Sexual exploitation, including sexual exploitation of children;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit arms trafficking;
- Illicit trafficking in stolen and other goods;
- Corruption and bribery;
- Fraud;
- Counterfeiting currency;
- Counterfeiting and piracy of products;
- Environmental crime;
- Murder, grievous bodily injury;
- Kidnapping, illegal restraint, and hostage-taking;
- Robbery or theft;
- Smuggling;
- Tax crimes;
- Extortion, Forgery;
- Piracy and
- Insider trading and market manipulation.

However, as the FATF expects countries to include the above-mentioned list at the minimum, the UAE's definition of Predicate Offense is broader to include **any act** constituting a felony or misdemeanor under the applicable laws of the UAE, whether this act is committed inside or outside the UAE when such act is punishable in both countries.

---

[2] Available at https://www.fatf-gafi.org/glossary/d-i/

2.2 Vulnerabilities of Alternatives to Cash

Illicit actors also use various monetary instruments in conjunction with, or as a replacement to, cash. Both bearer negotiable instruments and prepaid cards for instance offer similar benefits to cash, including anonymity and accessibility. They can store large amounts of value in a compact physical size that makes them potentially vulnerable to abuse by illicit actors who use them instead of cash to make physical cross-border transportations of value. Illicit actors seeking to avoid an LFI's identification and verification requirements can exploit the ease of payment offered by bearer negotiable instruments and prepaid cards for the purpose of moving their proceeds—thus obscuring the origin of the funds—and converting them to payments for other goods or services. This may also include obtaining funds in one jurisdiction and having access to cash withdrawals in another jurisdiction. Additional characteristics and associated vulnerabilities of bearer negotiable instruments and prepaid cards are discussed below.

2.2.1 Bearer Negotiable Instruments

Bearer negotiable instruments are financial instruments of whatever form, whether in the form of a bearer document, such as traveler's cheques, promissory notes and cheques, payment orders, or other forms that can be attractive to illicit actors as alternatives to cash. Bearer negotiable instruments provide the opportunity to move large amounts of funds in bearer form without the bulkiness of cash. They are transferable documents that provide unconditional guarantees of cash payments either on demand or at a future date. The individual who issues a negotiable instrument is known as the 'payer' or 'issuer,' and the person who receives a negotiable instrument is known as the 'bearer' or 'payee'.

Bearer negotiable instruments often include the instruction 'pay to the bearer', meaning the bearer would be the person in physical possession of the instrument. The risk, in this scenario, is that the holder is a criminal and/or not the intended payee of the negotiable instrument. Bearer negotiable instruments are also unique in that they can also be easily transferred from one party to another, which effectively obscures the paper trail on the 'payer' or 'issuer', and enables illicit actors to distance the proceeds of crime from the illegitimate source. **LFIs should seek to mitigate these risks by continuing accepting cash and third party cheques as long as the due diligence measures regarding the person presenting the cheque have been duly conducted by the LFI.**

2.2.2 Prepaid Cards

Prepaid cards can be used as an alternative to cash in that they provide access to funds that have been paid in advance. Funds can be claimed or transferred through an electronic device, such as through a card, code, electronic serial number, mobile identification number, or personal identification number within either an "open" or "closed" loop system:

- "Open loop" prepaid cards can be used for purchases at any merchant where that brand of the card is accepted and offers access to cash at any automated teller machine ("ATM") that connects to the affiliated ATM network. Some prepaid cards may be reloaded, allowing the cardholder or third-party (such as an employer) to add value to the card. For example, a travel card can allow cardholders to top up at various locations, including online and at kiosks, and then allows cardholders to utilize the card to purchase local travel as well as goods or services at various participating stores.

- "Closed loop" prepaid cards generally can only be used to buy goods or services from the issuing merchant of the card or a select group of merchants that participate in that specific network. These cards generally do not allow for cash access, although they can often be re-sold through third-party websites in exchange for other closed loop cards or payments. For example, a chain of coffee shops may offer reloadable cards that can only be used to purchase goods at the coffee shop.

Prepaid cards can be abused by illicit actors seeking to launder money and finance terrorist activities. For instance, both open and closed loop prepaid cards can be utilized in conjunction with, or as a replacement to, bulk cash smuggling. Specifically, drug traffickers have been known to convert cash derived from narcotic sales to prepaid debit cards, which they then use to purchase goods and services or send to narcotic suppliers, who in turn use the cards to withdraw cash from an ATM. In addition, funds can be loaded onto prepaid cards in support of terrorist activities, such as purchasing various products and services whether buying a terrorist a plane ticket or providing other resources (e.g. car rental or hotel) to support a terrorist group.

When assessing the risks associated with prepaid cards, LFIs should consider the specific risks posed by the features and functionalities of the monetary instrument. If the cardholder is anonymous, or if the holder or purchaser provides false information on their identity for instance, the money laundering and financing of terrorism and illegal organisations risks are higher. In addition, LFIs should evaluate the risks associated with cash access, and the volume and velocity of funds that can be loaded and retrieved on prepaid cards. Further risk factors include type and frequency of loads and transactions, geographic location where the transaction activity occurs, value limits, distribution channels, and the nature of funding sources.

2.3 Vulnerabilities of Cash-Intensive Businesses

2.3.1 Types of Cash-Intensive Businesses

Cash-intensive businesses are businesses that experience a high volume of cash flows. However, because cash-based transactions are inherently difficult to trace, as discussed above, cash-intensive businesses may potentially be used as vehicles for money laundering and the financing of terrorism and illegal organisations. Businesses that generate a large volume of cash revenue may be susceptible to abuse by illicit actors that integrate the proceeds of crime into the banking system under the guise of legitimate business. In particular, they may exploit cash-intensive businesses for money laundering and the financing of terrorism and illegal organisations by using cash-intensive business to:

- Provide a front to launder large amounts of cash and reinvest cash proceeds of crime in the economy;
- Co-mingle illicit and legitimate income; and
- Finance, though often through small amounts of cash, terrorist activities without traceability.

Cash-intensive businesses span across various industry sectors. Most of these businesses are operating a legitimate business; however, some aspects of these businesses may be vulnerable to money laundering or the financing of terrorism and illegal organisations. Examples of cash-intensive businesses include but are not limited to the following:

- Convenience stores;
- Retail stores;
- Restaurants;
- Wholesale or general trading businesses;

- Travel agencies and tour operators; and
- Car dealers.

In addition, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to the Real Estate and the Precious Metals and Stones sector*[3] for further information.

LFIs may expand on the above by considering additional factors when identifying cash-intensive businesses in their customer base. For example LFIs can define cash-intensive businesses based on specific criteria, such as a proportion or more of the business' revenue is in cash or the business has a monthly revenue in cash above a certain threshold. In either scenario, the definition of cash-intensive business should be determined by the LFI, justified by a sound methodology that considers various factors including risk and characteristics, documented in the LFI's policies and procedures, and approved by the LFI's senior management.

The LFI should monitor whether the cash-intensive business appears to generate unusual transactions compared to the business' expected activity and profile, and with other similar cash-intensive businesses. For example, a small business making significantly larger amounts of cash deposits than other businesses of a similar size in the same industry should be reviewed for potential money laundering activity. The extent of the vulnerability presented by cash-intensive businesses may be particularly severe due to large volumes of cash transactions, limited record keeping, and high customer turnover. LFIs should therefore understand the nature and purpose of the business relationship and expected activity of the customer in order to identify types of transactions that appear to be unusual, potentially suspicious, and/or inconsistent with the customer's profile and stated purpose of the account.

The following sections examine common features of cash-intensive businesses that impact risk. **LFIs should consider the specific risks posed by these features to determine whether the customer is considered as high-risk and should be subject to enhanced due diligence ("EDD") measures.** LFIs should incorporate this assessment into their AML/CFT program and update their policies, procedures, and processes with the aim to detect illicit activity and manage illicit financing risks.

---

[3] Available at https://www.centralbank.ae/en/cbuae-amlcft

2.3.1.1 Cross-Border Movement of Cash and Cash Couriers

Cash-intensive businesses may move cash across borders as part of their business model. Cross-border movement of licit cash can be legal, subject to compliance with reporting and other relevant legal and regulatory requirements. However, criminals may also seek to move cash across borders; according to FATF, the physical transportation of cash across an international border is *"one of the oldest and most basic forms of money laundering"* and is still widely used today.[4] The criminal economy tends to be cash-based with illicit proceeds of crime moving quickly and anonymously, including across borders. Illicit actors often choose to remove their illicit assets from a bank account in order to obscure the audit trail by transporting it to another country where they can spend the cash on goods or services or reintroduce the cash into the financial system. Illicit actors who generate cash proceeds also seek to move their profits to jurisdictions that will allow the placement of cash into the legal economy without detection. Their selection of a jurisdiction can be driven by the predominant use of cash in that jurisdiction, the weaker AML/CFT controls of a jurisdiction's financial system including few or no restrictions on cash payments, or a jurisdiction's reputation as a banking secrecy haven. Illicit actors can exploit the high volume of passenger, cargo, and mail movements into and out of jurisdictions to move cash without attracting the attention of authorities.

Cash-intensive businesses may utilize cash couriers to move cash across borders. Cash couriers are natural persons who physically transport currency and bearer negotiable instruments on their person or accompanying luggage from one jurisdiction to another. Couriers may be directly involved in the underlying crime or may be third parties recruited specifically to move money to another jurisdiction. Mechanisms to conceal the cash include within pieces of clothing on the physical persons (such as a money belt), hidden within luggage, or even concealed internally. Cash

couriers may use air, sea, or rail transport to cross an international border and typically use high denomination banknotes as part of their transportation, which decreases the size and bulk of low denomination banknotes.

Specifically, cross-border movements of cash across an international border are used to:

- Launder proceeds of crime by placing them in another jurisdiction, typically with weaker AML/CFT controls.
- Move illicit value to purchase assets that can hold considerable value, such as luxury goods, or transfer the value of the funds for them to be stored.
- Hide proceeds from authorities and complicate asset recovery.

It is not illegal to move cash into or out of the UAE. However, natural or legal persons must declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold of AED 60,000. The relevant extract of the Regulation on the Declaration of Currencies, Bearer Negotiable Instruments, and Precious Metals and Stones in Possession of Travelers Entering or Leaving the UAE (issued in the Official Gazette No 703 dated 31/05/2021) is in the box below.

Article (8) of Federal Decree-Law No. (20) of 2018 on Anti Money Laundering and Combating the Financing of Terrorism and the financing of Illegal Organizations stipulates that (when entering or leaving the country, any person must declare the currencies or bearer negotiable financial instruments, precious metals or stones of value, in accordance with the declaration regulation issued by the Central Bank).

Accordingly, the Board of Directors of the Central Bank has decided that the maximum threshold for currencies, bearer negotiable instruments, and precious metals and stones, shall be in accordance with the table below, and shall apply to all forms of physical cross-border transportation, whether by travelers or through mail and cargo. Bearer negotiable instruments mean financial instruments of whatever form, whether in the form of a bearer document, such as travelers checks, promissory checks, payment orders, or others. Based on the above, any natural or legal person shall declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold specified in the table and shall provide an honest and clear answer and adequate information to the Customs authority and its staff upon request. Declarations shall also be made for currencies, bearer negotiable instruments, precious metals or stones of a value exceeding the specified threshold crossing the border through cargo, mail or shipments transported using transport service companies using the official customs systems of the UAE.

Maximum threshold for currencies, bearer negotiable instruments, and precious metals and stones	
Currencies/Instruments/Metals/ Precious stones	**Threshold above which declaration is required**
1. Currencies (UAE Dhrs or equivalent in other currencies)	UAE Dhrs 60,000 or equivalent in any other currencies
2. Any type of bearer negotiable instruments	UAE Dhrs 60,000 or equivalent in any other currencies
3. Precious metals with high economic value in any form, type or classification, provided they are not intended for commercial purposes or transported by a traveler that engages in the same trade or a traveler that transports such materials as a profession and frequently visits the department or the customs port.	UAE Dhrs 60,000 or equivalent in any other currencies
4. Precious stones with high economic value in any form, type or classification, provided they are not intended for commercial purposes or transported by a traveler that engages in the same trade or a traveler that transports such	UAE Dhrs 60,000 or equivalent in any other currencies

materials as a profession and frequently visits the department or the customs port.	

Understanding whether customers have made any such declarations, in accordance with the Regulation should form part of any due diligence by the LFIs where required. As part of due diligence, LFIs may require additional information on the customer or the transaction, including the source of funds and relevant documentation.

Potential Risk Indicators:

- Transactions involving locations or customers originating from locations with poor AML/CFT regimes or high exposure to corruption.
- Significant and/or frequent cash deposits or currency exchanges made over a short period of time.
- Customer is in possession of money supposedly for business reasons while travelling to countries where cash payments are restricted.
- Customer requests to purchase, or has possession of, large volumes of high denomination banknotes.
- Customer requests to purchase, or has possession of, large amounts of foreign currency without a plausible explanation.
- Customers who use false identification or offer different identifications on separate occasions

[4] FATF "Money Laundering through the Physical Transportation of Cash" (October 2015), available at: https://www.fatf- gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

2.3.1.2 Cash Deposits

Cash-intensive businesses can be expected to make cash deposits, which is legal and a natural fit with their business model. Illicit actors, however, will seek ways to place their illicit cash into the financial system. Illicit actors involved in cash generating crimes frequently need to use a significant portion of the cash they have acquired to pay for the illicit goods they have sold, to purchase additional goods, and to pay the various expenses incurred in acquiring or transporting the goods. As part of the money laundering process, individuals seek to use the proceeds of crimes by disguising the origin of the funds as legitimate economic activities. Terrorists also seek to finance, often through small amounts of cash, terrorist activities without traceability. LFIs should therefore be aware of cash deposits placed into the banking system that involve high-risk customers and/or geographical areas, third parties without a relationship to the customer, and transactions that lack an apparent business purpose. LFIs should, as the case may be, undertake CDD measures on the third party cash depositors transacting in any accounts above the threshold specified in Article 6 of the AML-CFT Decision. **LFIs should also obtain appropriate information regarding the source of cash deposited in a customer's account as well as mandate the use of Emirates ID for cash deposits in ATMs.**

- **Potential Risk Indicators:**
  - Large cash deposits followed immediately by withdrawals or electronic transfers.
  - Large cash deposit followed by an immediate request that the money be wired out or transferred to a third party, without any apparent business purpose.
  - Frequent cash deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
  - Large cash deposit is followed within a short time by wire transfers to high-risk jurisdictions.
  - Numerous cash deposits made in different bank branches over a short period of time.
  - Frequent cash deposits in small amounts, without any apparent business purpose or reasonable grounds.
  - Customers who use false identification or offer different identifications on separate ccasions

2.3.1.3 Currency Exchanges

Cash-intensive businesses may include currency exchanges as legitimate providers of services. Currency exchanges, however, can also be an attractive vehicle that illicit actors seek to exploit to enter the financial system and transfer their funds. According to the FATF, the simplicity and certainty of currency exchanges transactions and the anonymity and portability of cash make them attractive to money laundering and the financing of terrorism and illegal organisations.[5] Once the money has been exchanged, it is difficult to trace its origin. There are two different ways to perform a currency exchange: (1) the use of cash to exchange and transfer the funds; or (2) the use of the internet to perform the currency exchange and transfer the funds to a bank account.

- Potential Risk Indicators:
  - Significant and/or frequent local or foreign currency exchanges.
  - Opening of foreign currency accounts with no apparent business or economic purpose.
  - Customers who know little about or are reluctant to disclose details about the payee, or customers or parties with no apparent ties to the destination country.
  - Suspicion that the customer is acting on behalf of a third party but not disclosing it.
  - Transactions involving charities and other non-profit organizations, which are not properly licensed or registered. It is reminded that when opening any accounts for non-profit organisations, LFIs must obtain an original signed letter from the Ministry of Community Development for opening accounts to collect donations and an authorization from the UAE Red Crescent for conducting financial transfers out of the UAE through some of these accounts.
  - Customers who use false identification or offer different identifications on separate ccasions.
  - Customers who receive transfers in seasonal patterns or transactions in a pattern consistent with criminal proceeds.

[5] FATF "Money Laundering through Money Remittance and Currency Exchange Providers" (June 2010), available at: https://www.fatf-gafi.org/media/fatf/ML%20through%20Remittance%20and%20Currency%20Exchange%20Providers.pdf

3. Mitigating Risks

Effective risk mitigation is critical to protecting the LFI, complying with its legal obligations, and meeting supervisory expectations. When establishing and maintaining relationships with cash-intensive businesses, LFIs should establish policies, procedures, and processes to identify higher-risk relationships, assess AML/CFT risks of the cash-intensive business, conduct due diligence at account opening and throughout the relationship, and monitor these relationships for unusual or potentially suspicious activity. When performing a risk assessment of cash-intensive businesses, LFIs should allocate resources to those accounts that pose the greatest risk of money laundering or financing of terrorism and illegal organisations. To that end, LFIs should understand their risk and take effective, risk-based steps to protect themselves from abuse and from illicit actors and transactions.

The sections below discuss how LFIs can apply specific preventive measures to identify, manage, and mitigate the risks associated with cash-intensive businesses. LFIs should consult the legal and regulatory framework currently in force, the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*, and the CBUAE issued Guidances for further information.[6] The controls discussed below should be integrated into the LFI's larger AML/CFT compliance program and supported with appropriate governance and training.

[6] Available at https://www.centralbank.ae/en/cbuae-amlcft.

3.1 Risk-Based Approach

LFIs must take a risk-based approach to the preventive measures they put in place for all customers, including cash-intensive businesses. A risk-based approach means that LFIs should dedicate compliance resources and effort to customers, business lines, branches, and products and services in keeping with the risk presented by those customers, business lines, branches, and products and services, as assessed in accordance with Article 4 of AML-CFT Decision. **The risk-based approach has three principal components**:

3.1.1 Conducting an Enterprise Risk Assessment

As required by Article 4.1 of AML-CFT Decision, the enterprise risk assessment must reflect the presence of higher-risk customers, including cash-intensive business customers, in an LFI's customer base. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the LFI's controls risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its cash-intensive business customers, including the preventive measures discussed below.

3.1.2 Identifying and Assessing the Risks Associated with Specific Customers

The LFI is expected to assess the risk of each customer to identify those that require EDD and to support its entity risk assessment. In assessing the risks of a cash-intensive business, LFIs should consider:

i. **Geographic Risk:** LFIs should assess the risks associated with the jurisdictions in which the business is registered/headquartered and where it operates, including the jurisdictions where it has subsidiaries, where it sources its products (where relevant), and where its main counterparties are based. These may include the overall risk of money laundering, financing of terrorism and illegal organisations, and financing of proliferation, as well as what is known regarding the prevalence of abuse of entities in these sectors. There are a number of sources that LFIs can use to develop a list of high-risk countries, jurisdictions, or regions. LFIs should consult any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee (NAMLCFTC)[7], the UAE Financial Intelligence Unit (UAE FIU), and the FATF, including the FATF's list of jurisdictions subject to countermeasures and to increased monitoring. LFIs may also use public free databases such as, for example, the Basel AML Index[8] or the Transparency International Corruption Perceptions Index.[9] LFIs should not solely rely on public lists, however, and should consider their own experiences and the nature of their exposure to each jurisdiction when assessing the risk of that jurisdiction.

ii. **Customer Risks:** LFIs should assess the type of cash-intensive business, the maturity of that relationship (if the relationship is a long-term business relationship of the LFI), and other characteristics of the business relationship, such as the customer's ownership structure. Cash-intensive businesses that have a complex legal ownership structure, for example, may be higher risk than those with simpler ownership structures.

iii. **Product, Service, and Delivery Channel Risk:** LFIs should assess risk in this category based on the products and services that the customer intends to use, and the delivery channels through which the LFI will provide these services. LFIs should draw on their entity risk assessment to assess the risk of the products and services each customer uses or intends to use. (See also Section 3.2.3 below in relation to understanding the nature of the customer's business and purpose of the business relationship.)

Questions that an LFI may ask to determine the risk profile of a cash-intensive business include, but are not limited to:

- Where is the business incorporated? Where does it operate? Are these high-risk jurisdictions?
- What type of industry does the cash-intensive business operate in?
- What types of products and services is the business requesting?

- What is the intended volume, frequency, and nature of cash transactions that the cash-intensive business intends to conduct through its account?
- What is the regulatory environment in the jurisdiction(s) where the cash-intensive business is incorporated/has operations?
- What is the ownership structure of the customer? Do the customer's beneficial owners, shareholders, directors, and senior managers reside in a high-risk jurisdiction?
- What is the availability of information on the customer? Is the customer cooperating with the LFI to provide all the necessary customer due diligence ("CDD")/EDD information to the LFI?
- If the customer is an existing customer, does the customer have a history of Suspicious Transaction Report ("STR") filings?

---

[7] Available at: https://www.namlcftc.gov.ae/en/high-risk-countries.php
[8] Available at: https://baselgovernance.org/basel-aml-index
[9] Available at: https://www.transparency.org/en/cpi/2020/index/nzl

3.1.3 Applying EDD and other Preventive Measures

Where the LFI determines a customer to be higher-risk, Article 4.2(b) of AML-CFT Decision requires that the LFI apply EDD. EDD is also required for specified higher-risk customer types, no matter their risk rating:

- Customers who are Politically Exposed Persons ("PEPs") or that are owned or controlled by PEPs;
- Customers from higher-risk jurisdictions; and
- Customers with whom the LFI is establishing a correspondent relationship.

EDD measures should be designed to mitigate the specific risks identified with particular customers. Examples of EDD measures are described below in Section 3.2.

3.2 Customer Due Diligence and Enhanced Due Diligence

CDD, and where necessary EDD, are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers. As discussed below, each stage of the CDD process gives LFIs an opportunity to collect the information they need to identify and manage the specific risks of higher-risk customers.

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFIs services. **Where an LFI cannot satisfy itself that it understands a customer, then it should not accept it as a customer. If there is an existing business relationship, the LFI should not continue it. LFIs should also consider filing a STR**, as discussed in Section 3.3.2.

Under Article 5 of AML-CFT Decision, LFIs should conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. Although Article 5 permits CDD to be delayed in circumstances of lower risk, the potential higher risk of cash-intensive businesses makes it unlikely that delayed CDD will be appropriate in the context of onboarding such customers. To this end, at the time of account opening, the LFI should seek to understand the cash-intensive business' operations and business structure, the intended use of the account (including anticipated transaction volume, products, and services used), the geographic location(s) involved in the relationship, and jurisdiction(s) of operations. As part of collecting this information, the LFI should also assess the availability of information on the cash-intensive business and cooperation of the business in providing information to the LFI.

The following elements of CDD should be carried out for all customers, no matter the customer type.

3.2.1 Customer Identification and Verification

Under Article 8 of AML-CFT Decision, LFIs are required to identify and verify the identity of all customers. As stipulated in the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*, the identification and verification of the identity of customers is a fundamental component of an effective ML/FT risk management and mitigation program. Please see Section 6.3.1 of the above-mentioned Guidelines for further information on customer identification.

3.2.2 Beneficial Owner Identification

The majority of cash-intensive businesses will be legal persons. Article 9 of AML-CFT Decision requires all financial institutions to identify the beneficial owners of a legal person customer by obtaining and verifying the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. Where no such individual meets this description, the LFI should identify and verify the identity of the individual(s) holding the senior management position in the entity.

The beneficial owner of a legal person must be an individual. Another legal person cannot be classified as the beneficial owner of a customer, no matter what percentage it owns. LFIs should continue tracing ownership all the way up the ownership chain until it discovers all individuals who own or control at least 25% of the LFI's customer. When the LFI has identified qualifying beneficial owners, it should perform CDD on each individual beneficial owner, in accordance with the requirements of Article 8.1(a) of AML-CFT Decision (10). If no individual qualifies as a beneficial owner, LFIs should identify the individual(s) holding the position of senior management officer(s) within the customer. This option should be used only as a last resort, however, and when the LFI is confident that no one individual, or small group of individuals, exercises control over the customer. Please see the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements*[10] for more information on identification of beneficial owners.

[10] Available at https://www.centralbank.ae/en/cbuae-amlcft.

3.2.2.1 EDD: Beneficial Ownership

If the LFI has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so is to identify additional beneficial owners below the 25% ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10% or even the 5% level, as risk warrants. It should also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

3.2.3 Nature of the Customer's Business and Purpose of the Business Relationship

Under article 8 of AML-CFT Decision, for all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This step requires the LFI to collect information that allows it to create a profile of the customer and of the expected uses to which the customer will put the LFI's products and services. This element of CDD will have important implications for the customer risk rating.

It is critical that LFIs have processes and controls in place to ensure that they are able to identify cash-intensive business customers. In line with a risk-based approach, LFIs should interview the customer, review the customer's business license, request recent financial statements (audited if available), tax returns or additional information,

search company databases and assess the primary business activity, products, and services offered by the customer to understand the full scope of the customer's business.

If an LFI determines that a customer or prospective customer has materially misrepresented itself or its business, it should not onboard the customer and should exit the relationship if one has been established. In addition, the LFI should consider filing a Suspicious Transaction Report (STR), Suspicious Activity Report (SAR) or other report types to the UAE FIU as discussed in section 3.3.2 below. The LFI may also consider adding the customer, its beneficial owners, directors, and its managers to internal watchlists.

High-risk customers should be treated as high risk no matter the financial services they use. Even so, the risk to which the LFI may be exposed can vary based on the purpose of the account and the types of financial products and services the customer wishes to use. LFIs should fully understand the uses to which the cash-intensive business intends to put the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. To that end, the LFI should seek to assess the expected volume, frequency, and nature of cash transactions that the customer intends to conduct through its account, as this will be an important risk factor for identifying money laundering and financing of terrorism and illegal organisations risks associated with the cash-intensive business. In addition, the LFI may wish to consider whether the expected volume of cash coming through the account is consistent with the declared sales income and whether the expected volume of cash appears reasonable compared to other similar cash-intensive customers of the LFI (i.e., operating as similar business types in similar markets).

3.2.4 Ongoing Monitoring

Under Article 7 of AML-CFT Decision, all customers must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

3.2.4.1 CDD Updating

LFIs are expected to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. This is particularly crucial in the context of customers that are companies or that engage in cash-intensive business. The risk associated with a cash-intensive business can change overnight if the customer changes its business activities. LFIs should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular should ascertain that:

- The customer's beneficial owners remain the same;
- The customer continues to have an active status with a company registrar;
- The customer has the same legal form and is domiciled in the same jurisdiction; and
- The customer is engaged in the same type of business, and in the same geographies.

In addition to a review of the customer's CDD file, the LFI should also review the customer's transactions to determine whether they continue to fit the customer's profile and business and are consistent with the business the customer expected to engage in when the business relationship was established. In this capacity, the LFI should pay particular attention whether the volume of cash coming through the account is consistent with the declared sales income of the cash-intensive business customer. This type of transaction review is distinct from the ongoing transaction monitoring discussed below. The purpose of the review is to complement ongoing transaction monitoring by identifying behaviours, trends, or patterns that are not necessarily subject to transaction monitoring rules.

The techniques used for transaction review will vary depending on the customer. For lower-risk customers, a review of alerts, if any, is likely to be sufficient. For higher risk customers, such as cash-intensive businesses rated as high-

risk, a more intensive review may be necessary. For customers with a large volume of transactions, LFIs may use data analysis techniques to identify unusual behaviour. If the review finds that the customer's behaviour or information has materially changed, the LFI should risk-rate the customer again. New information gained during this process may cause the LFI to believe that EDD is necessary or may bring the customer into the category of customers for which EDD is mandatory (i.e., customers that are PEPs; customers that are based in high-risk jurisdictions; etc.).

LFIs may consider requiring that the customer update them as to any changes in its beneficial ownership or business activities. Even if this requirement is in place, however, LFIs should not rely on the customer to notify it of a change but should still update CDD on a schedule appropriate to the customer's risk rating.

3.2.4.2 EDD: Ongoing Monitoring

When customers are higher risk, such as for cash-intensive businesses rated as high-risk following the completion of the CDD process, monitoring should be more frequent, intensive, and intrusive. LFIs should review the CDD files of higher risk customers on a frequent basis, such as every six or nine months for very high-risk customers. The methods LFIs use to review the account should also be more intense and should not rely solely on information supplied for the customer. For example, LFIs should consider:

- Reviewing more or all transactions on the account, rather than a sample of transactions;

- Conducting site visits at the customer's premises, whenever the LFI is not satisfied with the documentation provided by the customer, and requesting a meeting between an appropriate LFI representative and the customer's managing director or Chief Financial Officer. Site visits can be particularly important for certain cash-intensive businesses, including those that use an LFI's cash management services on a large scale, as they allow the LFI's compliance personnel to inspect the institution's cash management program and the controls it has in place to prevent illicit cash being commingled with legitimate funds; and

- Conducting searches of public databases, including news and government databases, to independently identify material changes in a customer's ownership or business activities or to identify adverse media reports. Such searches should include adverse media searches of public records and databases, using relevant key words, including but not limited to, allegation, fraud, corruption, laundering.

3.3 Transaction Monitoring and STR Reporting

3.3.1 Transaction Monitoring

Under Article 16 of AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types. As with all customer types, LFIs that use automated monitoring systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. For example, a series of transactions between two unconnected companies may not be cause for an alert. But if the companies are all owned or controlled by the same individual(s), the LFI should investigate to make sure that the transactions have a legitimate economic purpose. In addition, higher-risk customers should be subject to more stringent transaction monitoring, with lower thresholds for alerts and more intensive investigation.

Monitoring systems can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/TF risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated

to the size, nature, and complexity of each institution. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information.[11]

The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for cash-intensive business customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high-risk rating. Some red flags for cash-intensive business customers are described below. If an LFI's automated transaction monitoring system is not capable of alerting on these red flags, LFIs should have in place manual monitoring, such as management information systems.

- The business engages in significantly greater volumes of cash transactions in comparison to other similar business types operating in similar jurisdictions and markets.
- The business engages in unusually frequent domestic and international ATM activity.
- The customer makes a cash deposit followed by an immediate request that the money be wired out or transferred to a third party, without any apparent business purpose.
- There are frequent cash deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.
- The parties to the transaction (e.g. originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
- The customer uses a personal/individual account for business purposes or vice versa.
- Upon request, a customer is unable or unwilling to produce appropriate documentation (e.g. invoices) to support a transaction, or documentation appears doctored or fake (e.g. documents contain significant discrepancies between the descriptions on the invoice, or other documents such as the certificate of origin or packing list).
- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to high-risk jurisdictions.
- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.

---

[11] Available at https://www.centralbank.ae/en/cbuae-amlcft.

3.3.2 STR Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types with the UAE Financial Intelligence Unit ("UAE FIU") when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. **STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system.** STR filings assist law enforcement in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations involving higher-risk customers:

- A potential customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current customer cannot provide required information about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty; or
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the LFI should not establish the business relationship, or

continue an existing business relationship.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[12] for further information.

[12] Available at https://www.centralbank.ae/en/cbuae-amlcft.

3.4 Governance and Training

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. Additionally, the LFI's senior management must clearly endorse and support the AML/CFT program.

As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of cash-intensive business customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For example, an LFI that has a large number of cash-intensive business customers should offer training that includes an in-depth discussion of risk factors and red flags related to such customers.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this guidance is to assist Licensed Financial Institutions (LFIs) understand and mitigate the risks when providing services to customers who are cash-intensive businesses (CIBs), and to guide them in fulfilling their AML/CFT obligations. The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that, as the UAE is a cash-intensive economy and plays an important part in global trade, there are significant risks associated with the cross-border movement of cash and bearer negotiable instruments.
	Applicability	▪ This guidance applies to natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories: ▪ all national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and ▪ insurance companies, agencies, and brokers.
Understanding Risks	Vulnerabilities of Cash	The specific characteristics of cash—its anonymity, interchangeability, and transportability—make it an attractive option for illicit actors seeking to conceal the proceeds of crime. Cash holds no record of its source or owner and can be easily concealed in large quantities Cash transactions are also instantaneous and widely accepted across jurisdictions.
	Vulnerabilities of Alternatives to Cash	Illicit actors also use various monetary instruments in conjunction with, or as a replacementto, cash. Both bearer negotiable instruments and prepaid cards, for instance, offer similar benefits to cash, including anonymity and accessibility. They can store large amounts of value in a compact physical size that is easily transportable and obscures the origin of the funds. ▪ Bearer negotiable instruments are financial instruments of whatever form, whether in the form of a bearer document, such as traveler's cheques, promissory notes and cheques, payment orders, or others.

	▪	Prepaid cards can be used as an alternative to cash in that they provide access to funds that have been paid in advance Funds can be claimed or transferred through an electronic device, such as through a card, code, electronic serial number, mobile identification number, or personal identification number within either an *open* or *closed* loop system.
	Vulnerabilities of Cash- intensive Businesses	**Types of CIBs:** CIBs are businesses that experience a high volume of cash flows. CIBs span across various industry sectors and most are operating a legitimate business. However, some aspects of these businesses may be vulnerable to money laundering or the financing of terrorism and illegal organisations. Examples of cash-intensive businesses that can pose a higher risk include but are not limited to: convenience and retail stores; restaurants; wholesale and general trading businesses; travel agencies and tour operators and car dealers. LFIs may expand on the above by considering additional factors when identifying cash-intensive businesses in their customer base and should consider the specific risks posed by the below features to determine whether the customer is considered as high-risk and should be subject to enhanced due diligence ("EDD") measures.
		Cross-Border Movement of Cash and Cash Couriers: CIBs may move cash across borders as part of their business model including by utilizing cash couriers. Cross-border movement of licit cash can be legal, subject to compliance with reporting and other relevant legal and regulatory requirements. However, criminals may also seek to move cash across borders to launder proceeds of crime by placing them in another jurisdiction. Natural of legal persons must declare upon entering or leaving the UAE any currencies, bearer negotiable instruments, precious metals and stones above the threshold of AED 60000. Understanding whether customers have made any such declarations, in accordance with the Regulation should form part of any due diligence by the LFIs where required.
		Cash Deposits: CIBscan be expected to make cash deposits, which is legal and a natural fit with their business model. Illicit actors, however, will also seek ways to place their illicit cash into the financial system Terrorists also seek to finance, often through small amounts of cash, activities without traceability. LFIs should, as the case may be, undertake CDD measures on the third party cash depositors transacting in any accounts above the threshold specified in Article 5 of the AML-CFT Decision. LFIs should also obtain appropriate information regarding the source of cash deposited in a customer's account as well as mandate the use of Emirates ID for cash deposits in ATMs.
		Currency Exchanges: CIBs may include currency exchanges as legitimate providers of services Currency exchanges, however, can also be an attractive vehicle for illicit actors seeking to enter the financial system and transfer their funds. Once the money has been exchanged, it is difficult to trace its origin.
Mitigating Risks	Risk-Based Approach	LFIs must take a risk-based approach in their AML programs. This means that they should assess all customers, including CIB customers, to determine their degree of risk. The LFIis expected to assess the risk of each customer to identify those that require EDD

		and to support its entity risk assessment. In assessing the risks of a cash-intensive business, LFIs should consider: ▪ Geographic Risk related to the jurisdiction(s) in which the customer is based and where it operates; ▪ Customer Risks related to the customer's customer base, incl, its type and the characteristics of the business relationship; and ▪ Product, Service, and Delivery Channel Risk related to the products and services the customer intends to use and the delivery channels through which the LFI will provide these services.
	Customer Due Diligence and Enhanced Due Diligence	For all customers, including CIB customers, LFIs must perform Customer Due Diligence ("CDD") with the following components:
		Customer Identification: LFIsare required to identify and verify the identity of all customers. Please seethe *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and illegal Organisations for Financial Institutions* for further information on customer identification.
		Beneficial Owners identification: The majority of cash-intensive businesses will be legal persons. For all legal person customers, LFIs must identify all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. If no such individual can be identified, the LFI must identify the individual(s) holding the senior management position(s) within the legal person customer.
		Nature of the Customer's Business and Purpose of the Business relationship: The purpose of the account and the nature of the customer's business are critical drivers of risk for CIB customers. LFIs should fully understand the uses to which the CIB intends to put the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. As they seek to understand the customer's business, LFIs should collect all information necessary to assess customer risk.
		Perform Ongoing Monitoring: For all customers, LFIs should ensure that the customer information is accurate, complete and up-to-date, and that the customer's profile and business are consistent with the expectations set at onboarding. If not, the customer risk rating may need to be changed. When customers are higher risk, such as for cash-intensive businesses rated as high-risk following the completion of the CDD process, monitoring should be more frequent, intensive, and intrusive.
	Transaction Monitoring and Suspicious Transaction Reporting	The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for CIB customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high-risk rating. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information. LFIs must file a suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types with the UAE Financial Intelligence Unit ("UAE FIU")when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a

		crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.
	Governance and Training	The preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of cash-intensive business customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls.

Guidance for Licensed Exchange Houses

Effective from 11/11/2021 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") Licensed Exchange Houses ("LEH") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the Chapter 16 of the Standards for the Regulations Regarding Licensing and Monitoring for Exchange Business, Version 1.20 of November 2021 amending Version 1.10 of February 2018 *(issued by Notice No. xx/2021 dated xx/xx/2021),* the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LEH to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LEH in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LEH should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LEH expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all Exchange Houses that are licensed and supervised by the CBUAE.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law)" and its amendment (Federal Decree Law No. (26) of 2021 amending certain provisions of Federal Decree Law No. 20 for 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations).
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74").
- CBUAE Regulations regarding Licensing and Monitoring of Exchange Business issued in January 2014 ("the Regulations") issued by Notice 1/2014 dated 06/01/2014 and its amendment issued by Notice 269/2016 on 25/08/2016.
- Chapter 16 on AML/CFT Compliance of the Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business, Version 1.20 of November 2021 amending Version 1.10 of February 2018 ("The Standards").

Furthermore, LEH may be guided by the FATF standards on AML/CFT, Guidance for a Risk Based Approach for Money or Value Transfer Services, and Report on Money Laundering through Money Remittance and Currency Exchange Providers[2].

[2] FATF: Guidance-RBA-money-value-transfer-services.pdf (fatf-gafi.org); and Money laundering through money remittance and currency exchange providers (fatf-gafi.org)

1.4. Definitions

Beneficial Owner: The 'Natural Person' who ultimately owns or exercises effective control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted, or the natural person who exercises effective ultimate control over a legal person or legal arrangement.

Exchange Business: Shall mean: (1) Dealing in sale and purchase of foreign currencies and travelers cheques; (2) Executing remittance operations in local and foreign currencies; (3) Payment of wages through establishing a link to the operating system of "wages protection system" (WPS); and (4) Other business licensed by the CBUAE.

Exchange House: A juridical person licensed in accordance with the provisions *of Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities* to carry on money exchange activity, and conduct funds transfers within and outside the UAE, and any other businesses determined by the CBUAE.

Politically Exposed Person (PEP): natural persons who are or have been entrusted with a prominent public function in the UAE or any other foreign country such as heads of states or governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties, and persons who are, or have previously been, entrusted with the management of an international organization or any prominent function within such an organization; and the definition also includes the following:

1. Direct family members (of the PEP who are spouses, children, spouses of children, parents)
2. Associates known to be close to the PEP, which include:
   (a) Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP;
   (b) Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

Instant Money Transfer Service Provider: A money remitting institution licensed and regulated by an appropriate Regulator in its home country who will have the necessary proprietary software applications and infrastructure to transfer funds instantly from an agent in one country to an agent in another country and/or domestically.

Legal person: Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.

Legal arrangement: A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality. Examples include trusts or other similar arrangements. Many legal arrangements allow for ownership, control, and enjoyment of funds to be divided between at least two different persons.

Licensed Exchange House (LEH): An Exchange House licensed by the CBUAE.

Source of funds: How the money, involved in the transaction, was originally derived or earned. Examples of source of funds are: salary, wages, inheritance, gratuity, end of service benefits, bank loan, income from businesses, sale of property, sale of land, sale of investments, etc. For verification of the source of funds, documents include but are not limited to salary slip, labor contract, court order, bank statements, etc.

2. Risks related to the Exchange Houses Sector

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the Money or Value Transfer Services' sector (MVTS), including the Exchange Houses' sector, is weighted as highly important in terms of risk and materiality in the UAE. The inherent risk and materiality of these sectors has been notably increased by their exposure to cash transactions.

The Exchange Houses sector provides widely used financial services to diverse customer sectors. While the majority of its Exchange Business is legitimate in purpose, it can be abused to facilitate illegal activity, including terrorist financing, money laundering, and other type of criminal activity. The Exchange Houses sector may provide significant opportunities for criminals to move, conceal and eventually use the funds generated by their illegal activities, unless appropriate safeguards are in place. This is due to the simplicity and speed of transactions, worldwide reach and often cash-based nature of transactions. Importantly, money laundering and financing of terrorism (ML/FT) vulnerabilities also stem from the fact that Exchange Houses often carry out occasional transactions rather than establishing an ongoing formal relationship with their customers, which means that their understanding of the ML/FT risk associated with the customer may be limited.

Risks to the Exchange Houses sector also stem from generally uneven regulatory disparity, supervision and enforcement of the sector globally because Exchange Business often involves different jurisdictions. Criminals may seek to exploit differences in regulatory requirements in different jurisdictions or deficiencies in certain jurisdictions to move, structure and conceal their funds.

Exchange Houses may also potentially be abused by criminal groups and corrupt employees or agents cooperating with criminals, who may seek to own an Exchange House outright, or indirectly through an associate, or could seek to coerce employees through financial incentives in order to use the Exchange House to circumvent AML/CFT obligations and advance criminal schemes.

3. Regulation and Supervision of Exchange Houses

The Exchange Houses sector is regulated by the Regulations and the Standards issued by the CBUAE. For more details and information on AML/CFT compliance, please refer to *Chapter 16 of the Standards for the Regulations Regarding Licensing and Monitoring for Exchange Business, version 1.20 of November 2021 amending Version 1.10 of February 2018*. LEH are supervised by the CBUAE, who may examine the activities of the LEH at any time it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations. Similar to its all LFIs, the CBUAE applies the principle of proportionality in its supervision and enforcement process, whereby small LEH may demonstrate to the CBUAE that the objectives of the regulatory requirements are met without necessarily addressing all the specifics cited in the legal and regulatory framework in the UAE.

4. AML/CFT Program for Licensed Exchange Houses

LEH must carefully design, document and effectively implement an AML/CFT Program in line with the provisions of the Standards, AML-CFT Law, and AML-CFT Decision. As per Paragraph 16.1 of the Standards, LEH must establish, maintain and regularly update effective, written, and risk-based AML/CFT programs designed to prevent LEH from being abused to facilitate ML/FT. When designing or updating their AML/CFT programs, the scope of the AML/CFT Program should be proportionate to the level of the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, the business relationships it maintains, and the geographic areas in which it operates. For example, a large LEH with a high volume of Exchange Business with high-risk countries is expected to have an AML/CFT Program commensurate with its higher risk of possibly being abused to facilitate ML/FT. However, as all LEH are exposed to some degree of risk, they must perform their own assessments and design their AML/CFT programs in accordance with their overall risk profile in order to meet their statutory obligations.

LEH should ensure the AML/CFT Program includes the following ten (10) essential components, which are described in detail in the following sections:

- Risk assessment,
- Policies and procedures,
- Governance and the Compliance Officer,
- Customer due diligence,
- Transaction monitoring,
- Sanctions obligations and freezing without delay,
- Training,
- Independent audit,
- Record keeping requirements, and
- Managing employee risk.

4.1. Risk Assessment

As required by Article 4 of the AML-CFT Decision and Paragraph 16.2 of the Standards, LEH must identify, assess and understand the ML/FT risks associated with their businesses and perform an enterprise wide ML/FT risk assessment on a regular basis. It must develop a risk assessment in order to understand how and to what extent it is vulnerable to ML/FT, and help determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk.

The risk assessment creates the basis for the LEH's risk-based approach. LEH may utilize a variety of models or methodologies to analyze their risks. In general, the risk assessment process would entail the following six (6) steps:

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6

Scope Determination	Risk Identification	Inherent Risk Assessment	Controls Evaluation	Residual Risk Assessment	Risk Mitigation
Define in-scope processes	Assess the exposure to threats and vulnerabilities in order to identify risks	Assess the impact and likelihood of risks and assign inherent risk ratings	Identify and evaluate effectiveness of controls and identify weaknesses	Calculate Residual Risk (Inherent Risk Rating minus Controls Evaluation = Residual Risk Rating)	Develop and implement mitigation plans against risks that are above an acceptable level

The nature and extent of any assessment of ML/FT risks must be appropriate to the nature, size, and complexity of the LEHS business. The risk assessment should cover all relevant factors including but not limited to:

- Customer risk;
- Products and services risk;
- Delivery channel risk;
- New technologies risk;
- Jurisdiction or geographic risk;
- Counterparty risk; and
- Other areas of risk.

As per Article 4.2 of the AML-CFT Decision as well as Paragraphs 16.2 and 16.3 of the Standards, the senior management of the LEH must be closely engaged in the risk assessment process and take responsibility for conducting an appropriate assessment. It must review and approve at least on an annual basis the LEH's risk appetite statement, risk assessment methodology, and risk assessment findings. If an initial risk assessment assesses the LEH as higher risk, it may be necessary to conduct a more intensive assessment of certain areas of the LEH's operations. In assessing ML/FT risks, the LEH must have the following elements in place:

- Documented risk assessment methodology, procedures, and processes.
- Documented risk assessment findings, including determination of overall risk and specific risks, and mitigating measures to be applied to minimize the impact of risks.
- Written risk appetite statement that clearly identifies the acceptable level of risk.
- Appropriate mechanisms to provide information on risk assessments to the CBUAE when required.

The risk assessment must be regularly updated annually at a minimum as well as in response to major changes in the LEH's operations. The risk assessment process must also be fully aligned with the LEH's products, services, customers, and geographic locations, changes in the LEH's operations, appetite statement, the legal and regulatory framework in force in the UAE, and the guidance issued by the CBUAE. In addition, LEH may consult the FATF *Guidance on the Risk-Based Approach for Money Services Businesses* and the *Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption* for more information on how to plan and perform comprehensive and appropriate risk assessments.[3] In tandem, the risk assessment findings should be used to inform the AML/CFT Program policies, procedures, internal controls, and training in order to effectively mitigate risks. The risk assessment should also inform the LEH's risk-based approach by directing an efficient allocation of AML/CFT risk management resources to the areas of greatest concern. The risk assessment findings should be provided to all business lines across the LEH, its senior management, and relevant employees.

---

[3] Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf; and https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf.

4.1.1. Customer Risk

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk posed by their customers. Customer risk is a critical component of an institutional-level risk assessment because customers engaged in illicit activity can seek to exploit the LEH to facilitate ML/FT and other types of financial crimes. The customer risk assessment process is composed of the customer risk rating, and the assessment of the inherent risk of the customer base. It should be noted that these are closely related concepts, and that risk in the customer base depends in part on the customer risk rating.

4.1.1.1. Customer Risk Rating

LEH should be able to determine whether a particular customer poses higher risk and the potential impact of any mitigating factors on that assessment. Such categorization may be due to the occupation, behavior, or activity of customers. Accordingly, the LEH should assess the risk of key customer elements in order to generate an overall customer rating. Generally, the list of elements includes but is not limited to the following:

- Customer's address and country.
- Type of customer (Domestic, foreign, company/corporate, cash-intensive business, etc.).
- Industry in which the customer does business.
- Anticipated transactional activities.
- Customer's source of wealth.
- ML/FT risk of the customer's industry
- The beneficial owners.
- Purpose of the relationship or transactional activities.

Below are some examples of risk factors that could be considered by the LEH:

- Customers conducting their business or transactions in an unusual manner.
- Customers who travel unexplained distances to locations to conduct transactions.
- Customers who are Politically Exposed Persons (PEPs) or their direct family members or known close associates and customers whose beneficial owner is a PEP.
- Customers involved in transactions that have no apparent ties to the destination country and with no reasonable explanations.
- Customers who have been the subject of legal proceedings in relation to proceeds-generating crimes known to the LEH.

4.1.1.2. Assessment of the Inherent Risk of the Customer Base

In addition to assessing individual customers, LEH should assess the inherent ML/FT risk of the customer base overall.

1. **IDENTIFY**: LEH should identify categories or types of customers that pose elevated risks. Under Chapter 16 of the Standards, the categories identified will depend on the specific customer base of the LEH and may include but are not limited to: customer types like dealers in precious metals and stones (DPMS), customers that qualify as Designated Non-Financial Businesses and Professions (DNFBPs), cash-intensive businesses which are rated as high-risk[4], PEPs, and customers with ties to high risk jurisdictions. LEH should also include as a customer segment those customers who have been off-boarded or refused service due to ML/FT suspicions.

2. **ASSESS**: LEH should assign a risk rating (for example, low risk, medium risk, etc.) to each customer category or type identified above. In assessing the risk of each category or type, LEH should consider:

    - Guidance published by the FATF;
    - The potential exposure of customers in each category to illicit funds; and
    - The features of each customer type that make them useful to illicit actors.

3. **CALCULATE EXPOSURE**: The LEH should then determine its exposure to the customer categories or types identified and rated above. LEH should consider the proportion of their entire customer base that is made up of each category of customer, the proportion of all transactions carried out by each category of customer, and the total value of all transactions carried out by each customer as a proportion of the LEH's total transaction volume. The institutional risk assessment should also take into account the individual customer risk-ratings and the proportion of higher or lower risk customers within that group. Where a LEH has large exposure to higher-risk customer types and to higher-risk customers as assessed by individual risk ratings, its overall inherent risk will generally be higher.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

---

[4] For more details and information, please refer to the CBUAE's Guidance for Licensed Financial Institutions providing services to Cash-Intensive Businesses available at https://www.centralbank.ae/en/cbuae-amlcft

4.1.2. Products and Services Risk

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk posed by the products and services they offer. The products and services risk is a critical component of an institutional-level risk assessment because customers engaged in illicit activity can seek to exploit the LEH to facilitate ML/FT and other types of financial crimes.

1. **IDENTIFY**: LEH should identify the full list of products and services they offer.

2. **ASSESS**: LEH should assign a risk rating to each product type identified above. Determining the risk of products and services should include a consideration of their characteristics and attributes and could include factors such as:

    - Products or services that may inherently favor anonymity, or products that can readily cross international borders, such as cash, online money transfers, stored value cards, money orders and international money transfers by mobile phone.
    - Products or services that have a very high or no transaction limit.
    - The global reach of the product or service offered.
    - The complexity of the product or service offered.
    - Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or a money order.

3. **CALCULATE EXPOSURE**: The LEH should consider what proportion of its total products and services, and of total transactional activity, is associated with higher and lower-risk products and services. Where a LEH has large exposure to higher-risk products and services, its overall inherent risk will generally be higher.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

4.1.3. Delivery Channel Risk

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate the risk presented by the delivery channels they use. Some delivery channels can increase ML/FT risk because they increase the risk that the LEH does not truly know or understand the identity and activities of the customer.

1. **IDENTIFY**: The LEH should identify the delivery channels that they use to provide their products and services to customers. These may include, for example: face-to-face; via a website; via an introducer or other third party; and other methods.

2. **ASSESS:** The LEH should assign an inherent risk rating to the delivery channels identified. The rating should take into consideration the characteristics and attributes of these delivery channels that make them more susceptible to abuse by illicit actors, and could include factors such as whether the delivery channel makes it more difficult to observe the customer's behavior or to be certain that the person transacting is in fact the identified customer, allows for faster transactions, or involves reliance on a third party.

3. **CALCULATE EXPOSURE**: The LEH should then determine what proportion of its transactional activity involves each delivery channel, both by volume and value. Where a LEH delivers a large proportion of its products or services via higher-risk delivery channels, its overall risk is likely to be higher as well.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

4.1.4. New Technologies Risk

Under Article 23 of the AML-CFT Decision and Paragraphs 16.2.3 and 16.2.7 of the Standards, LEH must identify, assess, understand, and mitigate the ML/FT risk to which they may be exposed by new technologies, including new delivery mechanisms and the use of new or developing technologies for both new and existing products. LEH must undertake the risk assessment **prior to obtaining approval from the CBUAE to launch or use such products, services, and technologies if applicable**.

1. **IDENTIFY:** LEH should identify the new technologies they plan to introduce. New technologies can involve new or modified products and services and also new or modified delivery channels.

2. **ASSESS**: The LEH should assign an inherent risk to each proposed new technology. Determining the risk of new technologies should include a consideration of their characteristics and attributes. In addition to the factors listed above under sections 4.1.2 and 4.1.3, this could include factors such as features of the technology that promote anonymity or obstruct access to transaction or customer information, a history of ML/FT abuse of the technology, the inherent risk of the target customer and market segments that are projected to use the new technology, and expected growth in use of the technology.

3. **CALCULATE EXPOSURE**: The LEH should consider the projected or expected volume of transactional activity associated with the new technology and follow the procedure described in sections 4.1.2 and 4.1.3 above.

4. **DOCUMENT**: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

4.1.5. Jurisdiction or Geographic Risk

Under Article 4.1 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards, LEH must identify, assess, understand, and mitigate their jurisdiction or geographic ML/FT risk.

1. **IDENTIFY**: LEH should identify the geographic footprint of their operations, which should include:

    - The jurisdictions in which they have locations, including domestic locations;

- The jurisdictions in which their customers are resident or of which they are nationals (for Non-Resident Customers only);
- The jurisdictions to which they send remittances to or receive remittances from; and
- The jurisdictions to or from which they import or export foreign currency.

LEH need not include every single jurisdiction to or from which they send or receive remittances or with which their customers have ties in the risk assessment, but should at least include the jurisdictions to which they have regular or routine exposure.

2. ASSESS: The LEH should assign each jurisdiction identified above an inherent risk-rating, based on the degree of ML/FT risk present in that jurisdiction. The LEH is strongly encouraged to develop its own country risk model that takes into consideration any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee (NAMLCFTC)[5], the UAE Financial Intelligence Unit (FIU), the FATF lists of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring,[6] as well as the Organization for Economic Cooperation and Development (OECD) list of jurisdictions classified as uncooperative tax havens.[7] The LEH should also consider whether a jurisdiction:

   - Has been identified by credible sources as providing an environment conducive to funding or supporting terrorist activities or that have designated terrorist organizations operating within them.
   - Has been identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.
   - Is subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations.
   - Has been identified by credible sources as having weak governance/law enforcement/regulatory regimes, including countries identified by the FATF as having weak AML/CFT regimes [8], for which financial institutions should give special attention to business relationships and transactions.

   Finally, the LEH should take into consideration its own knowledge and experiences, such as the number of Suspicious Transaction Reports (STR) or Suspicious Activity reports (SAR) filed that involve each jurisdiction.

3. CALCULATE EXPOSURE: The LEH should consider what proportion of its total customer base and transactional activity, by volume and value, is associated with or linked to higher or lower-risk jurisdictions. Based on its documented understanding of the risks, the LEH may decide to weigh its exposure so that a cross-border transaction to a beneficiary in a high-risk jurisdiction has a greater impact than, for example, a domestic transaction between two UAE residents where one party is a citizen of a high-risk jurisdiction. Where a LEH has large exposure to higher-risk jurisdictions, its overall inherent risk will generally be higher.

4. DOCUMENT: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

---

[5] Available at: https://www.namlcftc.gov.ae/en/high-risk-countries.php
[6] Available at: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
[7] Available at: http://www.oecd.org/ctp/harmful/theoecdissuesthelistofunco-operativetaxhavens.htm.
[8] See footnote 12

4.1.6. Counterparty Risk

As required by Article 25 of the AML-CFT Decision and Paragraph 16.2.3 of the Standards LEH must identify, assess, understand, and mitigate counterparty risk prior to establishing business relationships with counterparties, and on an ongoing basis once the relationship is established. Counterparty relationships include the following types:

- Domestic and Foreign correspondent banking arrangements, such as those with banks, exchange houses, or any other financial institutions for the purpose of money transfer services.
- Money transfer arrangements with instant money transfer service providers.
- Hedging arrangements with local or foreign institutions.
- Arrangements to import or export banknotes from/to foreign institutions, such as Banks, exchange houses, or other financial institutions outside the UAE.
- Arrangements with local or foreign entities to offer special products/services.

1. IDENTIFY: LEH should identify all counterparties that fit the description above, including with affiliates and other members of the same group.

2. ASSESS: The LEH should assign an inherent risk rating to each counterparty. The determination of the counterparty's risk should include a consideration of all characteristics and attributes that make the counterparty more or less susceptible to abuse by illicit actors, as well as characteristics and features of the counterparty relationship that could increase or decrease risk. This could include for example:

    - The risk of the country in which a counterparty is registered;
    - The products and services it offers and the risks of the counterparty's customer base overall;
    - Its reputation in the sector and any adverse media;
    - Its ownership (including links to PEPs or persons associated with adverse media);
    - The counterparty's experience in this sector and its overall sophistication;
    - The quality and intensiveness of the counterparty's AML/CFT program, including whether the program's requirements are consistent with minimum requirements imposed in LEH by the legal and regulatory framework in force in the UAE;
    - The quality and rigor of supervision applied to the counterparty;
    - Any regulatory or criminal enforcement actions taken against the counterparty; and
    - The nature and purpose of the counterparty relationship, including the risk of the products and services involved and the types of customers who use the relationship.

3. CALCULATE EXPOSURE: LEH should determine the proportion of counterparties that are rated higher risk, both in terms of actual numbers and in terms of the volume and value of the transactions involving that counterparty. Because counterparty relationships may involve rapid, large changes in the volume of transactions, LEH should continuously monitor their exposure to counterparties and update their risk assessment whenever exposure changes substantially.

4. DOCUMENT: A LEH's approach to categorizing risk should be clearly documented. The LEH should keep detailed records of its assumptions, statistics used to complete this process, and the resulting analysis and outcomes.

4.1.7. Other Areas of Risk

In addition to the ML/FT risks discussed in this section, LEH may be exposed to other areas of illicit finance risk, including sanctions and proliferation financing. The LEH may choose to include these risk domains in its AML/CFT assessment as long as the resulting assessment gives appropriate space and attention to ML/FT risk. Given the evolving nature of ML/FT risks, LEH may also choose to assess their ML/FT risk in additional categories to those discussed above (although they must always address at least the categories covered in this section).

Under Article 4.1 (b) of the AML-CFT Decision and Paragraph 16.2.5 of the Standards, LEH must thoroughly document their risk assessment process so that they can fully explain and justify their assessment methodology.

4.2. Policies and Procedures

As required by Article 4.2.a) of the AML-CFT Decision and Paragraph 16.3 of the Standards, LEH must establish and implement comprehensive and documented AML/CFT policies and procedures to enable them to effectively manage and mitigate the risks they have identified. Under Paragraph 16.3.6 of The Standards, these must be approved by the Manager in Charge, the Compliance Officer, and the Board of Directors (or Owner/Partners where there is no Board of Directors). They must be reviewed and updated annually at a minimum to ensure that they are consistent with statutory obligations and other international best practices, and effective in mitigating existing as well as emerging ML/FT risks as per Paragraph 16.3.7 of the Standards. Policies and procedures should at a minimum:

- Be commensurate with the nature, size, and complexity of the LEH's operations.
- Outline the AML/CFT Program.
- Be consistently implemented across all branches, subsidiaries and affiliated entities in which the LEH holds a majority interest.
- Capture the LEH's day-to-day operations and processes.
- Clearly define the roles and the day-to-day responsibilities of the Manager in Charge, Compliance Officer, Compliance Committee and employees in relation to AML/CFT compliance as well as the ones of the Board of Directors (or Owner/Partners where there is no Board of Directors) in relation to implementing a robust compliance program across the business of the LEH.
- Enable the LEH to clearly and effectively identify, escalate, and report suspicious transactions and activities.
- Require enhanced due diligence to be conducted on all customers and transactions that are assessed to be high-risk.
- Prohibit employees from, directly or indirectly, informing the customer or any third party that their transactions are subject to monitoring or under investigation or have been reported to the FIU as suspicious transactions.
- Contain sufficient detail of their record keeping obligations.

Policies and procedures should be clearly communicated to all relevant employees. They should be easy to follow and be designed to support the compliant and effective functioning of the AML/CFT program and prevent employees from engaging in misconduct.

4.3. Governance and Compliance Officer

The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LEH's risks and obligations and who has the resources and autonomy necessary to ensure that the LEH's program is effective. As per Article 21 of the AML-CFT Decision and Paragraph 16.4 of the Standards, the LEH must appoint a Compliance Officer who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT Program. The role of Compliance Officer must be limited to tasks related to AML/CFT compliance and not be combined with any other functions of the LEH to avoid conflict of interest from multiple roles. Furthermore, as per Paragraphs 16.5 and 6.9.3 of the Standards, the LEH must further appoint an Alternate Compliance Officer to strengthen the AML/CFT Program as well as establish and maintain a Compliance Committee to provide additional oversight of the AML/CFT program. Chapter 6 of the Standards refers to Corporate Governance as the mechanisms and processes by which the LEH is managed, controlled and directed. For more details and information please refer to the relevant section in the Standards.

4.4. Customer Due Diligence

The goal of the CDD process is to ensure that LEH understand who their customer is and the purpose for which the customer will use the LEH's services. **Where a LEH cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LEH should not continue it.** LEH should also consider filing an STR, SAR or other report types to the FIU as discussed in section 5 below. This guidance is not an exhaustive list of CDD obligations and LEH should consult the legal and regulatory framework in force in the UAE for the measures to be taken.

Under Article 8 of AML-CFT Decision, LEHs are required to identify and verify the identity of all customers. In particular, when verifying the Emirates ID card (either physically or by way of digital or e-KYC solutions) the LEH must use the online validation gateway of the Federal Authority for Identity & Citizenship, the UAE-Pass Application, or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where acceptable IDs other than the Emirates ID are used in the KYC process, a copy must be physically obtained from the original ID and certified as "Original Sighted and Verified" by the employee who carries out the CDD process.

As required by Paragraph 16.7 of the Standards, LEH must implement a strong Know Your Customer ("KYC") process that is based on clear and comprehensive written policies and procedures. Implementation of an effective KYC process is an essential cornerstone of a LEH's AML/CFT Program and is necessary in order to:

- Understand who LEH's customers and counterparties are.
- Detect suspicious activity or transactions in a timely manner.
- Promote safe and sound business practices.
- Minimize the risk that the LEH is abused by illicit actors.
- Reduce the risk of processing transactions when the customer is involved in criminal activity.
- Protect the reputation of the LEH.
- Comply with statutory obligations.

The KYC process must be risk-based and, as such, the KYC measures applied must be commensurate with the ML/FT risks associated with their customers or transactions. Accordingly, Paragraph 16.7.3 of the Standards requires three types of KYC processes that must be applied depending on the customer's risk and the nature of the transaction and customer. These are:

- Customer Identification (CID);
- Customer Due Diligence (CDD); and
- Enhanced Due Diligence (EDD).

Please refer to the table below on when to use each KYC measure and to refer to the respective paragraphs in the Standards for the detailed requirements:

Customer Type	Customer Activity	Value of Transaction	Preventive Measure Required	Paragraph in the Standards, Version 1.20
Natural Persons	Currency Exchange	Equal to or greater than AED 3,500 and less than AED 35,000	CID	16.8
		Equal to or greater than AED 35,000 and less than AED 55,000 within a 90-day period	CID **and** CDD	16.8 16.9
		Equal to or greater than AED 55,000 within a 90-day period	CID, CDD, **and** EDD	16.8 16.9 16.10
	Money Transfer	Any value less than AED 55,000	CID **and** CDD	16.8 16.9
		Equal to or greater than AED 55,000 within a 45-day period	CID, CDD, **and** EDD	16.8 16.9 16.10
All Legal Persons or Arrangements	Any Activity	Any Value	CDD **and** EDD	16.11

Counterparty Relationships	Any Activity	Any Value	CDD **and** EDD	16.11.8 to 16.11.12 16.11.2
PEPs	Any Activity	Any Value	CID, CDD, **and** EDD	16.13
DNFBPs/DPMS	Any Activity	Any Value	CID (if the customer is a natural person), CDD, **and** EDD	16.14/16.15
High-Risk Natural Persons	Any Activity	Any Value	CID, CDD, **and** EDD	16.16 16.8, 16.9 16.10
High-Risk circumstances	Any Activity	Any Value	CID (if the customer is a natural person), CDD, **and** EDD	16.16 16.8, 16.9 16.10/11
Third Party Transactions	Any Activity	Any Value	CID (if the customer is a natural person), CDD, **and** EDD	16.20 16.8, 16.9 16.10/11

4.4.1. Ongoing Monitoring

Under Article 7 of the AML-CFT Decision, LEH are required to ensure that the documents, data or information obtained under CDD measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories. Ongoing monitoring allows the LEH to ensure that the Exchange Business is being used in accordance with the customer or relationship profile developed through KYC during onboarding, and that transactions are normal, reasonable, and legitimate.

As per Paragraphs 16.9.11 and 16.11.7 of the Standards, where the customer is a natural person (when CDD must be applied) or a legal person or arrangement, the customer profile must be reviewed and updated either annually, or at least upon the expiry of the ID, the trade license or the ID of any person authorized to make transactions on behalf of the customer, whichever comes first. At this time, the LEH must conduct ongoing monitoring on the customer which must consist of the following:

- The original ID must be verified (in accordance with Paragraphs 16.8.3, 16.9.6 and 16.9.7) and its copy must be held in the records during the review of a customer profile;
- CDD (and, where appropriate, EDD) must be repeated and the customer profile updated, including the information required under Paragraph 16.9.4 or 16.11.2 of this Chapter.
- CDD and EDD must also be repeated whenever there is a change in the profile of the customer;
- LEH must scrutinize the transactions concluded by a customer to ensure that transactions are consistent with its knowledge of the customer, the customer's business, risk profile, the source of funds and where necessary, source of the customer's wealth; and
- LEH must review transaction monitoring results for the customer to determine whether any STR/SARs or other reports have been filed or whether the customer's behavior has generated alerts.

Unless otherwise required, such as in the cases above mentioned, LEH should update the KYC information on customers and counterparties on a risk-based schedule, with KYC on higher-risk customers being updated more frequently. KYC updates should include a refresh of all elements of initial KYC, and in particular must ascertain whether:

- The customer/counterparty's beneficial owners remain the same.
- The customer continues to have an active status with the LEH Point of Sale system.
- The customer/counterparty is domiciled in the same jurisdiction.
- The customer/counterparty is engaged in the same type of business, and in the same geographies.
- The customer/counterparty's transactions continue to fit its profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established, or the business that the LEH expected to engage in when it established the counterparty relationship.

If any of the above characteristics have changed, the LEH should risk-rate the customer/counterparty again.

Furthermore, LEH should conduct EDD when the revised risk rating demands it or if the customer/counterparty's history of transactions is not consistent with its profile and the expectations established at account opening. In particular, if the customer/counterparty's transactions/behavior have resulted in the filing of an STR/SAR with the FIU, the LEH should review the customer/counterparty profile and the activity that led to the report and make a determination as to whether the risk rating should be raised or the relationship should be terminated. LEH may consider requiring that the customer/counterparty update them as to any changes in its beneficial ownership. Even if this requirement is in place, however, LEH must not rely on the customer/counterparty to notify it of a change, but must still update KYC on a schedule appropriate to the customer's risk rating.

4.5. Transaction Monitoring

As required by Article 7 of the AML-CFT Decision and Paragraph 16.24 of the Standards, LEH must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. Transaction monitoring systems allow the LEH to monitor the transactions made by their customers in real-time and/or on a daily basis. All LEH should have a form of transaction monitoring system in place in order to monitor for any suspicious transactions to and from customers. **Failure to have such a system in place may not only cost a LEH its reputation, but also lead to large fines and other penalties.**

Transaction monitoring is distinct from the ongoing monitoring discussed in section 4.4.1. Both are required, but the purpose of transaction monitoring is not primarily to update the customer risk profile but to detect and investigate transactions that may need to be reported to the FIU because they are potentially related to illicit activity. While CDD review (as discussed in section 4.4.1) may take place once a year, transaction monitoring occurs in real time and is thus able to support prompt reporting to the FIU after the transaction takes place.

Under Article 4.2 (a) of the AML-CFT Decision and Paragraph 16.24.1 of the Standards, Transaction monitoring must be commensurate with the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, and the geographic areas in which it operates. The transaction monitoring system used by a LEH, whether automated or manual, must be able to flag unusual movements of funds or transactions for further analysis. Rules and parameters must take account of ML/FT typologies in the Exchange Houses sector.

When the monitoring system generates an alert, it must be investigated and either escalated or otherwise dispositioned in a timely fashion in order to support prompt reporting to the FIU. Transaction monitoring systems should create an audit trail of all activity related to alert generation, investigation, and disposition to have a clear understanding of the activity, and potentially report it to the relevant authorities.

For more details and information, please refer to the *CBUAE Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanction screening*[9].

[9] Available at https://www.centralbank.ae/en/cbuae-amlcft.

4.5.1. Indicative Risk Factors Associated with Transactions

The following is an indicative and non-exhaustive list of risk factors associated with transactions[10].

- **Customer's behavior at point of origination:**
  - Customer structures transaction in an apparent attempt to break up amounts to stay under any applicable CDD threshold to avoid reporting or other requirements.
  - Customer attempts a transaction, but given he or she would likely be subject to the CDD monitoring, cancels transaction to avoid reporting or other requirements.
  - Transaction is unnecessarily complex with no apparent business or lawful purpose
  - Number or value of transactions is inconsistent with financial standing or occupation, or outside the normal course of business of the customer in light of the information provided by the customer when conducting the transaction or during subsequent contact.
  - Customer offers a bribe or a tip, or is willing to pay unusual fees to have transactions conducted.
  - Customer has vague knowledge about amount of money involved in the transaction.
  - Customer makes unusual enquiries, threatens or tries to convince employees to avoid reporting.
  - Customer sends money internationally and then expects to receive an equal incoming transfer or vice versa.
  - Customer transfers money to illegal online gambling sites. Email addresses containing gambling references or transfers to countries with large numbers of internet gambling sites.
  - Customer wires money to higher-risk jurisdiction/country/corridor.
  - Customer transfers money to claim lottery or prize winnings
  - Customer transfers money to someone met only online or appears to have no familial relationship with the receiver and no explanation forthcoming for the transfer.

- **Activity detected during monitoring** (in many of these scenarios the customer's activity may be apparent both during point-of-sale interaction and back-end transaction monitoring):
  - Transfers to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
  - Unusually large aggregate wire transfers or high volume or frequency of transactions with no logical or apparent reason.
  - Customer uses aliases, nominees or a variety of different addresses.
  - Customers whose concentration ratio of transfers made to a jurisdiction is notably higher than what is to be expected considering overall customer base.
  - Customer transfers/receives funds from persons involved in criminal activities as per the information available.
  - A network of customers using shared contact information (such as address, telephone or e-mail) where such sharing is not normal or reasonably justifiable.

- **Transactions received:**
  - Transactions that are not accompanied by the required originator or beneficiary information.
  - Additional customer or transactional information was requested from an ordering counterparty but not received.
  - Large number of transactions received at once or over a certain period of time which do not seem to match the recipient's usual past pattern.

---

[10] FATF: Guidance-RBA-money-value-transfer-services.pdf (fatf-gafi.org)

4.6. Sanctions Obligations and Freezing Without Delay

Article 16.1 of the AML-CFT Law and Article 60 of the AML-CFT Decision require LEH to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision 74 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS").

For more information and details on their obligations in relation to their sanctions obligations LEH should consult Paragraph 16.25 of the Standards; the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's *"Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions";* the *"CBUAE Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions"* as well as the *"CBUAE Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening"*[11].

Furthermore, LEH must sign up for the Integrated Enquiries Management System (IEMS) introduced by the FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests. Via this system, the FIU can make requests to all LFIs simultaneously with the goal of processing requests and providing results to Law Enforcement Agencies more efficiently. For more information, LEH should consult the IEMS User Guide published by FIU[12].

---

[11] Available at: https://www.centralbank.ae/en/cbuae-amlcft

[12] Available at: https://www.uaefiu.gov.ae/media/jtdnttby/integrated-enquiry-management-system.pdf

4.7. Training

As per Paragraph 16.23 of the Standards LEH must provide comprehensive AML/CFT compliance training to all employees. The effective application of AML/CFT policies and procedures depends on the employees understanding not only of the processes they are required to follow, but also the risks these processes are designed to mitigate, and the possible consequences of those risks. Employees should remain abreast on an ongoing basis of emerging ML/FT typologies and new internal and external risks. The AML/CFT compliance training should be relevant to the LEH's ML/FT risks, business activities and up to date with the latest legal and regulatory obligations and internal controls. It should be tailored to particular lines of business within the LEH, equipping employees with a sound understanding of specialized ML/FT risks they are likely to face, and their obligations in relation to those risks and must be provided to all new employees within thirty (30) calendar days from the date of joining. Thereafter, refresher training must be provided to all employees at regular intervals depending on the ML/FT risk exposure of each employee; for example, employees who deal directly with customers, products or services must be trained annually at a minimum. Refresher training must also be provided whenever there are changes in the legal and regulatory framework in force in the UAE or the LEH's AML policy/procedures. Furthermore, the AML/CFT compliance training should be provided to relevant employees upon learning of a confirmed negative risk assessment result or audit finding, or other deficiency pertaining to the AML/CFT Program. Evidence for all trainings conducted must be retained for inspection by the CBUAE.

4.8. Independent Audit

The independent audit process helps the LEH assess the effectiveness and adequacy of its current processes, including by assessing the adequacy of the AML/CFT Program and checking for any inconsistencies between the policy and procedures and day-to-day operations in order to identify any weaknesses and deficiencies. Independent auditing must be undertaken regularly to review and assess the effectiveness of the AML/CFT compliance policies, procedures, systems and controls, and their compliance with the LEH's obligations. As per Paragraph 16.31.1 of the Standards, the Compliance Officer's function must undergo regular audit by the LEH's internal audit department. In addition, under Paragraph 16.31.2 of the Standards, "agreed-upon procedures" for the review of the AML/CFT Compliance function must be performed by external auditors annually.

The independent audits, whether internal or external, should be undertaken by skilled and competent auditors. The internal audit department should be resourced with skilled and competent employees that understand the AML/CFT Program of the LEH. The audit should be commensurate to the level and sophistication of the LEH, and be updated to account for changes in risk assessments and the legal and regulatory framework in force in the UAE. The internal audit function should be accountable to the Board of Directors (or the Owner/Partners if there is no Board of

Directors), independent of the audited activities and functions, and have sufficient authority, skills, expertise, and resources within the organization.

4.9. Record Keeping Requirements

Under Article 24 of the AML-CFT Decision, LEH must retain all records, documents, data and statistics for all transactions for a minimum period of five (5) years from the date of completion of the transaction or termination of the business relationship or from the closing date of the account. Records must be maintained in an organized manner so as to permit data analysis and, where relevant, the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. For more details and information please refer to paragraph 16.29 of the Standards.

4.10. Managing Employee Risk

As per Paragraphs 8.2 and 16.22 of the Standards, the LEH must implement an appropriate recruitment and Know Your Employee ("KYE") process for hiring employees and confirm the background of applicants prior to placing them in employment. The level of vetting procedures applied should reflect the ML/FT risks to which individual employees are exposed in their assigned roles. The LEH should be aware of potential conflicts of interest for employees with AML/CFT responsibilities and should act to reduce or manage such conflicts of interest.

Furthermore, under Paragraph 16.28 of the Standards, the LEH must watch out for its employee's behavior and be aware of possible indicators of illicit behavior displayed by employees, such as:

- An employee whose lifestyle cannot be supported by his/her salary, which may indicate receipt of tips or bribes.
- An employee who is reluctant to take a vacation, which may indicate they have consented or are being forced to provide services to customers in violation of the law or company policy.
- An employee who is associated with an unusually large number of transactions or a transaction in an unusually large amount, which may indicate they have consented or are being forced to provide services to customers in violation of the law or company policy.

5. Reporting Obligations

5.1. Reporting to the CBUAE

As per Paragraph 4.21 of the Standards, LEH must submit reports to the CBUAE, which may be updated from time to time in terms of the frequency and form of submission and their deadline. For the submission of periodical returns/reports via the online system, the LEH must obtain access to the CBUAE reporting portals, such as its Integrated Regulatory Reporting System, Remittance Reporting System and/or other applicable system.

5.2. Reporting to the FIU

All LEH should have procedures and systems in place to ensure that suspicious activity is reported to authorities in an appropriate and timely manner. LEH must take into account all information from both the ordering and beneficiary sides in order to determine whether an STR or SAR is to be filed.

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LEH must file without any delay an STR or SAR or other report types with the FIU using the "goAML" portal when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Under Article 24 of the AML-CFT Law, any person, including a LEH or their managers and employees, who violates on purpose or by gross negligence

their statutory obligation to report a suspicion of money laundering and related predicate offences, financing of terrorism or illegal organisations is liable of the following sanctions:

- Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or
- Any of these two sanctions (i.e. imprisonment or fine of no less than AED100,000 and no more than AED1,000,000).
- For more details and information, please refer to Paragraph 16.27 of the Standards as well as the "*CBUAE Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*"[13].

[13] Available at: https://www.centralbank.ae/en/cbuae-amlcft

6. Prohibition of Tipping Off

Under Article 25 of AML-CFT Law, anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated by the competent authorities is punishable by a penalty of imprisonment for no less than six months and/or a fine of no less than AED 100,000 and no more than AED 500,000. Any such action is known as "tipping off." As per Paragraph 16.27 of the Standards, the prohibition on tipping off means that the LEH or its employees must not inform customers or any persons or third parties, either directly or indirectly, that their transactions are subject to monitoring, under investigation or have been reported to the FIU as suspicious transactions. The Compliance Officer should ensure that all employees of the LEH are aware of the consequences of tipping off. Sufficient AML/CFT training should be provided to all employees to ensure that they understand what constitutes tipping off and how to avoid it.

Annex1 - Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding of risks and effective performance by the Licensed Exchange Houses ("LEH") of their AML/CFT statutory obligations. The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the Money or Value Transfer Services' sector, including the Exchange Houses' sector, is weighted as highly important in terms of risk and materiality in the UAE. The inherent risk and materiality of these sectors has been notably increased by their exposure to cash transactions.
	Applicability	This Guidance applies to all Exchange Houses that are licensed and supervised by the CBUAE.
Risks Related to the Exchange House Sector	The Exchange House sector provides widely used financial services to diverse customer sectors. While the majority of its Exchange Business is legitimate in purpose, it can be abused to facilitate illegal activity, including terrorist financing, money laundering, and other type of criminal activity. This is due to the simplicity and speed of transactions, worldwide reach, global regulatory disparity and often cash-based nature of transactions. Exchange Houses may also potentially be abused by criminal groups and corrupt employees or agents co-operating with criminals, who may seek to own an Exchange House outright, or indirectly through an associate or could seek to coerce employees through financial incentives.	
Regulation and Supervision of Exchange Houses	The Exchange Houses sector is regulated by the Regulations and the Standards issued by the CBUAE. For more detail and information, please refer to *Chapter 16 on AML/CFT Compliance of the Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business* (Version 1.20 of November 2021 amending Version 1.10 of February 2018 ("The Standards")). LEH are supervised by the CBUAE, which may examine the activities of the LEH at any time it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations.	

AML/CFT Compliance Program for LEH	AML/CFT Program	LEH must carefully design, document and effectively implement an AML/CFT Program in line with the provisions of the Standards, AML-CFT Law, and AML-CFT Decision. When designing or updating their AML/CFT programs, the scope of the AML/CFT Program should be proportionate to the level of the risk posed by the LEH's size, scale, complexity, the nature and volume of its Exchange Business, the nature of its customer base, the business relationships it maintains, and the geographic areas in which it operates.
	Risk Assessment	LEH must develop a risk assessment in order to understand how and to what extent it is vulnerable to ML/TF, and help determine the nature and extent of AML/CFT resources necessary to mitigate and manage that risk, which should cover all relevant factors including but not limited to: • Customer risk; • Products and services risk; • Delivery channel risk; • New technologies risk; • Jurisdiction or geographic risk; • Counterparty risk; and • Other areas of risk.
	Policies and Procedures	LEH must establish and implement comprehensive and documented AML/CFT policies and procedures to enable them to effectively manage and mitigate the risks identified. They must be approved, reviewed and updated, annually at a minimum, to ensure that they are consistent with the legal and regulatory framework in the UAE and other international best practices, and effective in mitigating existing as well as emerging ML/FT risks.
	Governance and the Compliance Officer	The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LEH's risks and obligations and who has the resources and autonomy necessary to ensure that the LEH's program is effective. The role of Compliance Officer must be limited to tasks related to AML/CFT compliance and not be combined with any other functions of the LEH to avoid conflict of interest from multiple roles. The LEH must also appoint an Alternate Compliance Officer.
	Customer Due Diligence and Ongoing Monitoring	The goal of the CDD process is to ensure that LEH understand who their customer is and the purpose for which the customer will use the LEH's services. Where an LEH cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LEH should not continue it. LEH should also consider filing an suspicious transaction report ("STR") or suspicious activity report ("SAR") or other report types to the FIU as discussed in section 5 of the Guidance. The Standards require three types of KYC processes that must be applied depending on the customer's risk and the nature of the transaction and customer. These are Customer Identification (CID); Customer Due Diligence (CDD); and Enhanced Due Diligence (EDD). Please refer to the table in Section 4.4 on when to use each KYC measure and to the respective paragraphs in the Standards for the detailed requirements. LEH are required to ensure that the documents, data or information obtained under CDD measures are up-to-date and appropriate by reviewing

		the records, particularly those of high-risk customer categories. Unless otherwise required, LEH should update the KYC information on customers and counterparties on a risk-based schedule, with KYC on higher-risk customers being updated more frequently. When customer's characteristics has changed, LEH should risk-rate the customer again, and, where necessary, conduct EDD.
	Transaction Monitoring	LEH must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. All LEH should have a form of transaction monitoring system in place in order to monitor for any suspicious transactions to and from customers; failure to have such a system in place may not only cost an LEH its reputation, but also lead to large fines and other penalties. For more information and details, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanction screening*.
	Sanctions Obligations and Freezing Without Delay	LEH are required to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations and the requirements set by Cabinet Decision 74 of 2020 regarding Targeted Financial Sanctions. For more information and details, please consult the Standards, the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's *Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions,* the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions* as well as the CBUAE's *Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*. Furthermore, LEH must sign up for the Integrated Enquiries Management System (IEMS) introduced by the FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests.
	Training	LEH must provide comprehensive AML/CFT compliance training to all employees, which should be relevant to the LEH's ML/FT risks, business activities and up to date with the latest legal and regulatory obligations and internal controls. It should be tailored to particular lines of business within the LEH, equipping employees with a sound understanding of specialized ML/FT risks they are likely to face and their obligations in relation to those risks, and provided to all new employees within thirty calendar days from the date of joining and regularly thereafter proportionate to their ML/FT risk exposure.
	Independent Audit	Independent auditing must be undertaken regularly to review and assess the effectiveness of the AML/CFT compliance policies, procedures, systems and controls, and their compliance with the LEH's obligations by the LEH's Internal Audit Department. In addition, "agreed-upon procedures" for the review of the AML/CFT Compliance function must be performed by external auditors annually.
	Record-Keeping	LEH must retain all records, documents, data and statistics for all transactions for a minimum period of five (5) years from the date of completion of the transaction or termination of the business relationship or from the closing date of the account. Records must be maintained in an

		organized manner so as to permit data analysis and, where relevant, the tracking of financial transactions.
	Managing Employee Risk	The LEH must implement an appropriate recruitment and Know Your Employee ("KYE") process for hiring employees and confirm the background of applicants prior to placing them in employment. The level of vetting procedures applied should reflect the ML/FT risks to which individual employees are exposed in their assigned roles.
Reporting Obligations	Reporting to the CBUAE	LEH must submit reports to the CBUAE, which may be updated from time to time in terms of the frequency and form of submission and their deadline. For the submission of periodical returns/reports via the online system, the LEH must obtain access to the CBUAE reporting portals, such as its Integrated Regulatory Reporting System ("IRR"), Remittance Reporting System ("RRS") and/or other applicable system.
	Reporting to the FIU	LEH must file without any delay a STR, SAR or other report types with the FIU using the "goAML" portal when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for Licensed Financial institutions on Suspicious Transaction Reporting* for further information.
Prohibition of Tipping Off	The prohibition on tipping off means that the LEH or its employees must not inform customers or any persons or third parties, either directly or indirectly, that their transactions are subject to monitoring, under investigation or have been reported to the FIU as suspicious transactions.	

Guidance for Licensed Financial Institutions Providing Services to Legal Persons and Arrangements

Effective from 7/6/2021 **Status:** In-Force

1. Introduction

1.1. Purpose of this Guidance

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58")

1.4. Definitions

Key Terms
Beneficial owner: The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client; or the natural person on whose behalf a transaction is being conducted; or the natural person who exercises effective ultimate control over a legal person or legal arrangement.
Legal person: Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.
Legal arrangement: A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality. Examples include trusts or other similar arrangements. Many legal arrangements allow for ownership, control, and enjoyment of funds to be divided between at least two different persons.
Settlor: A natural or legal person who transfers the control of his funds to a trustee under a trust document.

Trust: A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.

Trustee: A natural or legal person who has the rights and powers conferred to him by the settlor or the trust, under which he administers, uses, and acts with the funds of the settlor in accordance with the conditions imposed on him by either the settlor or the trust.

2. Understanding and Assessing the Risks of Legal Persons and Arrangements

Legal persons and arrangements are critical to the conduct of business, charitable activity, estate planning, and many other activities. They have a wide variety of acceptable and desirable purposes, and the vast majority of legal persons and arrangements are engaged solely in licit behaviour.

Nevertheless, certain aspects of legal persons and arrangements are acknowledged to pose risk for LFIs that accept such entities as customers. **Most importantly, the use of legal persons and arrangements to manage funds or do business can obscure or conceal the identity of the individuals who are truly controlling, directing, or benefiting from the services the LFI offers its legal person or legal arrangement customer.** This concealment can allow illicit actors to abuse services offered by LFIs in order to launder the proceeds of crime, engage in terrorist financing, evade United Nations or UAE sanctions, and threaten the integrity of the UAE financial system and the security of the State.

Legal persons and arrangements are attractive to participants in illicit finance—including money laundering (ML), the financing of terrorism (TF), and the financing of proliferation (PF)—because these entities offer the opportunity to transact anonymously, or nearly anonymously, through complex and/or opaque corporate structures. Section 2.1 discusses the ways that legal persons and arrangement can be abused to conceal illicit transactions from financial institutions.

It is important to be aware, however, that not all legal persons and arrangements pose equal risk of abuse. The vulnerabilities arising from the basic characteristics of legal persons and arrangements can be enhanced or mitigated through the formation process and other controls jurisdictions apply to legal persons and arrangements. Thus, it is critical for LFIs seeking to understand the risks of their customer base to be aware of the presence or absence of these features and controls in the jurisdiction of formation. Section 2.2 below discusses specific aspects of a control regime and how these can impact vulnerability.

2.1. ML/TF Risks Legal Persons and Arrangements Pose to LFIs

Legal persons and arrangements offer many advantages to illicit actors. Most importantly, however, they could be abused to hide the identity of natural persons and allow bad actors to seek to open an account or carry out a transaction with an LFI under a name other than their own. Weak laws governing the formation of legal persons and arrangements, could allow for bad actors to abuse legal persons and arrangements and enable them to conduct a transaction or transactions almost without the LFI understating the real risks and the involvement of the bad actors —an action that would otherwise be prohibited under the laws of most jurisdictions. This ability to conceal identity has a number of ramifications for financial institutions.

2.1.1. Obscuring Identity/Beneficial Ownership

Individuals can use legal persons and arrangements to obscure or conceal their involvement in a transaction. In many jurisdictions, the individuals who truly own, control, direct, or benefit from a transaction—known as the beneficial owners—are not required to reveal their identities to the authorities. Individuals who are wanted criminals,

known terrorist financiers, or connected to heavily sanctioned jurisdictions can form opaque companies in lower-risk jurisdictions and seek financial services under the name of a legal person or arrangement they control.

Even in jurisdictions where legal persons and arrangements are required to report their beneficial ownership, illicit actors can seek to conceal their ownership interest through the use of complex corporate structures, intermediaries, and nominees, as discussed below.

2.1.2. Obscuring the Purpose of an Account or Transaction

Legal persons, particularly businesses, engage in a wide variety of transactions with a wide range of counterparts. Depending on its size and the nature of its business, a legal person customer might be likely to send and receive far larger and more irregular transfers than would an individual—many of them with counterparties that are also legal persons. For example, a company that manufactures for export may send payments to suppliers in a number of foreign jurisdictions, and receive payments from purchasers in different jurisdictions.

The variety and unpredictability of transactions carried out by legal persons can make it more difficult to identify behaviour that is unusual or has no obvious economic purpose. This is especially true when the counterparts are also opaque legal persons or arrangements. For example, a company may seek to reduce its tax burden by claiming that certain transfers are tax-deductible expenses, when in reality they are payments to a legal person with the same beneficial owners as the originating company.

2.1.3. Obscuring Source of Funds or of Wealth

Legal persons can also be abused by individuals seeking to hide the source of an incoming transfer. For example, a politically exposed person (PEP) might receive a transfer that supposedly represents investment returns from a company located in another jurisdiction. Without knowing the beneficial owners of the originating company, it is difficult to say whether the transfer does in fact represent a return on investments, or whether it is in fact a bribe or somehow related to corruption.

The involvement of legal persons and arrangements can also make it more difficult for LFIs to identify a customer's true source of wealth. A legal person that is represented as a profitable business, for example, may in fact be a shell company that merely passes on income from illicit sources.

2.1.4. Common Typologies of Abuse of Legal Persons and Arrangements

The use of shell companies: Shell companies, commonly defined as companies that have no significant operations or related assets, may have legitimate business purposes. A shell company's lack of employees and physical presence, however, makes it possible to abuse it as a vehicle for illicit transactions. These features also make it very difficult for law enforcement agencies in jurisdictions where the company operates to investigate its owners and activities.

Case Study: Shell Companies

A group of individuals conducted an investment fraud scheme which promised victims high returns on an initial investment of USD 35,000. As part of the scheme, the group established a complex web of bank and brokerage accounts and shell companies in the United States and several foreign jurisdictions. The group also opened cash management accounts at brokerages utilizing the shell corporations. Investors were told to send their investment funds to the accounts established utilizing the shell corporation names. Once in this account, the funds were transferred to secondary accounts. From these accounts, the funds were then disbursed to various foreign and domestic accounts and liquidated through the use of checks, debit cards, and ATM cards.

Complex ownership and control structures: Individuals who seek to hide their interest in a company may create multiple layers of ownership and control that make it difficult to identify who really owns and controls the company. For example, a company may be owned by a second legal person, that is in turn owned by three legal persons, that are controlled via a debt financing arrangement. Where directors are required to be reported to the registering authority, a company may name legal persons as directors, further complicating the control structure.

Case Study: Complex Ownership

Company G was 95% owned by Mr. A and 5% by Mr. B. Company G purchased a power generator from Company K, owned by Company R in the Cayman Islands. Company R was linked to Panamanian Foundation P, which had Mr. A and his spouse as beneficiaries. Company G leased the generator to Company E, receiving amounts cleared by Company L The funds were drawn against Company K's bank account, and Company G made payments to Company K to settle a debt. The funds were credited to the accounts of Companies S, T and R.

Use of nominee shareholders and directors: Nominee arrangements involve an individual (the nominator) assigning his or her shares or voting rights to a second individual (the nominee) who agrees to act in accordance with the wishes of the nominator. The nominee is listed as the shareholder or director of record, but in fact has no power to direct the company and does not have a legal ownership right over the benefits accruing to the ownership interest, such as dividends. Nominee relationships may be contractual or based on a handshake agreement. Such informal arrangements often involve a nominator and nominee who are close associates or family members.

Case Study: Informal Nominee Shareholders and Directors

A Russian state agency contracted with Company 1 and Company 2 to perform software development. Neither company had the relevant expertise; they each hired subcontractors to do the work. The majority of funds received by both companies were funnelled into foreign shell companies, invested in real estate, or used to purchase luxury goods. Company 2 had previously been owned by Mr. X, who transferred the ownership to complicit associates. The real estate company that received the investment funds was owned by Mr. X's daughter. Mr. X also controlled the nominal owners of Company 1, who received a salary from the company. Mr. X was the brother of the director of the state agency's research department.

Use of intermediaries: Individuals seeking to create complex, opaque corporate structures will often seek out professional intermediaries (lawyers, accountants, and trust and company service providers (TCSPs)) who are experienced in bending and manipulating the rules in the jurisdiction where the legal person or arrangement is formed. Intermediaries may create new legal persons or arrangements, or sell the rights to existing legal persons that appear to have been in operation for some time. These intermediaries may also serve as directors, nominees, or trustees of the resulting legal persons and arrangements.

Case Study: Use of Intermediaries

Companies registered in New Zealand by a Vanuatu-based TCSP operated by New Zealand citizens were suspected of acting as shell companies that facilitated crime in foreign jurisdictions. The TCSP acted as nominee shareholders and provided nominee directors who resided in jurisdictions such as Vanuatu, Panama and the Seychelles. The TCSP also provided a New Zealand-based nominee director to satisfy the legal requirement to have a New Zealand resident director and address. By 2010, the TCSP had registered approximately 2,000 companies in New Zealand on behalf of clients in foreign jurisdictions. Its address, in Auckland, was used as the registered office for most of the companies. Authorities suspect that at least 73 of these companies facilitated crimes in foreign jurisdictions.

2.2. Features and Controls that Mitigate the Risk of a Legal Person or Arrangement

At a high level, features and controls that affect the vulnerabilities of legal persons and arrangements can be divided into four categories:

- The formation process and requirements to establish the legal person or arrangement;
- The identification of the individuals actually owning and controlling legal persons and arrangements;
- The reporting and recordkeeping requirements imposed on companies throughout their lifetime; and
- The formation authority's supervisory regime and enforcement tools.

The subsections that follow briefly discuss the various measures that—if effectively implemented—can help mitigate the vulnerabilities of legal persons and arrangements.

LFIs should be aware of the risks associated with all customer types, including legal persons and arrangements established outside the UAE. Appropriately assessing these risks will often involve developing an understanding of the controls in place to ensure transparency.

CBUAE recognizes that LFIs do not control the legal frameworks governing their customers. Nevertheless, CBUAE recommends that LFIs familiarize themselves with the features of the company forms most commonly found within their customer base, and the controls in place in the jurisdictions where their legal person customers are most commonly registered. LFIs should also consider seeking some or all of the following information in order to understand legal person and legal arrangement risks, particularly when conducting enhanced due diligence on legal person and legal arrangement customers that pose higher risks.

2.2.1. Formation Requirements and Process

Abuse of legal persons and arrangements for ML/TF/PF often includes the creation of complex ownership structures with many such entities—including entities of different types and in different jurisdictions; the use of one-time 'disposable' entities that are abandoned after they have served their purpose; or the use of previously inactive 'shelf companies. In addition, illicit actors will be able to more easily transact anonymously if they are required to reveal only minimal information during the formation process, can rely on nominees, or can complete processes without face-to-face interaction. For these reasons, legal persons and arrangements in jurisdictions whose formations processes allow for rapid, remote, and inexpensive formation and registration may be more attractive to illicit actors.

2.2.2. Identification and Reporting of Beneficial Owners

Because anonymity is one of the greatest attractions for illicit actors who seek to abuse legal persons and arrangements, they are likely to gravitate towards jurisdictions and company forms that require them to provide minimal information about the entities and themselves and that make it difficult for third parties to identify who in fact owns and controls the entity. The following controls that may be applied by the jurisdiction registering the entity in question can, to a certain extent, reduce the vulnerabilities created by corporate opacity.

- The registering authority collects key information about the company (such as name, address, and the names of directors) at formation and makes it available to the public;
- The registering authority collects the identities of all beneficial owners, or all beneficial owners owning at least a given percentage of the company, at the time of establishment, and makes this information available to domestic and foreign law enforcement, as well as AML/CFT regulated entities.
    - The threshold for identifying ownership should be in line with international and UAE standards.
    - Where the registering authority applies a threshold that exceeds 25% of the ownership interests in a legal person, LFIs should be aware that the customer is not required to report all individuals qualifying as beneficial owners in the UAE;

- The legal person or arrangement is prohibited from being owned by another legal person or arrangement;
- Nominee shareholders and directors are prohibited, or are appropriately regulated.

2.2.3. Reporting and Recordkeeping

Unlike individuals, legal persons and arrangements can swiftly change fundamental elements of their identity, rendering information provided during the formation process obsolete. Legal persons and arrangements can also compartmentalize information about themselves so that no single individual possesses full information about the entity. Because legal persons and arrangements abused for ML/TF/PF may not engage in licit commercial activity and may be controlled by only a small number of closely connected individuals, there is little commercial rationale for such entities to maintain adequate books and records. Illicit actors take advantage of these features by purchasing already-established companies "off the shelf;" selling companies to new owners; changing the company name; or failing to maintain records of their ownership. These vulnerabilities can, to a certain extent, be mitigated through effective controls, such as:

- Legal persons and arrangements are required to promptly update the registering authority if their key information (including beneficial ownership) changes;
- Legal persons and arrangements are required to appoint a resident agent in the jurisdiction where they are established to respond to inquiries;
- Legal persons and arrangements are required to make annual financial reports to their registering authority and/or to undergo a regular audit and provide the audit report to their registering authority.

2.2.4. Supervision

The effectiveness of any regime of controls over legal persons and arrangements depends on the consistency with which such controls are enforced and on the sanctions available to the supervisor and law enforcement.

- Legal persons and arrangements are monitored by their supervisor for their compliance with requirements;
- The supervisor can and does levy substantial penalties, whether civil or criminal, for violations of these requirements.

3. Legal Persons and Arrangements in the UAE

The UAE has a complex regime for formation of legal persons and arrangements, with 39 corporate registrars across the Emirates, the Commercial Free Zones (CFZs), and the Financial Free Zones (FFZs). Historically, each registrar has its own processes, but following the passage of AML-CFT Decision, which institutes common basic standards for all registrars, these processes are being harmonized across the UAE.

Certain information on legal persons doing business in the UAE is publicly available through the National Economic Register. For entities with a UAE business license, the National Economic Register contains the entity's license number, address, business activities, and the name of a manager. LFIs are encouraged to consult the Register when conducting CDD on legal persons, but should not rely on information contained in the Register without independently verifying it with the customer.

3.1. Identification of Beneficial Owners

Under AML-CFT Decision, all registrars of legal persons in the UAE must comply with the following requirements:

- Registrars must provide the public with information on the types and features of companies they establish, the process for creating those companies, and the process by which members of the public can obtain information on those companies, including on the beneficial owner(s).

- Registrars must obtain and maintain certain basic information on each company they register, including its name, address, a list of directors, its legal form, and its founding statutes.
- Registrars must identify the beneficial owners of each company they register, defined as any individual owning or controlling at least 25 percent of the company.

In addition, all legal persons in the UAE are required to:

- Maintain accurate and up to date information on their shareholders and beneficial owners;
- Identify nominee shareholders and directors to their Registrar; and
- Appoint an individual resident in the UAE to be responsible for providing this information to the Registrar.

Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures further defined these requirements. All legal persons in the UAE must be licensed or registered, must identify their beneficial owners, and must hold accurate, up-to-date information on their beneficial owners in a Register of Beneficial Owners. They must also report the same information to the relevant registrar. The Resolution also requires that nominee directors identify themselves to the legal person for which they serve as director, and this information must also be included in the legal person's Register.

There are certain limited exemptions to this requirement. For example, legal persons that are publicly traded on a stock exchange, or that are owned by such a company, do not have to identify or report their beneficial owners because of other transparency-related measures and obligations associated. In addition, if no individual meets the threshold by owning at least 25% of a legal person, that entity can report an individual who controls the entity (such as its managing director) instead of a true beneficial owner.

Together, these requirements aim to ensure that customers that are legal persons established and registered under the laws of the UAE must identify their beneficial owners and must always have up-to-date information on these individuals available. LFIs cannot rely solely on customers' statements and must verify the identity of beneficial owners independently. But a UAE-based legal person customer that claims to be unfamiliar with the requirements, or represents that it has never been required to identify its beneficial owners, may not be in compliance with the law and should be treated as at least high risk.

3.2. Legal Arrangements Under UAE Law

Two types of legal arrangements can be formed under UAE law:

- **Trusts** can be formed in the Mainland as well as in the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM). In a trust arrangement, the owner of certain funds, known as the settlor, places these funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.
- **Awqaf** (singular **waqf**), also known as endowments, can be created on the Mainland. Awqaf are a form of legal arrangement created according to shari'a law. A waqf allows a property owner to endow certain assets (often real property, but also shares or other income-producing assets) for the benefit of family members or a charitable cause. The endower loses control and ownership of the assets, which are registered as endowed and managed by a supervisor or trustee. Many awqaf are directly managed by the General Authority for Islamic Affairs and Endowments, but others are privately superintended.

Under AML-CFT Decision, Articles 9 and 37, trustees of legal arrangements, or persons holding analogous positions in other legal arrangements, are required to hold accurate and up-to-date information on the beneficial owners of the trust or other legal arrangement. For legal arrangements, the beneficial owners are defined as the settlor, the trustee, and the beneficiaries or identifiable class of beneficiaries, along with any other individual exercising ultimate effective control over the legal arrangement. Under Article 9 of AML-CFT Decision, LFIs must identify these individuals as the beneficial owners of their legal arrangement customers.

In both cases, it is important for financial institutions to be aware that these legal arrangements allow for an individual to legally hold and control funds that he or she does not own and does not have the right to benefit from. A trustee of a trust or waqf may open an account for trust funds under his or her own name, so that the account appears to belong to an individual rather than a legal arrangement. Although trustees are required to disclose their status, LFIs, as part of Customer Due Diligence (CDD), should take a proactive approach to identifying whether a customer is a trustee. This may include directly asking customers whether they are acting as trustees.

3.3. Economic Substance Requirements

Under Cabinet Resolutions (31) of 2019, (7) of 2020, and (57) of 2020, UAE legal persons operating in certain sectors with relevant income must meet requirements related to the level of core business activities that they carry out in the UAE (the Economic Substance Test). All firms conducting any of the following activities must pass the annual Economic Substance Test:

- Banking;
- Insurance;
- Investment Funds Management;
- Lease-Finance;
- Headquarters operations;
- Shipping;
- Holding Company activities;
- Intellectual Property;
- Distribution and service centres.

In order to pass the test, these firms are required to make an annual report, the Economic Substance Report, to their registrar showing that they in fact carry out core income-generating activities within the UAE, that these activities are directed and managed from the UAE, that the firms maintain an appropriate number of employees, and that the firms have appropriate physical premises. The report is then reviewed by the Federal Tax Authority, which makes a determination as to whether the criteria for economic substance have been satisfied. The Economic Substance Report is not currently available to financial institutions directly, but LFIs may request an attested copy of the Report from their customer or prospective customer.

The Economic Substance Test could help reduce the likelihood that UAE companies in these sectors are shell companies. The Economic Substance Test is retroactive, however, with companies required to submit Reports at the end of the twelve-month period in which the qualifying activity took place. In addition, Reports may not be promptly reviewed. LFIs should not rely on a customer's assertion that it has passed the Economic Substance Test and must conduct appropriate customer due diligence, as discussed in section 4.3 below. This may include requesting the customer's Economic Substance Report from the customer itself.

4. Mitigating Risk

Legal persons and arrangements are an important part of LFIs' customer base and of economic activity in the UAE. However, legal persons and arrangements create real, and diverse, risks for financial institutions. LFIs are not expected to prohibit legal person and arrangement customers. Instead, they must understand, manage, and mitigate the risk through the appropriate application of preventive measures required under AML-CFT Decision and CBUAE directives and guidance documents.

This section describes LFIs' obligations under UAE Law with specific reference to legal persons and arrangements. It is not a comprehensive discussion of all requirements imposed on LFIs. LFIs should consult the Laws and regulations including AML-CFT Decision and the CBUAE's Anti-Money Laundering the Combating the Financing of Terrorism and Illegal Organizations Guidelines. The controls discussed below must be integrated into the LFI's larger AML/CFT compliance program, and supported with appropriate governance and training.

4.1. Requirements for Legal Person and Arrangement Customers Under AML-CFT Decision

Under Article 8(b) of AML-CFT Decision, when conducting CDD on legal persons and arrangements, LFIs must collect the following information and verify it based on documents from a reliable and independent source:

- The name [this may not apply for legal arrangements], Legal Form and Memorandum of Association;
- Headquarters' office address or the principal place of business; in addition, if the legal person or arrangement is a foreign entity, the name and address of its legal representative in the State;
- Articles of Association or any similar documents, approved by the relevant authority within the State;
- Names of relevant persons holding senior management positions in the legal person or legal arrangement.

Legal persons and arrangements, by definition, cannot take action on their own and must be represented by a natural person. Therefore, for all legal persons and arrangements the LFI must verify that the individual acting on behalf of the customer is authorized to do so, and conduct CDD on that person as required by Article 8(a) of AML-CFT Decision.

In addition to the information described above, under Article 9 of AML-CFT Decision, the LFI must take reasonable measures to identify the beneficial owner(s) of all legal person and legal arrangement customers.

- For legal persons, LFIs must at least obtain and verify the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. If no individual can be identified, the LFI must identify the individual(s) holding the senior management position(s) within the legal person customer.
- For legal arrangements, LFIs must verify the identity of the settlor and the trustee (or anyone holding equivalent positions for non-trust legal arrangements), the beneficiaries or class of beneficiaries, and any other individuals in control of the legal arrangement. LFIs must also obtain sufficient information on the beneficial owners of a legal arrangement to enable verification of the beneficial owner when paying trust funds to the beneficial owner, or when the beneficial owner begins to exercise his or her legally acquired rights. (This may take place, for example, when a beneficiary of a trust reaches his or her majority and takes full control and ownership of the trust funds.)

As stipulated by Article 10 of AML-CFT Decision, LFIs may omit collecting information from the customer to identify the beneficial owner of a legal person or arrangement customer only in two narrowly defined circumstances, which both apply to legal persons only:

a) The customer is a company listed on a regulated stock exchange and subject to disclosure requirements that ensure adequate transparency with regards to the customer's beneficial owner(s);
b) A subsidiary whose majority shares or stocks are held by the shareholders of the holding company.

In both cases, LFIs must still identify the beneficial owner(s) using reliable public sources. LFIs must also verify that the customer does in fact qualify for the exemption. LFIs remain responsible for using a risk-based approach and for ensuring that they understand their customer. LFIs should not seek to take advantage of this exemption if they cannot identify the beneficial owner(s) using reliable public sources. LFIs are unlikely to find reliable public information on the beneficial owners of privately-held holding companies.

In all cases, LFIs are also required by Article 8.4 of AML-CFT Decision to understand the customer's ownership and control structure.

4.2. The Risk-Based Approach, Customer Risk Rating, and the Institutional Risk Assessment

LFIs should take a risk-based approach to the preventive measures they put in place for all customers, including legal persons and arrangements. A risk-based approach means that LFIs should dedicate compliance resources and effort to customers, business lines, branches, and products and services in keeping with the risk presented by those customers, business lines, branches, and products and services, as assessed in accordance with Article 4 of AML-CFT Decision.

The risk-based approach has three principal components:

1. Conducting an enterprise risk assessment, as required by Article 4.1 of AML-CFT Decision.

The enterprise risk assessment should reflect the presence of legal persons and arrangements in an LFI's customer base. The risk assessment should consider the most common forms of legal persons and arrangements in the LFI's customer base and should assess the risks of each form. This assessment should carefully consider and incorporate the ML/TF risks legal persons and arrangements pose to LFIs discussed above (section 2.1), although LFIs may have legal person and arrangement customers from outside the UAE whose risks will also need to be assessed. These assessments should in turn be reflected in the LFI's inherent risk rating.

In addition, the LFI's risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its legal person and arrangement customers, including the preventive measures discussed below.

2. Identifying and assessing the risks associated with specific customers.

The LFI should assess the risk of each customer to identify those that require enhanced due diligence (EDD). Customer risk assessment for legal person and arrangements should incorporate at least all elements of the customer risk assessment for individuals, but should apply them both to the legal person or arrangement customer itself and to the individuals prominently associated with it. For example, the assessment of the legal person or arrangement's jurisdictional risk should take into consideration not just the customer's jurisdiction of establishment, but also the residence and nationality of the beneficial owners, senior manager, and directors.

Other risk assessment considerations that are unique to legal person and arrangement customers include:

- The legal form of the customer, and the controls in place to ensure transparency;
- The status of the beneficial owners and senior management. For example, if a beneficial owner or senior manager of a customer is a PEP, as defined in Article 15 of AML-CFT Decision, the customer may also need to be treated as PEP, depending on the extent of the PEP's ownership and control and his or her relationship to the other beneficial owners or managers.

3. Applying EDD and other preventive measures to customers the LFI determines to be higher-risk, as required by Article 4.2(b) of AML-CFT Decision, or to specific customer types, no matter their risk rating, as required by AML-CFT Decision.

Many EDD measures for legal persons and arrangements are the same as those applied to individual customers. EDD measures that are specific to legal person and arrangement customers are discussed in section 4.3 below.

Under AML-CFT Decision, the legal person customer types for which enhanced or special due diligence is required are:

- Legal persons based in high-risk countries (Article 22);
- Financial institutions with which the LFI proposes to enter into a correspondent relationship (Article 25);
- Legal person customers that are fully owned or controlled by PEPs, their direct family members, or their close associates (Article 15). If a PEP, a direct family member, or an associate is a partial owner of a customer, LFIs may take a risk-based approach to applying EDD to the customer.

- Non-Profit Organisations (Article 33).

4.3. Customer Due Diligence and Enhanced Due Diligence

CDD, and, where necessary, EDD are the core preventive measures that help LFIs manage the risks of legal person and legal arrangement customers. Because of this, LFIs are prohibited from maintaining anonymous accounts, and from onboarding any account or customer with fictitious names or characteristics. LFIs must perform CDD on every customer.

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFI's services. Therefore, the LFI must identify customers that are legal persons and legal arrangements. When the customer is a legal person or arrangement, the process of understanding the customer ("knowing your customer") is more complex and requires additional steps.

Where an LFI cannot satisfy itself that it understands a legal person or legal arrangement-including when it has doubts that it has identified the individuals who truly own and control the legal person or legal arrangement—then it must not accept that legal person or legal arrangement as a customer. If there is an existing business relationship, the LFI should not continue it. LFIs should also consider filing a Suspicious Transaction Report, as discussed 4.4 below.

4.3.1. Core Elements of Customer Due Diligence

LFIs are reminded that all elements of CDD (and EDD) apply to customers that are legal persons and legal arrangements. LFIs should refer to the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* for a full discussion of CDD obligations. CDD obligations include, but are not limited to, the requirement that LFIs, using a risk-based approach:

- Identify the customer and verify if the customer's identity is reliable by using independent sources (discussed in this section);
- Identify beneficial owners of the customer (discussed in section 4.3.2 below);
- Assess and understand customer risk (discussed in section 4.2 above);
- Obtain information on the purpose and intended nature of the account (discussed in section 4.3.3 below); and
- Ensure ongoing due diligence is conducted and that the business relationship and transactions are scrutinized in the course of the relationship (discussed in section 4.3.4 below).

LFIs must maintain records of the customer information obtained through CDD to enable the LFI to demonstrate compliance to CBUAE and to comply with requests for information from competent authorities.

As discussed above in section 4.1, LFIs must identify legal person customers by collecting the following information and verifying it using independent, reliable sources:

- The name [this may not apply for legal arrangements], Legal Form and Memorandum of Association;
- Headquarters' office address or the principal place of business; in addition, if the legal person or arrangement is a foreign entity, the name and address of its legal representative in the State;
- Articles of Association or any similar documents, approved by the relevant authority within the State;
- Names of relevant persons holding senior management positions in the legal person or legal arrangement.

Verification of information collected to identify the customer should be risk-based. In standard cases, verification should rely on government-issued or certified documents, such as business licenses and notarized copies of the legal person's memorandum of association. Where risks are lower, LFIs may consider using non-documentary sources, such as public registries, including the registries maintained by company registrars in the UAE. Consulting a

registry, however, is not a replacement for collecting the documents specifically required by the AML-CFT Decision, even if the customer was required to submit the same documents to the registry.

4.3.2. Identification of Beneficial Owners and of Ownership and Control Structure

4.3.2.1. UAE Requirements

As discussed in section 4.1 above, the UAE requires all financial institutions to identify the beneficial owners of a legal person customer by **obtaining and verifying the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more**. Where no such individual meets this description, the LFI must identify and verify the identity of the individual holding the senior management position in the entity.

The AML-CFT Decision does not define "senior management position," and LFIs should make a judgment, based on the specific facts and circumstances, as to the individual who meets this description. The senior management official should be a single individual with significant responsibility to control, manage, or direct a legal person customer. This may include the entity's Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Director, General Partner, or President.

LFIs should consider whether the individual's background, experience, and expertise make it plausible that they would indeed hold a position of responsibility at a legal person of the customer's size. Where a customer identifies a relatively young or inexperienced individual as its senior manager, that may be a sign that the individual does not in fact control the customer and instead takes orders from another individual who wishes to obscure his or her identity.

For legal arrangement customers, LFIs must **verify the identity of the settlor and the trustee (or anyone holding equivalent positions for non-trust legal arrangements), the beneficiaries or class of beneficiaries, and any other individuals in control of the legal arrangement**.

The beneficial owner of a legal person or arrangement must be an individual. Another legal person or arrangement cannot be the beneficial owner of a customer, no matter what percentage it owns. LFIs must continue tracing ownership all the way up the ownership chain until it discovers all individuals who own or control at least 25% of the LFI's customer.

When the LFI has identified qualifying beneficial owners, it should perform CDD on each individual beneficial owner, in accordance with the requirements of Article 8.1(a) of AML-CFT Decision. Where the customer is a UAE legal person, LFIs may require the customer provide the beneficial ownership report it has submitted to its company registrar as per Cabinet Decision (58). This should not be a substitute, however, for independent identification of beneficial owners by the LFI.

LFIs are also required to understand the customer's ownership and control structure. This means that LFIs must be aware of who owns the customer, even if they have not verified the identity of the individuals owning every company in the customer's ownership chain. LFIs should have confidence that they fully understand who has the power to direct and control their customer's actions.

4.3.2.2. Applying a Risk Based Approach

It is important to note that the legal requirements mentioned above (section 4.3.2.1) are baseline obligations rather than definitions of beneficial ownership. A beneficial owner, as defined in AML-CFT Decision, is any individual who owns or controls all or part of a legal person. This means that a legal person can have several beneficial owners, not all of whom are required to be identified under the law. LFIs should always identify and verify the identity of all individuals owning or controlling at least 25% of a legal person, **but they should also make a risk-based decision as to whether to identify and verify the identity of additional beneficial owners**. For legal person customers that require

EDD, whether as a function of law or because they are higher risk, LFIs should always consider lowering the ownership threshold below 25%.

LFIs should be aware that even minority owners of a legal person customer can exercise control over the legal person through information arrangements, family relationships, and specific governance arrangements (e.g. preferred stock), among other methods. Customers whose minority owners include individuals that are subject to United Nations or UAE sanctions may also create serious risks for LFIs, even if the individual only owns a small share of the customer (see section 4.5 below). Thus, particularly in higher risk scenarios, LFIs should consider completing an ownership and control chart that includes at least the names of all beneficial owners of every legal customer, or all individuals owning at least 5% of the customer. Collecting the names of beneficial owners is distinct from identifying them and verifying their identity and does not require the LFI to collect identifying information. LFIs must still identify and verify the identity of all individuals owning at least 25% of legal person customers.

Beyond lowering the ownership threshold, EDD methods related to identification of ownership and control can include requiring the beneficial owners of customers to verify their ownership by presenting share certificates or contracts.

Example 1: Company A is a UAE-based company that leases office space. Company A applies to open an account with Bank Lion, a CBUAE-supervised LFI. Bank Lion verifies that Company A is 50% owned by Mr. Y and 40% owned by Ms. W. Bank Lion is aware that Company A has additional owners, but knows they own less than 10% of Company A.

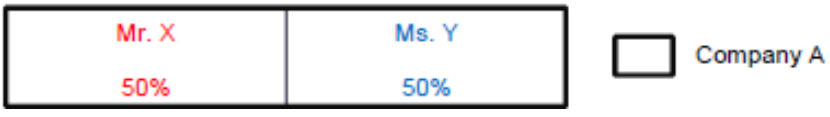
Because Company A is a low-risk domestic firm, Bank Lion is not required to identify the additional owners of Company A.

Example 2: Company B is a Cayman Islands-based company with no business operations and a letterbox address on the premises of a known Cayman Islands TCSP. Company B applies to open an account with Bank Lion, a CBUAE-supervised LFI. Bank Lion verifies that Company B is 50% owned by Mr. Y, a citizen of Russia and 40% owned by Ms. W, a citizen of Malta.

Company B is likely a shell company, and its known beneficial owners are from high-risk jurisdictions. Therefore, Bank Lion decides to take the step of identifying and verifying the identity of the individuals who owns the remaining 10% of the company before accepting Company B as a customer. It discovers that the remaining 10% of shares are owned by Mr. Y's father, a well-known Russian businessman. Because Mr. Y is only 22 and a recent university graduate, Bank Lion suspects that Mr. Y is a nominee and that his father may be the true controlling owner of Company B.

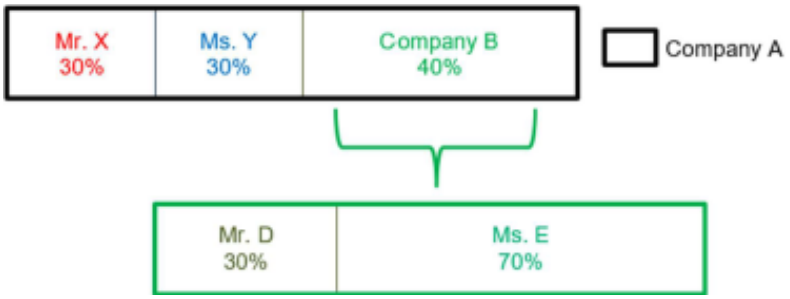
4.3.2.3. Legal Persons – Common Situations

In many cases, identifying the beneficial owners of a legal person customer will be a straightforward process. A customer may be directly owned by one or two individuals:



In such cases, an LFI is obliged to identify and to verify the identity of both individuals, Mr. X and Ms. Y.

Legal persons may have more complex ownership structures, however, in which other legal persons are involved in the ownership chain. In such cases, LFIs must continue up the chain until they identify an individual:

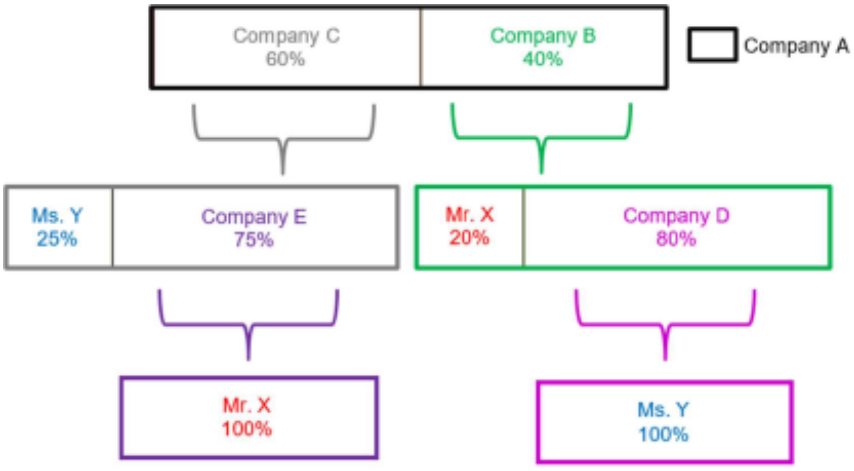


In this situation, the owners of Company A are as follows:

Owner	Share	Ownership Type
Mr. X	30%	Direct
Ms. Y	30%	Direct
Ms. E	28%	Indirect - Ms E owns 70% of Company B, which in turn owns 40% of Company A
Mr. D	12%	Indirect - Mr. D owns 30% of Company B, which in turn owns 40% of Company A

Mr. X, Ms. Y, and Ms. E must all be identified under UAE law, as they own at least 25% of Company A. Mr. D owns 12%, so he is not required to be identified. But the LFI should make a risk-based decision as to whether to identify him.

Illicit actors may seek to use complex ownership structures to hide the fact that they own 25% or more of the customer. This is why it is important for LFIs to use a risk-based approach and to be confident that, at the end of the process, they fully understand who controls their customer.



In this situation, although it at first appears that Ms. Y and Mr. X each own less than 25% of Company A, in fact between them they own 100% of the company. Their ownership interests can be calculated as follows:

Mr. X:

- 20% of Company B, which owns 40% of Company A: 20% of 40% is **8%**; *plus*
- 100% of Company E, which owns 75% of Company C, which owns 60% of Company A: 100% of 75% of 60% is **45%**.
- Mr. X owns **53%** of Company A.

Ms. Y:

- 25% of Company C, which owns 60% of Company A: 25% of 60% is **15%**; *plus*
- 100% of Company D, which owns 80% of Company B, which owns 40% of Company A: 100% of 80% of 40% is **32%**.
- Ms. Y owns **47%** of Company A.

Both Mr. X and Ms. Y must be identified under UAE law. In addition, LFIs should be aware that Mr. X and Ms. Y are likely associated parties and should question whether there is a legitimate economic purpose for the ownership structure of Company A.

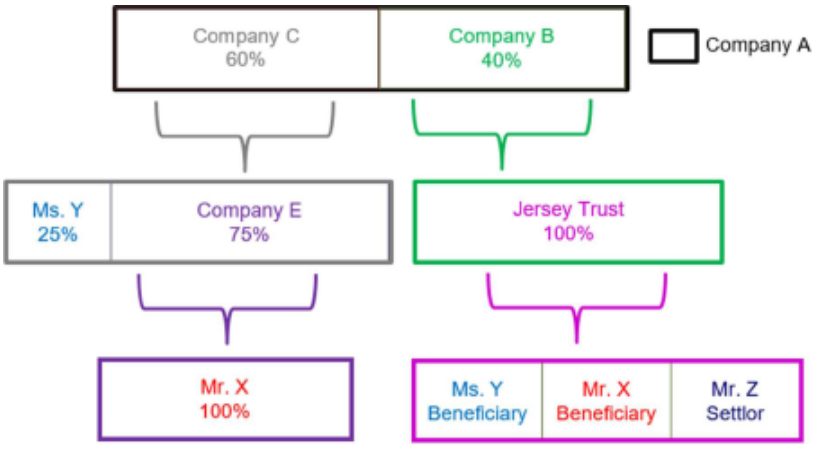
4.3.2.4. Legal Arrangements - Common Situations

Legal arrangements may not present the layered ownership structures seen in legal persons. This does not mean, however, that identifying the beneficial owners of legal arrangements is always straightforward. In particular, the very different forms of legal arrangements that may be formed in different jurisdictions can make it difficult to identify the individuals who hold roles analogous to settlor, trustee, and beneficiary. LFIs should always identify the following individuals:

- The legal entities or individuals who have the power to control the property of the legal arrangements. These legal entities or individuals are analogous to trustees. If a legal entity (such as a financial institution) acts as trustee, LFIs must identify the beneficial owners of that legal entity.
- The legal entities or individuals for whose present or future benefit the trustees are safeguarding the legal arrangement property. These legal entities or individuals are analogous to the beneficiaries.
    - Beneficiaries may be defined as a class which can change over time (e.g., "all the underage grandchildren of the settlor").
    - LFIs should identify the class of beneficiaries, and all beneficiaries currently in existence, at the time of onboarding the customer. During periodic CDD refresh, they should ascertain whether additional identifiable individuals have joined or left the beneficiary class (e.g. a new child has been born, a beneficiary has come of legal age).
    - If a legal entity is the named beneficiary, LFIs must identify the beneficial owners of that legal entity.
- The legal entities or individuals who assigned control of the legal arrangement property to the trustees (or individuals holding a similar position). This individual or legal entity is analogous to the settlor. A settlor may or may not retain underlying legal ownership of the legal arrangement property. If a legal entity acts as settlor, LFIs must identify the beneficial owners of that legal entity.

In addition, where trustees are financial institutions, lawyers or any other professional with secrecy rules in a foreign jurisdiction, it may be difficult to obtain the information LFIs need. LFIs should be aware that if they cannot obtain this information, they should not establish the business relationship or continue an existing relationship.

Legal arrangements may also be part of the ownership structures of other legal persons or arrangements. Because trusts do not have shares or equity, LFIs should treat all participants in a trust or similar legal arrangement as if they own 100% of the legal arrangement.



In the example above, Company A is 40% owned by Company B, which is in turn wholly owned by a trust established in the Isle of Jersey. Ms. Y and Mr. X are beneficiaries of the trust and also indirectly own shares of the Company A through Company C. Mr. X has to be identified and verified based solely on his indirect 45% ownership of Company A

through Company E. Ms. Y and Mr. Z, must also be identified and verified because they are beneficial owners of a legal arrangement that owns 40% of Company A.

4.3.3. Understanding the Purpose of the Account and Nature of the Customer's Business

For all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This step requires the LFI to collect information that allows it to create a profile of the customer and of the expected uses to which the customer will put the LFI's services. Because almost all legal persons and arrangements are created to make it easier to do business, invest assets, or engage in some form of organized activity, this element of CDD is critical to understanding customers who are legal persons and arrangements.

Legal persons and arrangements engage in an extremely wide variety of financial activity, potentially a wider variety than individual customers are likely to display. The activity profile of a cash-intensive business such as a taxi firm will be completely different from that of an investment vehicle or of a waqf that collects revenues from real property and distributes them to charitable causes. But specific legal person and arrangements customers are also likely to engage in patterns of activity that remain constant from month to month and year to year. Understanding the purpose of the account allows LFIs to develop expected patterns and compare them to actual behaviour. For example:

- A taxi company is likely to see substantial cash inflows and make regular, predictable transfers to cover payroll and to a limited set of suppliers (e.g. mechanics, gas stations). If a taxi company starts making transfers to a foreign jurisdiction, even a low-risk one, that behaviour may not fit the expected pattern and if so would require investigation.
- A waqf managing an apartment building should receive very regular monthly rent payments from residents, whether by cash, check or Automated Clearing House. The waqf should have regular expenses for maintenance and property taxes, as well as predictable payments to the beneficiaries of the waqf. If the waqf suddenly doubles its cash deposits, the LFI will need to investigate to understand why the customer's behaviour has changed.

Understanding the nature of the customer's business can be a straightforward process. Most legal person customers will be engaged in familiar, easily identifiable activities in recognized sectors: manufacturing, retail, agricultural production, etc. In other cases, it may not be so simple. A legal person customer may be formed solely to facilitate a complex financial transaction. In other cases, the legal person may not have fully determined their business model or may plan to engage in a business activity that is out of keeping with the owners' and managers' resources and expertise, or that don't seem to make economic sense. Finally, a customer may try to conceal its actual business; for instance, a company that is engaged in computer hacking and fraud may describe itself as a software engineering firm or a call centre.

As LFIs advance efforts to understand their customer's business and financial activities, they should consider whether aspects of the customer profile require EDD. The following are some situations in which EDD may be appropriate:

- The customer has business or other ties to high-risk jurisdictions (if the customer or its beneficial owners are based in a high-risk jurisdiction, EDD is mandatory).
- The customer is engaged in a high-risk sector. High-risk sectors can include, but are not limited to:
  - Sectors with high flows of cash;
  - Other financial sectors (e.g. customers who are MSBs or payment processors);
  - Sectors that involve the import or export of dual-use technology (technology that may be used for proliferation);
  - Sectors that are at high risk for human trafficking (bars and dance venues; construction; cleaning);
  - Charitable activities, especially those involving high-risk jurisdictions.

- The customer is a state-owned-enterprise (SOE). SOEs engage in a wide variety of business activities; their close relationship to government and government officials means that they may be at higher risk for corruption-related transactions.
- The customer intends to use high-risk financial products and services, such as bulk cash services or purchase and exchange of virtual assets.
- The LFI does not fully understand the customer's business model or activities. Customers that generate revenue, but that have no apparent business activities, are perhaps the highest risk.

When conducting EDD on the business activities and account use of legal persons and arrangements, LFIs should use techniques designed to manage the specific risks of the customer. These may include, but are not limited to:

- Requiring the customer to provide invoices documenting incoming and outgoing transfers;
- Requiring the customer to provide its Economic Substance Report;
- For customers operating in licensed sectors, requiring the customer to provide proof that it has a valid business license;
- Inspecting payroll documents and other business records;
- Visiting the customer's business premises and interviewing its personnel;
- Requesting a reference from a current customer or other well-known firm with which the new customer claims to do business, or which operates in the same sector as the new customer.

4.3.4. Ongoing Monitoring

Like all customers, legal persons and arrangements must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

4.3.4.1 CDD Updating

LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. This is particularly crucial in the context of legal person and arrangement customers, which, by their very nature, can change their fundamental identity overnight. With the stroke of a pen, a company engaged in a low-risk business and owned by reputable UAE residents can move its activities to a high-risk sector and can transfer ownership to nationals of a high-risk foreign jurisdiction.

LFIs should update CDD on legal person and arrangement customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers, including legal persons and arrangements, should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular must ascertain that:

- The customer's beneficial owners remain the same;
- The customer continues to have an active status with a company registrar (this may not apply to legal arrangement customers);
- The customer has the same legal form and is domiciled in the same jurisdiction;
- The customer is engaged in the same type of business, and in the same geographies;
- The customer's transactions continue to fit its profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established.

If any of the above characteristics have changed, the LFI should risk-rate the customer again.

The LFI should conduct EDD when the revised risk rating demands it or if the customer's history of transactions is not consistent with its profile and with the expectations established at account opening. LFIs must always conduct

EDD when this is required by law (a beneficial owner of the customer is a PEP, as defined in Article 15 of AML-CFT Decision, or the customer or its beneficial owner is domiciled in a high-risk jurisdiction).

LFIs may consider requiring that the customer update them as to any changes in its beneficial ownership. Even if this requirement is in place, however, LFIs should not rely on the customer to notify it of a change, but must still update CDD on a schedule appropriate to the customer's risk rating.

4.3.4.2. Transaction Monitoring

As with all customers, LFIs must monitor activity by legal person and arrangement customers to identify behaviour that is potentially suspicious and that may need to be the subject of a Suspicious Transaction Report (see section 4.4 below). Legal persons, especially those that engage in commerce, are likely to engage a wider range of financial activity than are individual and most legal arrangement customers. This can make identifying suspicious behaviour by legal persons difficult.

As with other customer types, LFIs that use automated monitoring systems should apply rules that are designed to detect common typologies for illicit behaviour. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. For example, a series of transactions between two unconnected companies may not be cause for an alert. But if the companies are all owned or controlled by the same individual(s), the LFI should investigate to make sure that the transactions have a legitimate economic purpose.

Where possible, monitoring systems should also flag unusual behaviour that may indicate that a legal person customer's business has changed—for example, a first transfer to or from a high-risk jurisdiction, or a large transaction involving a new counterparty. LFIs should follow up on such transactions with the customer to discover whether the customer has changed its business model in such a way as to require a higher risk rating.

A list of red flags for illicit behaviour involving legal persons and arrangements is provided in the Annex to this Guidance.

4.4. Suspicious Transaction Report Filing

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file a Suspicious Transaction Report (STR) with the UAE Financial Intelligence Unit (UAE FIU) when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, the proceeds of crime, is related to a crime, or is intended to be used in a crime. STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. By filing STRs with the UAE FIU, LFIs alert law enforcement about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations involving legal persons or arrangements:

- A potential legal person or arrangement customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current legal person or customer cannot provide required information about its business or its beneficial owners;
- A legal person or arrangement customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the legal person or arrangement. In such cases, the LFI should not establish the business relationship, or continue an existing business relationship, and should also consider filing an STR.

Please consult the CBUAE's Guidance on Suspicious Transaction Reporting for further information.

4.5. Implementation of Targeted Financial Sanctions - Special Considerations for Legal Persons and Arrangements

Key Terms for Targeted Financial Sanctions

Affiliate is an entity owned by another entity by more than 25% and less than 50% of its capital.

Controlling shareholder is a shareholder who has the ability to directly or indirectly influence or control the appointment of the majority of the Board of directors, or the decisions made by the board.

Listed Person is a person or organization listed by the UN Security Council on the Sanctions List, or listed by the Cabinet on Local Lists, as the case may be.

Subsidiary is an entity owned by another entity by more than 50% of its capital or under full control of that entity regarding appointment of the Board of Directors.

Legal persons can be included on international sanctions lists. In addition, the obligation to freeze the funds of a listed person, imposed by AML-CFT Decision and by articles 15 and 21 of Cabinet Decision (74) of 2020, extends to funds that a Listed Person owns or controls through ownership or control of a legal person or through a legal arrangement.

Listed individuals and legal persons are known to seek to evade sanctions by hiding their interest in a transaction via complex layers of control and ownership, through informal nominee arrangements, and through the assistance of complicit professionals. Listed Persons may also use front companies-companies mixing legitimate and illicit economic activity—to conceal their activities. For this reason, identification of beneficial ownership through the entire corporate ownership structure is critical for effective sanctions implementation, as is fully understanding the nature of the customer's business.

LFIs that employ automated screening technologies to identify matches to sanctions lists must ensure that their screening tools include all individuals associated with a legal person customer, including beneficial owners, authorized signatories, directors, and senior management.

Legal persons and arrangements that are directly or indirectly (i) owned 50% or more in the aggregate, or (ii) controlled, by one or more Listed Person, including subsidiaries of a Listed Person, and entities where a listed person is a controlling shareholder, are subject to the same prohibitions as the Listed Person, even if such entities are not specifically listed by the UAE or the United Nations.

Financial institutions should observe caution when considering a transaction with an entity that is not a Listed Person in which one or more Listed Persons have a significant ownership interest that is less than 50 percent or which one or more Listed Persons may control by means other than a majority ownership interest. Such non-listed entities, to include affiliates, may become the subject of future designations or enforcement actions. As discussed above, LFIs should make a risk-based decision as to whether to identify beneficial owners who own or control less than 25% of the legal persona or arrangement. LFIs are not required to identify every beneficial owner in order to conduct sanctions screening. But should an LFI, in the course of enhanced due diligence, discover that a Listed Person owns a minority interest in a legal person, this information must be taken into consideration in risk-rating that customer.

Please see the Guidance on Targeted Financial Sanctions for more information on this issue.

LFIs should consult the CBUAE and the Supreme Council for National Security if they have any questions regarding implementation of UN or UAE sanctions. LFI employees must be trained on these issues as part of comprehensive ongoing training.

Example: Listed individual Ms. Y owns 25% of foreign Company A. Foreign Company A owns 30% of UAE Company B. Company B is a customer of UAE LFI Lion Bank. Ms. Y has no other ownership interests in Company B. Ms. Y therefore ultimately owns 7.5% of Company B.

Ms. Y's minority interest may not in itself give her ownership or control Company B. But Lion Bank should also consider the following factors when determining whether Ms. Y exercises control over Company B:

- The other beneficial owners of Company B are known close associates of Ms. Y's; and
- Ms. Y has loaned Company B a sum equal to 100% of its operating revenue in the previous financial year, and under the terms of the loan agreement, if Company B does not repay the loan Ms. Y will acquire an additional 35% of Company B.

When these factors are considered, it becomes likely that Ms. Y does in fact exercise control over Company B, despite her relatively small ownership stake, and transactions with Company B may therefore be prohibited under Cabinet Decision (20) of 2019.
Alternatively, if Company B operates in the high-tech manufacturing sector, and Ms. Y has been listed for proliferation activities, the LFI may conclude that the sanctions evasion risk posed by Company B is too great to permit accepting it as a customer, even if Ms. Y does not exercise control of the company.

4.6. Training

As will all risks to which the LFI is exposed, the AML/CFT training program must ensure that employees are aware of the risks of legal persons and arrangements, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls.

5. Lessons Learned and Examples from Amld Supervision

The CBUAE's examinations of LFIs have found that some LFIs struggle with key aspects of the preventive measures regime for legal persons. LFIs should take care to implement effective compliance programs, including by avoiding common deficiencies such as:

- **Incomplete and out of date CDD:** CBUAE has identified instances where CDD files are missing key information, such as the country of operation, the nature of the business, and the nationality of beneficial owners, shareholders, and directors. Equally important, CDD files are often out of date, with expired customer information.

- **Inadequate systems:** LFIs' systems for supporting CDD do not always mandate the collection of all required information or guide the compiler to supply complete information, such as the full name of a beneficial owner. LFIs' core banking systems may not be capable of linking or tracking related parties, which inhibits identification of suspicious behavior. In some cases, risk-rating and identification of UBOs is done manually, which increases the likelihood of user error or manipulation.

- **Incomplete risk-rating:** LFIs' risk rating tools for legal persons and arrangements did not always take into account critical information, such as the type of entity and the risk rating of beneficial owners.

Annex 1. Red Flags for Concealment of Beneficial Ownership

The following are indicators that Financial Action Task Force (FATF) member states have observed in connection to abuse of legal persons and arrangements. This is not an exhaustive list of every potential indicator of illicit activity involving legal persons and arrangements, but it represents a wide range of behaviours and activities that should prompt LFIs to investigate further, to consider closing or not opening an account, and to consider filing an STR.

Indicators Related to the Customer

- The customer is reluctant to provide personal information.
- The customer is reluctant or unable to explain:
    - their business activities and corporate history
    - the identity of the beneficial owner
    - their source of wealth/funds
    - why they are conducting their activities in a certain manner
    - who they are transacting with
    - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Individuals or connected persons:
    - insist on the use of an intermediary (either professional or informal) in all interactions without sufficient justification;
    - are actively avoiding personal contact without sufficient justification;
    - are foreign nationals with no significant dealings in the country in which they are procuring professional or financial services;
    - refuse to co-operate or provide information, data, and documents usually required to facilitate a transaction
    - are politically exposed persons, or have familial or professional associations with a person who is politically exposed;
    - are conducting transactions which appear strange given an individual's age (this is particularly relevant for underage customers);
    - have previously been convicted for fraud, tax evasion, or serious crimes;
    - are under investigation or have known connections with criminals;
    - have previously been prohibited from holding a directorship role in a company or operating a trust and company service provider (TCSP);
    - are the signatory to company accounts without sufficient explanation;
    - conduct financial activities and transactions inconsistent with their customer profile;
    - have declared income which is inconsistent with their assets, transactions, or lifestyle.
- Legal persons or legal arrangements:
    - have demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activities;
    - describe themselves as a commercial business but cannot be found on the internet or social business network platforms (such as LinkedIn, XING, etc.);
    - are registered under a name that does not indicate the activity of the company;
    - are registered under a name that indicates that the company performs activities or services that it does not provide;
    - are registered under a name that appears to mimic the name of other companies, particularly high-profile multinational corporations;
    - use an email address with an unusual domain (such as Hotmail, Gmail, Yahoo, etc.);
    - are registered at an address that does not match the profile of the company;
    - are registered at an address that cannot be located on internet mapping services (such as Google Maps);
    - are registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service;
    - where the director or controlling shareholder(s) cannot be located or contacted;
    - where the director or controlling shareholder(s) do not appear to have an active role in the company;

- where the director, controlling shareholder(s) and/or beneficial owner(s) are listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees;
- have declared an unusually large number of beneficiaries and other controlling interests;
- have authorised numerous signatories without sufficient explanation or business justification;
- are incorporated/formed in a jurisdiction that is considered to pose a high money laundering or terrorism financing risk;
- are incorporated/formed in a low-tax jurisdiction or international trade or finance centre;
- regularly send money to low-tax jurisdictions or international trade or finance centre;
- conduct a large number of transactions with a small number of recipients'
- conduct a small number of high-value transactions with a small number of recipients;
- regularly conduct transactions with international companies without sufficient corporate or trade justification;
- maintain relationships with foreign professional intermediaries in the absence of genuine business transactions in the professional's country of operation;
- receive large sums of capital funding quickly following incorporation/formation, which is spent or transferred elsewhere in a short period of time without commercial justification;
- maintain a bank balance of close to zero, despite frequent incoming and outgoing transactions;
- conduct financial activities and transactions inconsistent with the corporate profile;
- are incorporated/formed in a jurisdiction that does not require companies to report beneficial owners to a central registry;
- operate using accounts opened in countries other than the country in which the company is registered;
- involve multiple shareholders who each hold an ownership interest just below the threshold required to trigger enhanced due diligence measures.

- There is a discrepancy between the supposed wealth of the settlor and the object of the settlement.
- Individuals, legal persons and/or legal arrangements:

  - make frequent payments to foreign professional intermediaries;
  - are using multiple bank accounts without good reason;
  - are using bank accounts in multiple international jurisdictions without good reason;
  - appear focused on aggressive tax minimisation strategies;
  - demonstrate limited business acumen despite substantial interests in legal persons;
  - provide falsified records or counterfeit documentation;
  - appear to engage multiple professionals in the same country to facilitate the same (or closely related) aspects of a transaction without a clear reason for doing so.

- Examination of business records indicate:

  - a discrepancy between purchase and sales invoices;
  - double invoicing between jurisdictions;
  - fabricated corporate ownership records;
  - false invoices created for services not carried out;
  - falsified paper trail;
  - inflated asset sales between entities controlled by the same beneficial owner;
  - agreements for nominee directors and shareholders;
  - family members with no role or involvement in the running of the business are listed as beneficial owners of legal persons or arrangements;
  - employees of professional intermediary firms acting as nominee directors and shareholders;
  - the resignation and replacement of directors or key shareholders shortly after incorporation;
  - the location of the business changes frequently without an apparent business justification;
  - officials or board members change frequently without an appropriate rationale.

- Complex corporate structures that do not appear to legitimately require that level of complexity or which do not make commercial sense.
- Simple banking relationships are established using professional intermediaries.

Indicators of shell companies

- Nominee owners and directors:
    - formal nominees (formal nominees may be "mass" nominees who are nominated agents for a large number of shell companies);
    - informal nominees, such as children, spouses, relatives or associates who do not appear to be involved in the running of the corporate enterprise.
- Address of mass registration (usually the address of a TCSP that manages a number of shell companies on behalf of its customers).
- Only a post-box address (often used in the absence of professional TCSP services and in conjunction with informal nominees).
- No real business activities undertaken.
- Exclusively facilitates transit transactions and does not appear to generate wealth or income (transactions appear to flow through the company in a short period of time with little other perceived purpose).
- No employees (or only a single employee). Pays no taxes, superannuation, retirement fund contributions or social benefits.
- Does not have a physical presence.

Indicators about the transaction

- The customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers.
- The connections between the parties are questionable, or generate doubts that cannot be sufficiently explained by the client.
- Finance is provided by a lender, whether a natural or a legal person, other than a known credit institution, with no logical explanation or commercial justification.
- Loans are received from private third parties without any supporting loan agreements, collateral, or regular interest repayments.
- The transaction:
    - is occurring between two or more parties that are connected without an apparent business or trade rationale;
    - is a business transaction that involves family members of one or more of the parties without a legitimate business rationale;
    - is a repeat transaction between parties over a contracted period of time;
    - is a large or repeat transaction, and the executing customer is a signatory to the account, but is not listed as having a controlling interest in the company or assets;
    - is executed from a business account but appears to fund personal purchases, including the purchase of assets or recreational activities that are inconsistent with the company's profile;
    - is executed from a business account and involves a large sum of cash, either as a deposit or withdrawal, which is anomalous, or inconsistent with the company's profile;
    - appears cyclical (outgoing and incoming transactions are similar in size and are sent to, and received from, the same accounts, indicating that outgoing funds are being returned with little loss) (aka "round-robin" transactions);
    - involves the two-way transfer of funds between a client and a professional intermediary for similar sums of money;
    - involves two legal persons with similar or identical directors, shareholders, or beneficial owners;

- involves a professional intermediary without due cause or apparent justification;
- involves complicated transaction routings without sufficient explanation or trade records;
- involves the transfer of real property from a natural to a legal person in an off-market sale;
- involves the use of multiple large cash payments to pay down a loan or mortgage;
- involves a numbered account;
- involves licensing contracts between corporations owned by the same individual;
- involves the purchase of high-value goods in cash;
- involves the transfer of (bearer) shares in an off-market sale;
- a loan or mortgage is paid off ahead of schedule, incurring a loss;
- includes contractual agreements with terms that do not make business sense for the parties involved;
- includes contractual agreements with unusual clauses allowing for parties to be shielded from liability but make the majority of profits at the beginning of the deal;
- is transacted via a digital wallet.

- The funds involved in the transaction:

  - are unusual in the context of the client or customer's profile;
  - are anomalous in comparison to previous transactions;
  - are sent to, or received from, a foreign country when there is no apparent connection between the country and the client; and/or are sent to, or received from, a low-tax jurisdiction or international trade or finance centre;
  - are sent to, or received from, a jurisdiction that is considered to pose a high money laundering or terrorism financing risk.

- Unexplained use of powers of attorney or other delegation processes (for example, the use of representative offices).
- Unexplained use of express trusts, and/or incongruous or unexplained relationships between beneficiaries and the settlor.
- Unexplained or incongruous classes of beneficiaries in a trust.

Annex 2. Synopsis of the Guidance

introduction	Purpose	The purpose of this guidance is to assist Licensed Financial Institutions (LFIs) understand and mitigate the risks when providing services to legal persons and arrangements, and to guide them in fulfilling their AML/CFT obligations.
	Applicability	This guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories: ▪ national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and ▪ insurance companies, agencies, and brokers.
Understanding and Assessing the Risks of Legal Persons and Arrangements	ML/TF Risks of Legal Persons and Arrangements	Legal persons and arrangements are attractive to illicit actors because they can assist criminals and their associates to: ▪ Hide the identify of the individuals directing a transaction or controlling an account; ▪ Obscure the true nature and purpose of an account or transaction; and ▪ Conceal the source of funds involved in a transaction or account.
	Features and Controls that Mitigate Risks	Certain rules governing the formation and operation of legal persons and arrangements can, if enforced, reduce the risk that they will be

		abused by illicit actors: ▪ Formation processes that deter creation of shell companies; ▪ Collection of beneficial ownership information for all legal persons and arrangements; ▪ Requiring legal persons and arrangements to keep certain records and make regular reports; ▪ Supervision and monitoring by appropriate government authorities.
Legal persons and arrangements in the UAE	Identification of Beneficial Owners	All legal persons and arrangements in the UAE (except those traded on a stock exchange, or owned by a company traded on a stock exchange) are required to identify all individuals who own or control at least 25% of the legal person or arrangements. Legal persons and arrangements must hold this information, and legal persons must also report it to their registrar. They must maintain and update this information when their beneficial owners change.
	Legal Arrangements Under UAE Law	UAE law allows for the creation of two types of legal arrangements: trusts and awqaf. Trustees and waqf supervisors must comply with certain requirements related to identifying the individuals party to the legal arrangement.
	Economic Substance Requirements	All companies operating in certain sectors must prove on an annual basis that they actually conduct substantive activities in the UAE by submitting certain required information to their registrar. Although this information is not directly available to LFIs, they should be aware of these requirements and can request the information from legal person customers.
Mitigating Risk: Requirements for LFIs	Risk-Based Approach	LFIs must take a **risk-based approach** in their AML programs and to individual customers. This means that they should assess all customers, including legal person/legal arrangement customers, to determine their degree of risk. In assessing the risk of a legal person or arrangement customer, LFIs should consider at least the following factors: ▪ The legal form of the customer; ▪ The controls governing the formation of that type of customer; ▪ The controls in place to ensure that the customer identifies and reports its beneficial owners; ▪ Whether the customer is subject to recordkeeping and reporting requirements; ▪ Whether the customer is appropriately supervised for its compliance with these requirements.
	Customer Due Diligence	For all customers, LFIs must perform Customer Due Diligence with the following components:
		Customer Identification: For all legal person and legal arrangement customers, LFIs must collect the following information ▪ The name [this may not apply for legal arrangements], Legal Form and Memorandum of Association; ▪ Headquarters' office address or the principal place of business; in addition, if the legal person or arrangement is a foreign entity, the name and address of its legal representative in the State; ▪ Articles of Association or any similar documents, approved by the relevant authority within the State; ▪ Names of relevant persons holding senior management positions in the legal person or legal arrangement.

		Identification of Beneficial Owners: For all legal person and legal arrangement customers, LFIs must identify the following individuals: ▪ For legal persons, all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. If no individual can be identified, the LFI must identify the individual(s) holding the senior management position(s) within the legal person customer. ▪ For legal arrangements, the individuals acting as the settlor and the trustee (or anyone holding equivalent positions for non-trust legal arrangements), the beneficiaries or class of beneficiaries, and any other individuals in control of the legal arrangement.
		Understand the Purpose of the Account and the Nature of the Customer's Business: LFIs must understand the business in which their customer engages as well as the reason for creating the account. The answers to these questions can have a significant impact on the risk the customer poses for the financial institution and therefore should be reflected in the customer risk rating.
		Perform Ongoing Monitoring: For all customers, LFIs must ensure that the customer information on file is up to date and accurate, and that the customer's activities are in line with the expectations set at onboarding. If not, the customer risk rating may need to be changed.
	Suspicious Transaction Reporting	For customers of all types, LFIs must report any behavior that they reasonably suspect may be linked to money laundering, the financing of terrorism, or a criminal offence. Please consult the CBUAE's Guidance on Suspicious Transaction Reporting for further information.
	Implementation of TFS	A legal person or arrangement that is not itself designated on a sanctions list may be owned by someone who is designated. LFIs should screen the beneficial owners of all legal person and legal arrangement customers against sanctions lists, and should freeze any accounts or transactions related to a legal person or legal arrangement that is more than 50% owned or controlled by a designated person.

Guidance for Licensed Financial Institutions Providing Services to the Real Estate and the Precious Metals and Stones Sectors

Effective from 16/6/2021 **Status:** In-Force

Introduction

1.1 Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions...with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and

regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.1 As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at centralbank.ae/en/cbuae-amlcft.

1.2 Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and
- Insurance companies, agencies, and brokers.

1.3 Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").

2. Understanding Risks

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the two sectors of real estate and precious metals and stones are weighted as highly important in terms of risk and materiality in the UAE. While the nature and extent of the risk posed by the two sectors to the LFIs providing them with accounts and other financial services is different, they do share common characteristics that LFIs should recognize and take into account:

- **Attractiveness to illicit finance.** The real estate and precious metals and stones sectors are important parts of the UAE's economy, and each provides important, legitimate goods and services to the UAE population

and global trading partners. Nevertheless, experience shows that these sectors offer services that are particularly attractive to illicit actors.

- **Facilitation of the international movement of value.** Despite their different natures, both sectors allow individuals to move large values across international borders, sometimes with only minimal involvement from the formal financial system. For example, a courier carrying a valuable diamond can move millions of AED of value simply by taking a short international flight. In addition, the real estate and precious metals and stones sectors allow individuals to hold value in a form that retains value over time (such as gold or real property) without having to maintain an account in the formal financial system. These facilities are useful to many legitimate businesses, but are also highly sought-after by illicit actors.

- **Varying regulatory regimes.** The extent and nature of regulation on these sectors varies widely between jurisdictions. In some jurisdictions, participants such as dealers in precious metals and stones (DPMS) and real estate agents and brokers are required to be licensed or registered, and to comply with AML/CFT requirements that are similar to those imposed on LFIs. These include, at a minimum, the requirement to perform CDD on customers and to report suspicious transactions. Despite the existence of these requirements, however, sector participants are in many cases not closely supervised or monitored for compliance. Their understanding of their risk and of their compliance obligations may not be well-developed or accurate. In other jurisdictions, there are limited or no obligations placed on these actors, and they may not have any understanding of how they can be abused by illicit actors, or the steps they should take to protect themselves.

2.1 Understanding and Assessing Risks Related to DPMS

Dealers in precious metals and stones (DPMS) play a significant role in the economy of the UAE. DPMS engage in a wide range of activities related to precious metals and stones, from production to trading, establishing the UAE as an important regional hub for this sector. The Dubai Multi Commodities Centre specializes in providing services to precious metal dealers and exchanges, and a significant volume of transactions also goes through the Jebel Ali Free Zone. A significant amount of activity also occurs in the Dubai Gold Souk.

Nonetheless, the precious metals and stones sector offers opportunities for criminals seeking to conceal, transfer, and/or invest their illicit proceeds. Like cash, precious metals and stones offer high value by weight, are difficult to trace and identify, and retain their value over time. DPMS, if they do not apply effective preventive measures, could be vulnerable to abuse by illicit actors engaged in laundering the proceeds of crime, financing of terrorism, arms trafficking, sanctions evasion, and other illicit activities.

2.1.1 Risks of Precious Metals and Stones

The characteristics of precious metals and stones make them uniquely appropriate as media to store, transfer, and exchange value:

i. Precious metals and stones are generally compact, durable, odourless, and of high value.

ii. Certain metals and stones (e.g., gold or diamond) are widely accepted as a method of exchange or currency.

iii. Precious metals and stones retain their value over time, and have roughly the same value all over the world.

In addition to these properties, precious metals and stones have characteristics that make them particularly attractive to criminals seeking to launder funds and others engaged in illicit behaviour:

i. Differentiating precious metals and stones often requires laboratory techniques, so it can be difficult or impossible to track their movement;

ii. Precious metals and stones can be transformed (through re-cutting or recycling) into different objects while retaining their value, interrupting known custody and transfer chains;

iii. Purchase, sale, and exchange of precious metals and stones often takes place outside the formal financial system.

For these reasons, DPMS may be targeted by illicit actors seeking to abuse their services and exploit the advantages of precious metals and stones. Although the majority of transactions involving DPMS are legal, these businesses may trade in items that could be the proceeds of crime, purchased with the proceeds of crime, and/or used to launder the proceeds of crime, unknowingly or complicitly.

Because they are themselves at high risk of abuse, DPMS pose a risk to LFIs. Complicit DPMS may knowingly partake in illicit activities and may in turn use their business relationships with LFIs to launder the proceeds of crime or carry out other illicit activity. Even DPMS that are not knowingly involved in illicit activities may use their accounts with an LFI to deal in the proceeds of crime. For example, a DPMS may wire payment for illegally mined gold to the entity responsible for mining and processing the gold.

Gold as a High-Risk Medium of Exchange

Gold is easy to exchange and transfer, and may provide anonymity when processing transactions, as it is difficult to trace. It also has a universal price standard, a relatively stable market for investment, and may be used as a currency. Gold dealers may provide specific services to their clients, such as metal accounts, for storage or for investment properties. This may enable criminals to move gold under the guise of legitimate business.

2.1.2 Features of DPMS that Increase Risk

Not all DPMS pose equal risk. A DPMS is likely to be considered higher risk when it provides products or services that are attractive to illicit actors, has operations in high-risk jurisdictions, or does not apply appropriate anti-money laundering/combatting the financing of terrorism (AML/CFT) controls.

2.1.2.1 Regulatory Environment

In many jurisdictions, DPMS are not required to comply with requirements related to identification of customers and reporting suspicious activities. In other jurisdictions, these requirements are nominally in place, but DPMS are not subject to effective supervision and enforcement. Even in a jurisdiction that imposes and enforces such requirements, they frequently apply only to DPMS that engage in cash transactions above a certain value threshold. Where DPMS are unregulated or under-regulated, they are unlikely to be taking effective measures to protect themselves from abuse.

In contrast, an effective AML/CFT framework and supervisory regime for DPMS can protect DPMS and LFIs that serve them by effectively imposing AML/CFT requirements and by detecting, deterring, and prosecuting ML/TF crimes. It is important to note that, like LFIs, certain DPMS in the UAE are required to comply with all requirements of AML-CFT Decision, including the requirement to perform Customer Due Diligence (CDD) and report suspicious transactions (see section 2.1.4).

2.1.2.2 Products, Services, and Delivery Channels

Products, services, and delivery channels that facilitate the rapid, efficient, anonymous movement of value on a large scale will be more attractive to illicit actors and may put a DPMS at a higher risk of abuse. Such products, services, and delivery channels may include:

- Products (such as bullion and uncut stones) that are particularly hard to trace, retain or even increase in value despite being transformed into new forms (melted down, re-cut, etc.), and offer high value by weight.
- Services, such as metal accounts, that allow customers to rapidly purchase and sell precious metals or stones.
- Delivery channels that allow transactions to be carried out quickly and anonymously, such as accepting cash or virtual assets and conducting transactions online or through intermediaries.

2.1.2.3 Customer Base

The types of customers that a DPMS serves can also impact risk. For example, a DPMS that primarily deals with PEPs may be higher risk than one that serves a lower-profile clientele.

2.1.2.4 Geography

DPMS may be based, or may trade internationally, in jurisdictions that are higher risk for money laundering, the financing of terrorism, and the financing of proliferation. Such DPMS may pose heightened risk to LFIs. Higher-risk jurisdictions may be characterized by:

- A low level of government oversight and regulation of the precious metal and stone value chain;
- Low economic and political stability;
- High use of the informal banking system;
- High levels of corruption;
- The presence of terrorist and other non-state armed groups;
- Weak border control measures; and/or
- Sanctions and embargoes

Where a DPMS is based in a high-risk jurisdiction, LFIs are required by AML-CFT Decision to perform Enhanced Due Diligence.

2.1.3 Typologies

Precious metals and stones may be involved in a wide variety of illicit finance schemes. The following are some of the most common.

- **Illegal mining or mining supported by the proceeds of crime.** In jurisdictions where precious metals or stones are mined, illicit actors may operate small-scale 'artisanal' mines without receiving a license or paying taxes to the state. The products of these mines are then exported to a refining or cutting hub for processing into saleable goods, like gold bullion and cut stones.

  In many cases, criminal organizations control a mine or a network of small-scale miners. They may invest the proceeds of other illegal activities, such as drug trafficking, into the illegal mines and take the majority share of the resulting production as a return on investment. When the resulting precious metals or stones are processed, the criminal organization can sell them on world markets. The proceeds fund further illicit activities and may also support terrorism.

Example: Trading in gold to legitimise the proceeds of drug trafficking

A criminal organisation in Country X was buying gold from various precious metals retailers using illicit proceeds from narcotics sales. The gold was then sold to a precious metals broker who then sold it to other businesses. The proceeds of the sale were then wired to a third party outside of Country X with links to the drug trafficking organization, thus completing the money laundering cycle.

- **Use of precious metals and stones in sanctions evasion.** The tradable nature, liquidity, wide availability, and anonymity of precious metals and stones has made them popular with individuals, organizations, and governments seeking to evade sanctions imposed by the United Nations or other jurisdictions. This activity may involve mining precious metals or stones under the control of the sanctioned person; the resulting products are then injected into legal trade using front companies and complicit DPMS, earning money for the sanctioned group. Or sanctioned actors may use precious metals and stones to disrupt a transaction chain involving the formal financial system and thus hide their interest in a transaction.

Example: Large-scale sanctions evasion using precious metals

According to Country A's federal indictments, a government sanctioned by Country A used front companies and complicit financial institutions to buy large quantities of gold in Country B. The gold was supposedly exported to the purchasing country, but was in fact moved by courier to the UAE, where it was sold in exchange for cash (U.S. dollars and euros). The cash was deposited with LFIs in the UAE under the names of front companies, and was made available to the sanctioned government to use in proliferation activities.

- **Evasion of duties on precious metals and stones.** Precious metals and stones are often the subject of heavy customs duties and other taxes. As a result, illicit actors will frequently seek to smuggle these goods from high-tax to low-tax jurisdictions, or may declare artificially low values for the goods by misrepresenting their quality or purity.

- **Trade-based money laundering (TBML).** The value of precious metals and stones varies highly based on their quality and purity, features which may not be apparent to the naked eye. In addition, the value of certain precious stones, particularly diamonds, can differ for different non-industry customers based on their personal preferences. This makes precious metals and stones particularly vulnerable to TBML, in which illicit actors use supposedly or actually licit trade to hide illicit finance. This can take a variety of forms:

    - Trading the same goods—often precious stones—repeatedly between co-conspirators to justify funds transfers between members of a criminal network, or between companies owned by the same individual(s). In these schemes, a single precious stone may be repeatedly sold between members of the network, or a single stone may be sold to multiple “purchasers” at the same time, each time with a different description.

    - Inflation or deflation of the value of traded stones to provide justification for cross-border transfers. A merchant may sell low-value precious metals or stones to a purchaser, but invoice for higher-quality goods and thus a higher sum. The purchaser pays the full invoice price, justifying the transaction to financial institutions, and also receives illicit goods such as drugs or smuggled items.

- **Use of precious metals and stones as security for fraudulent loans.** In a typology that is often related to TBML, precious metals or stones may be repeatedly sold or falsely valued between members of a network in order to justify loans and other forms of financing.

Example: Over-Valuation to Justify Illicit Transfers

Mr. A, a licensed DPMS, entered Country X numerous times, each time declaring that he was carrying valuable precious stones. He was in fact carrying gems that were lower value than the ones he declared. He then substituted the lower value gems for higher value gems that were already in Country X and presented them for inspection and clearance at an official diamond exchange. Through these methods, Mr. A obtained validated official importation statements for multiple importations of high-value stones which did not actually take place. He used these statements, together with fake invoices, to facilitate international foreign currency transfers to entities abroad in the guise of payment for the imported goods. He ordered these transactions both for himself and on behalf of other DPMS wanting to receive funds abroad without having to face scrutiny by financial institutions and public authorities.

2.1.4 Regulation and Supervision of DPMS in the UAE

DPMS that qualify as Designated Nonfinancial Businesses and Professions (DNFBPs) are subject to AML/CFT requirements that are substantially the same as those imposed on LFIs, including the requirement to identify customers, to report suspicious transactions, and to perform a risk assessment. Under Article 3 of AML-CFT Decision, DPMS qualify as DNFBPs only if they are *"carrying out any single monetary transaction or several transactions that appear to be interrelated or equal to more than AED 55,000".* A DPMS that does not engage in such transactions is not required to take any preventive measures. Although cash transactions are certainly high risk, LFIs should be aware that the fact that a DPMS does not qualify as a DNFBP does not mean that it is low-risk. All DPMS, regardless of whether they qualify as DNFBPs, must have a commercial license to operate legally in the UAE. The Ministry of Economy is also responsible for identifying and classifying DPMS as DNFBPs; LFIs are not required to make this determination. But LFIs should discover, through the CDD process, whether their customer has been classified as a DNFBP by the Ministry of Economy.

Obliged DPMS are supervised for compliance by the Ministry of Economy, which has issued guidelines for supervised entities describing their AML/CFT compliance obligations.[2]

[2] Available at economy.gov.ae/english/Pages/AML.aspx.

2.2 Understanding and Assessing Risks Related to the Real Estate Sector

The real estate sector is an important part of the UAE's economy, responsible for as much as 20 percent of Gross Domestic Product (GDP). The UAE real estate sector is diverse, encompassing construction and development, commercial real estate sales, and a wide variety of residential real estate, from apartments to luxury villas. A large number of professional real estate agents and brokers—over 11,500—support this sector.

Most transactions within the sector are legitimate. Nevertheless, LFIs should be aware that the real estate sector offers opportunities for criminals seeking to conceal, transfer, and/or invest their illicit proceeds. The real estate market is a fairly liquid market in which assets generally retain stable values over time. Real estate transactions are generally large and offer criminals the opportunity to launder large values in a single transaction. And unlike other stores of value, such as cash or precious metals and stones, real estate can be enjoyed or can earn income while it is in the owner's possession.

2.2.1 Risks of the Real Estate Sector

The real estate sector is attractive to criminals and other illicit actors for many of the same reasons that it is popular with legitimate investors: real estate is a fairly liquid market, with assets that generally maintain or appreciate in value over time. Like certain forms of gold and precious metals, and unlike stores of value such as currency and stocks, real estate can be enjoyed by the owner. Indeed, the purchase of luxury real estate may in fact be the ultimate goal of the money laundering process.

In addition, certain characteristics of the sector, while not in themselves illicit or undesirable, offer advantages for those seeking to launder funds and to move large values between individuals and across borders in a relatively short time:

- The sale or purchase of real estate is a normal, everyday transaction, and offers a simple, convenient explanation for the source of funds in a large transaction.

- Real estate transactions are typically high-value, allowing illicit actors to launder large sums in a single transaction.

- Real estate transactions of all kinds often take place between shell companies created for the sole purpose of owning real property. This practice makes it difficult to identity the true owner of the property. In addition, the ubiquity of this practice makes it difficult to distinguish licit from illicit transactions.

- The price of real estate is not fixed and is somewhat subjective, allowing illicit actors to inflate or deflate sales or purchase prices to better suit to their schemes.

- Real estate is frequently sold and re-sold in fairly quick succession, making it less suspicious when a criminal engages in similar behaviors in order to layer laundered funds.

- In some jurisdictions, the ownership of real estate gives the owners access to residency rights. Illicit actors may take advantage of these rights to expand their criminal networks to new jurisdictions, to escape criminal investigation in their home countries, and to hold assets offshore without alerting their home authorities.

The real estate sector may be abused at any stage of the laundering process

- **Placement:** A criminal may invest illicit funds into the sector through an initial purchase in cash.
- **Layering:** A criminal may conceal the true origin of illicit funds by selling and purchasing a number of properties, extending the distance between current assets and the original placement of the funds.
- **Integration:** A criminal may sell a property and invest the funds in stocks, using the paperwork from the sale to demonstrate an apparently acceptable source of funds.

2.2.2 Features of the Real Estate Sector that Increase Risk

Certain features of the real estate sector in different jurisdictions can increase the attractiveness of the sector to illicit actors. Although these features are not in themselves negative or undesirable, they have the effect of increasing the ease with which illicit actors can use the sector to launder funds.

- **Varying regulation and supervision of real estate professionals**. Real estate agents and brokers are well placed both to detect and to collude in suspicious transactions. Agents and brokers are able to observe suspicious client behaviour, as well as aspects of a transaction that do not have a reasonable explanation. Conversely, complicit real estate professionals may advise a client on how to avoid scrutiny from LFIs and government authorities. This risk is increased in jurisdictions where agents handle client funds, such as in escrow or trust accounts.

  Because of the special role played by real estate professionals, the FATF Recommendations require that many such professionals be regulated and supervised, with AML/CFT obligations like those imposed on financial institutions. Where these obligations are not imposed and enforced, and where real estate professionals are not monitored for their compliance, the sector may be higher risk.

- **Widespread use of cash**. In certain jurisdictions, real estate transactions are frequently executed entirely or partially in cash. This allows a transaction to take place without involving the formal financial system. In

addition, criminal activities often produce high volumes of cash, and placement of cash derived through illegal activities is often the first step in the money laundering process. Even if a particular transaction is executed through bank cheque or other similar means, if the property was purchased for cash in the recent past it can be difficult or impossible to fully understand the chain of ownership and thus to identify whether a transaction is part of the money laundering process (e.g., the property was purchased in cash by A, sold to B to launder the original purchase funds, and is now being re-sold to A).

- **Lack of transparency on beneficial owners.** As discussed above, illicit actors, like many purchasers of real estate, often engage in transactions using shell companies, and engage intermediaries such as law firms to represent them and obscure their interest in a property transaction. Where a jurisdiction does not collect beneficial ownership information for such companies or for real property in general, and permits foreign companies to own real estate, it increases the likelihood that law enforcement and LFIs will not be able to identify the individuals behind a purchase or sale.

- **Openness to foreign purchasers**. A real estate sector that is entirely open to non-residents and non-citizens is likely to be more liquid than a closed sector. In addition, an open sector is exposed to illicit funds generated all over the world. Jurisdictions that offer residency or citizenship rights to foreign purchasers of domestic real estate may be particularly attractive to foreign illicit actors.

- **High liquidity and rising prices.** Illicit actors, like licit investors, want assurance that they will be able to sell an investment property for an amount that recoups their investment or offers a profit. Although they may be willing to tolerate a modest loss on the investment as the cost of money laundering, they may be more likely than most purchasers to seek to 'flip' properties, buying and selling them in quick succession. A highly liquid market facilitates flipping and increases the likelihood that the sale price will meet or exceed the purchase price. In addition, rising prices and a 'hot' market make it easier to disguise certain typologies, such as making small renovations to a property and then reselling it to an associate for a steeply increased price. The difference between the purchase price and the market value is then secretly refunded to the buyer in cash.

2.2.3 Typologies

Illicit actors may use a wide variety of strategies to launder the proceeds of crime through the real estate sector. Many of these strategies are not specific to the real estate sector and appear in a variety of contexts.

The following are some of the most common.

- **Placement of cash.** There are a variety of ways that the real estate sector can be used to place the cash proceeds of crime.

    - Perhaps the simplest is purchasing a property in cash and then selling it, with the purchase price paid via wire or bank cheque. The criminal can identify a clear source of funds for the funds received, and can proceed to layer them using other techniques.

    - This basic typology is subject to a number of variations. A property owner may pay for renovations in cash that represents the proceeds of crime, thus increasing the property's value. When the property is sold, the purchase price will include the value of illicit funds spent on renovations.

    - An illicit actor may receive a bank loan to purchase the property, and then pay the loan back early in cash, or make payments in cash.

    - Real estate investments, such as rental properties, may also be cash-intensive businesses. In jurisdictions where it is common to pay rent in cash, these properties can be used to commingle licit

with illicit funds.

- **Use of shell companies or other legal entities to obscure ownership**. As discussed above, the use of shell companies—legal persons with no operations or employees—to hold real property is a common feature of real estate sectors all over the world. This practice facilitates investment and business (e.g. owning a shopping mall and collecting rent from tenants) and also preserves privacy (e.g. a prominent individual purchasing a home using a shell company to avoid her address becoming public knowledge).

  Despite the legitimate uses of this technique, however, it can also be used to hide ownership when the true owner is an individual who does not want to be linked to the purchase. This may include Politically Exposed Persons (PEPs) who are purchasing properties that are inconsistent with their known sources of wealth; individuals who have past convictions for proceeds-generating offenses or are associated with negative news; and sanctioned individuals.

  In place of or in addition to shell companies, illicit actors may use complex ownership structures, legal arrangements, and nominee arrangements to conceal their ownership interest in a real estate transaction. Please see the CBUAE's *Guidance for Licensed Financial Institutions providing services to Legal Persons and Arrangements*[3] for more information on the risks of legal persons and arrangements.

- **Use of intermediaries to obscure ownership.** Similarly, individuals who wish to hide their connection to a real estate purchase or sale may rely on professional intermediaries—such as real estate brokers, lawyers, and accountants—to engage directly with financial institutions. Such intermediaries may be directly complicit in the concealment and aware that the true identity of their customer would raise questions about the transaction. Or they may simply be following professional rules that mandate professional secrecy regarding their clients.

- **Manipulation of property values.** Although real estate pricing is somewhat predictable, prices are sufficiently subjective to justify inflated or deflated pricing in service of laundering schemes.

  - Two co-conspirators may arrange a sale of a property for a sum that does not represent its market value, with the difference being paid in cash: for example, the sale price is 20% higher than the market value, and the seller repays the buyer in cash. A purchase price higher than market value may be justified to authorities on the grounds that the property was perfect for the buyer's needs, or the buyer was anxious to complete the sale quickly. Similarly, a purchase price below market value may be justified on the grounds that the seller wanted a quick sale, or the property had structural issues.

  - Illicit actors may conspire with corrupt officials or bank employees to inflate the assessed value of a property, facilitating these schemes.

  - A criminal may also disguise illicit transfers as loans raised using the property as security. The higher the value of the property, the more money that can be laundered using this technique.

- **Sequential selling.** The repeated selling of real estate by a group of conspirators, or by a single individual using multiple shell companies, in an attempt to separate the ultimate owner from the criminal proceeds originally used to purchase the property. In many cases, the same individual(s) will buy the property or sell the property multiple times.

---

[3] Available at centralbank.ae/en/cbuae-amlcft.

2.2.4 Regulation and Supervision of the Real Estate Sector in the UAE

2.2.4.1 Regulation of the Real Estate Sector

Regulation of the real estate sector as a whole—as opposed to regulation of real estate professionals—is the responsibility of each of the emirates and as a result varies across the UAE. This section discusses key aspects of regulation of the sector in Dubai and Abu Dhabi, the two largest property markets. Section 2.2.4.2 discusses regulation of real estate agents and brokers.

2.2.4.1.1 Openness to Foreign Purchasers

- **Dubai:** With the exception of nationals of the Gulf Cooperation Council (GCC), non-residents and non-citizens of the UAE are permitted to own real estate in Dubai only in one of the designated real estate investment areas. In general, foreign purchasers must be individuals; legal persons are not able to purchase real estate in the investment areas unless they make the purchase through a subsidiary incorporated in a Free Zone. Foreign trusts and other legal arrangements, including trusts or legal arrangements established in the Free Zones, are also not permitted to purchase real estate anywhere in the Emirate.

- **Abu Dhabi:** As in Dubai, foreigners are permitted to purchase real estate in Abu Dhabi only in one of nine designated real estate investment areas. Within these areas, there are no restrictions on the type of property they can own or the period of time for which they can own it. Outside of these areas, foreigners cannot exercise freehold ownership of property, although they can exercise other forms of long-term ownership, such as leaseholds and usufruct rights.

2.2.4.1.2 Residency Rights

Owners of freehold properties above a certain value may obtain an investor visa that grants them limited residency rights in the UAE. The larger the value of the property, the longer the length of the visa. Visa rules are set by the UAE federal government through Cabinet Resolution (56) of 2018 on Regulating the Residence Permits for Investors, Entrepreneurs and Specialised Talents, and thus apply to all emirates:

- Ownership of a property worth at least AED 1 million comes with a six-month multi-entry visa. Dubai will grant a three-year renewable residency visa in such circumstances.

- An individual who purchases a property of at least AED 5 million and retains it for three years is entitled to a five year residency visa.

- An individual who purchases a property of at least AED 10 million without a mortgage or other loan and retains it for three years is entitled to a ten year residency visa.

2.2.4.1.3 Use of cash

There are no legal restrictions on use of cash to purchase real estate or property in Dubai or Abu Dhabi.

2.2.4.2 Regulation and Supervision of Real Estate Professionals

Real estate agents and brokers in the UAE are required to be licensed. The Land Departments or municipality of each emirate and CFZ are responsible for granting licenses in the Mainland and CFZs; the Financial Services Regulatory

Authority (FSRA) and Dubai Financial Services Authority (DFSA) license real estate agents in the FFZs.

Under Article 3 of AML-CFT Decision, real estate agents and brokers qualify as DNFBPs when they *"conclude operations for the benefit of their Customers with respect to the purchase and sale of real estate."* When they qualify as DNFBPs, real estate agents and brokers must comply with the same AML/CFT preventive measures as LFIs, including the requirements to conduct a risk assessment, perform CDD, and report suspicious transactions.

The Ministry of Economy supervises real estate professionals in the mainland and CFZs for compliance with AML/CFT obligations, and the FSRA and DFSA supervises them in the FFZs. The Ministry of Economy has issued guidelines for supervised entities describing their AML/CFT compliance obligations.[4]

---

[4] These guidelines may be found at economy.gov.ae/english/Pages/AML.aspx.

3 Mitigating Risks

Although LFIs should judge their own risk tolerance and risk management capabilities, **the CBUAE does not expect or encourage LFIs to broadly prohibit or exit customer relationships with the real estate and precious metals and stones sectors.** These sectors are important parts of the UAE economy, and they need access to financial services to conduct their legitimate business. **The CBUAE does expect, however, that LFIs understand their risk and take effective, risk-based steps to protect themselves from abuse and from illicit actors and transactions.** Effective risk mitigation is therefore critical to protecting the LFI, complying with its legal obligations, and meeting supervisory expectations.

The sections below discuss how LFIs can apply specific preventive measures to identify, manage, and mitigate the risks associated with the real estate and precious metals and stones sectors. It is not a comprehensive discussion of all AML/CFT requirements imposed on LFIs. LFIs should consult the UAE legal and regulatory framework currently in force. The controls discussed below should be integrated into the LFI's larger AML/CFT compliance program, and supported with appropriate governance and training.

3.1 Risk-Based Approach

3.1.1 Overarching common requirements

LFIs must take a risk-based approach to the preventive measures they put in place for all customers, including customers in the real estate and precious metals and stones sectors. A risk-based approach means that LFIs should dedicate compliance resources and effort to customers, business lines, branches, and products and services in keeping with the risk presented by those customers, business lines, branches, and products and services, as assessed in accordance with Article 4 of AML-CFT Decision.

The risk-based approach has three principal components:

3.1.1.1 Conducting an enterprise risk assessment, as required by Article 4.1 of AML-CFT Decision.

The enterprise risk assessment should reflect the presence of higher-risk customers, including DPMS and real estate sector participants in an LFI's customer base. This assessment should include higher-risk customers from outside the UAE whose risks will also need to be assessed. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the controls risk element of the LFI's enterprise risk assessment, as required by section 4.2.1 of the *Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions*, should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its higher-risk customers, including the preventive measures discussed below.

3.1.1.2 Identifying and assessing the risks associated with specific customers.

The LFI should assess the risk of each customer to identify those that require enhanced due diligence (EDD) and to support its entity risk assessment. In assessing the risks of a DPMS or real estate sector participant, LFIs should consider:

i. **Geographic Risk:** The risks associated with the jurisdictions in which the customer lives (for individuals) or is registered/headquartered (for legal persons) and where it operates, including the jurisdictions where it has subsidiaries, where it sources its products (where relevant), and where its main counterparties are based. These may include the overall risk of money laundering, terrorist financing, and financing of proliferation, as well as what is known regarding the prevalence of abuse of entities in these sectors.

   There are a number of sources that LFIs can use to develop a list of high-risk countries, jurisdictions, or regions. LFIs should consult any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee (NAMLCFTC)[5], UAE FIU and by the FATF, including the FATF's list of jurisdictions subject to countermeasures and to increased monitoring. LFIs may also use public free databases such as, for example, the Basel AML Index[6] or the Transparency International Corruption Perceptions Index.[7] LFIs should not rely solely on public lists, however, and should consider their own experiences and the nature of their exposure to each jurisdiction when assessing the risk of that jurisdiction.

ii. **Customer Risks:** For real estate agents and brokers and DPMS, customer risk can be assessed as the proportion of higher-risk customer types (e.g. PEPs, legal persons, and customers from high- risk jurisdictions) within a customer's customer base.

iii. **Product, Service, and Delivery Channel Risk:** LFIs should assess risk in this category on two dimensions:

   a. The products and services that the customer offers to its customers, and the delivery channels through which it offers these products and services. Products, services, and delivery channels that promote the rapid, anonymous transfer of high values are particularly attractive to illicit actors. These may include, but are not limited to:

      i. Online/non-contact sales: Non-face to face transactions make it easier for criminals to hide their identifies.

      ii. Accepting cash for high-value purchases. Cash is very difficult to trace and can be exchanged without involving the formal banking system, and thus is particularly attractive to criminals.

      iii. Accepting virtual assets: Virtual assets, like cash, are anonymous and difficult to trace to their users. Unlike cash, virtual assets allow parties to carry out transactions even when they are at a distance from one another. These qualities, combined with the lack of consistent regulation of entities that deal in virtual assets, make virtual assets high risk for abuse by illicit actors.

      Specific high-risk products and services offered by each customer type are discussed below in sections 3.1.2 and 3.1.3.

   b. The LFI products and services that the customer intends to use, and the delivery channels through which the LFI will provide these services. LFIs should draw on their entity risk assessment to assess the risk of the products and services each customer uses or intends to use. (This subject is also discussed in section 3.2.1.3.2 below in relation to understanding the nature and purpose of the business

relationship.)

iv. **Controls Risk:** LFIs should seek to understand the regulatory requirements in place for the customer, as well as how well they are enforced. This assessment is particularly important for those DPMS and real estate brokers that qualify as DNFBPs and therefore are also subject to such requirements. Other participants in the real estate sector, such as developers, are not required to comply with AML/CFT preventive measures. In addition, participants in the precious metals and stones sector may also be required to comply with UAE requirements or global standards related to sourcing precious metals and stones and transparency of supply chains. Where relevant to a customer's business, LFIs should consider whether its customer conducts appropriate supply chain due diligence.

Questions that an LFI may ask to determine customer risk profile include, but are not limited to:

- Where is the customer incorporated? Where does it operate? Are these high-risk jurisdictions?
- What products and services does the customer provide?
- What is the trading volume of the business?
- What customer base does the customer serve?
- What is the regulatory environment in the jurisdiction(s) where the customer is incorporated/has operations?
- Is there an authority that actively enforces the requirements?
- Is the customer required to perform CDD on cash customers above a certain threshold in all jurisdictions where it operates? In such scenarios, is it required to identify the beneficial owners of legal person customers?
- Is the customer required (as are DNFBPs in the UAE) to conduct a regular independent audit? Did the most recent audit have any material findings?
- Does the customer perform sanctions screening?
- What is the main channel (in-person vs. online) and methods (cash, wire transfers, checks, etc.) of conducting transactions and in which currency (or multiple currencies)?

In addition to risk rating customers, LFIs should also consider the risks of specific transactions, especially high-value transactions, those involving high-risk jurisdictions, and those that represent departures from a customer's standard or expected behavior. LFIs should be aware of sectoral risks when reviewing large transactions associated with the DPMS or real estate sectors, or transactions of any size that do not have a clear licit economic purpose.

---

[5] Available at: namlcftc.gov.ae/en/high-risk-countries.php
[6] Available at: baselgovernance.org/basel-aml-index
[7] Available at: transparency.org/en/cpi/2020/index/nzl

3.1.1.3 Applying EDD and other preventive measures

LFIs must apply EDD and other preventive measures to customers determined to be higher-risk, as required by Article 4.2(b) of AML-CFT Decision, or to specified higher-risk customer types, no matter their risk rating, as required by AML-CFT Decision. EDD measures should be designed to mitigate the specific risks identified with particular customers. Examples of EDD measures are offered below in section 3.2.

3.1.2 Key Considerations for DPMS

Beyond the general considerations discussed above, in assessing the risk of a DPMS customer LFIs should consider:

- **Geographic Risk:** Whether the jurisdiction(s) in which the customer is based or operates are known centres for illegal or unregulated mining of precious metals and stones.

- **Product, Service, and Delivery Channel Risk:** The following products and services are particularly high risk:

- Trade in gold bullion and diamonds: The high inherent value of these substances, their ability to retain value for a long period of time, the size and stability of the market, relative ease of exchange, high value by weight, and the difficulty of tracing them makes gold and diamonds particularly attractive to criminals.

- Metal accounts: Metal accounts are accounts held by a custodian institution and denominated in precious metals (such as gold, silver, or platinum) rather than in fiat currencies. They allow the account holder to quickly buy and sell precious metals without needing to have a face-to-face interaction with a DPMS.

3.1.3 Key Considerations for the Real Estate Sector

Beyond the general considerations discussed above, in assessing the risk of a customer who is a participant in the real estate sector, LFIs should consider:

- **Controls Risk:** In the case of transactions or customers related to the real estate sector, an assessment of controls risk should also include the regulations governing the real estate sector as a whole, and not just regulations governing the sector participants (real estate agents and brokers). LFIs should assess whether regulations governing property transactions are likely to make the sector more or less attractive to illicit actors. As discussed above in section 2.2.2, these may include the openness to foreigners, the widespread use of cash and shell companies, and the intensity of scrutiny of real estate transactions.

In many cases neither party to a real-estate related-transaction will be a business or individual whose primary activity is related to the real estate sector (e.g., the sale of a private home). In such cases, in addition to the risk of the specific customer involved, LFIs should consider aspects of the transaction itself, including:

- The jurisdiction in which the real property that is the subject of the transaction is located;
- The jurisdiction in which the customer's counterparty is located;
- If the LFI's customer is the purchaser, whether the purchase price is consistent with the purchaser's known means and income;
- Whether the purchase price is generally consistent with the market price for roughly similar properties;
- Whether all parties to the transaction are resident in jurisdictions other than the jurisdiction in which the property is located;
- Whether the seller of the property has owned it only for a short period of time;
- Whether shell companies or other legal structures are involved in the purchase in such a way as to obscure the true owner of the property; and
- Whether the parties to the transaction appear to be related (e.g. are represented by the same law firm or real estate broker, share corporate directors, or share an address), but the relationship between them is unclear.

3.2 Customer Due Diligence and Enhanced Due Diligence

CDD, and where necessary EDD, are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers. As discussed below, each stage of the CDD process gives LFIs an opportunity to collect the information they need to identify and manage the specific risks of higher- risk customers.

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFI's services. Where an LFI cannot satisfy itself that it understands a customer, then it should not accept that legal person or legal arrangement as a customer. If there is an existing business relationship, the LFI should not continue it. LFIs should also consider filing a Suspicious Transaction Report (STR), as discussed in section 3.3 below.

Under Article (5) of AML-CFT Decision, LFIs must conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a Customer with whom there is no business relationship. Although Article 5 permits CDD to be delayed in circumstances of lower risk, the higher risk of the DPMS and real estate sectors makes it very unlikely that delayed CDD will be appropriate in the context of onboarding such customers.

LFIs should consult the UAE legal and regulatory framework currently in force for a full discussion of their CDD obligations and of the CBUAE's expectations for CDD procedures.

3.2.1 Overarching common requirements

The following elements of CDD should be carried out for all customers, no matter the customer type.

3.2.1.1 Customer Identification and verification

Under Article 8 of AML-CFT Decision, LFIs are required to **identify and verify the identity of all customers**.

In most countries, including the UAE, anyone operating a business, whether as an individual or a legal person, must have a business license. Such persons may also need to be registered with their country's ministry of commerce or economy. Among other documents required for customer identification and verification, LFIs should ensure that they collect proof of an active license and/or registration from all business customers. Where a license is required, lack of one may indicate that a customer is attempting to avoid regulation and supervision by the authorities in the UAE or in its home jurisdiction.

3.2.1.2 Beneficial Owner Identification

The majority of DPMS and real estate sector customers will be legal persons. The UAE requires all financial institutions to identify the beneficial owners of a legal person customer by **obtaining and verifying the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more.** Where no such individual meets this description, the LFI must identify and verify the identity of the individual(s) holding the senior management position in the entity.

Legal arrangements may be involved in transactions related to real estate. For legal arrangement customers, LFIs must **verify the identity of the settlor, the trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement and obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment, or at the time he/she intends to exercise his/her legally acquired rights.**

The beneficial owner of a legal person or arrangement must be an individual. Another legal person or arrangement cannot be the beneficial owner of a customer, no matter what percentage it owns. LFIs must continue tracing ownership all the way up the ownership chain until they discover all individuals who own or control at least 25% of the LFI's customer.

When the LFI has identified qualifying beneficial owners, it should perform CDD on each individual beneficial owner, in accordance with the requirements of Article 8.1(a) of AML-CFT Decision.

Please see the CBUAE's *Guidance for Licensed Financial Institutions providing services to Legal Persons and Arrangements*[8] for more information on identification of beneficial owners.

[8] Available at centralbank.ae/en/cbuae-amlcft

3.2.1.2.1 EDD: Beneficial Ownership

If the LFI is not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so is to identify additional beneficial owners below the 25% ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10% or even the 5% level. It may also involve requiring the customer to provide the names of all persons who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

3.2.1.3 Nature of the Customer's Business and Nature and Purpose of the Business Relationship

For all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This step requires the LFI to collect information that allows it to create a profile of the customer and of the expected uses to which the customer will put the LFI's services. This element of CDD will have important implications for the customer risk rating. This is particularly true of the nature of the customer's business, which will likely be the critical determinant of risk for customers of the types addressed in this Guidance.

3.2.1.3.1 Nature of the Customer's Business

Understanding the nature of the customer's business involves first i) identifying that the customer is a participant in a higher-risk sector; and ii) collecting all the information necessary to assess the risk factors for that specific customer type, as described in section 3.1 above. Customers may not identify themselves explicitly as DPMS or real estate sector participants. In some cases, the nature of the customer's business will be clear based on the customer's own statements; in others, the LFI may need to ask additional questions to ascertain whether or not the customer carries out any of the qualifying activities. For example, an importer/exporter may qualify as a DPMS if it trades in precious metals and stones among other products, or a department store may qualify if it sells fine jewelry.

Following the determination of the customer's sector, the LFI should collect the information necessary to understand the products and services the customer offers, where it operates, and who its customers are. The exact information collected will depend on both the nature of initial findings and on the risk level of the entity. For example:

- Company A is a large commercial real estate broker licensed in Sharjah and supervised as a DNFBP by the Ministry of Economy. Company A applies for a general purpose business account with Bank C, an LFI. Bank C interviews Company A regarding its business activities and customer base, and asks Company A to supply a copy of its institutional risk assessment and its CDD and STR policies.

- Company B, a small business based in Dubai, seeks to establish a checking account with Bank C, an LFI. Company B represents that it primarily sells furniture and curios, but in response to questions from Bank C during the CDD process discloses that it sells gold and silver coins and also that it accepts cash payments. Company B is not licensed as a DPMS and is not registered by the Ministry of Economy. Bank C decides to make an unannounced site visit to Company Band discovers that gold objects make a up a large part of its inventory. Bank C declines to consider opening the account until Company B is licensed and registered as a DPMS.

3.2.1.3.2 Nature and Purpose of the Business Relationship

The risk to which the LFI may be exposed can vary based on the purpose of the account and the types of financial products and services the customer wishes to use. Nevertheless, if other risk factors are present a customer may still qualify as high risk even if they use only low-risk products and services.

- Certain aspects of a customer's business may be higher risk than others. For example, an account used for payroll may be lower risk than an account used to pay suppliers or that receives payments directly from customers.

- Certain LFI products and services may expose the LFI to higher risk. These include cash management services or large-scale cash deposits, and international wires, especially wires to or from high-risk or secrecy jurisdictions. These services are higher risk because they facilitate rapid movements of value across borders, or (in the case of cash) because they are conducive to anonymity. The LFI's entity risk assessment should identify its higher-risk products and services, and a customer that intends to use such services should be risk-rated accordingly.

For example:

- Company X is a small DPMS operating in the Dubai Gold Souk that applies for a general purpose checking account with Bank C, an LFI. Company X tells Bank C that it sells gold jewelry. It claims that it does not accept cash and has not registered as a DNFBP, but tells Bank C to expect weekly cash deposits. The relationship manager visits the store and observes a sign by the cash register saying "Payment by Cheque or Credit Only." Bank C decides to prohibit cash deposits into the account with prior authorization, and to restrict such deposits to a low monthly total.

3.2.1.3.3 Developing a Customer Profile

Businesses, including those in the DPMS and real estate sectors engage in an extremely wide variety of financial activity, potentially a wider variety than individual customers are likely to display. The activity profile of a cash-intensive business such as a small DPMS is likely to be completely different from that of a large- scale commercial developer. At the same time, specific businesses are also likely to engage in patterns of activity that remain constant from month to month and year to year. Understanding the purpose of the account allows LFIs to develop expected patterns and compare them to actual behaviour.

3.2.1.3.4 EDD: Customer's Business and the Business Relationship

As LFIs advance efforts to understand their customer's business and financial activities, they should consider whether aspects of the customer profile require EDD. The following are some situations in which EDD may be appropriate:

- The customer has business or other ties to high-risk jurisdictions (if the customer or its beneficial owners are based in a high-risk jurisdiction, EDD is mandatory).
- The customer intends to use high-risk financial products and services, such as bulk cash services or purchase and exchange of virtual assets.
- The LFI does not fully understand the customer's business model, or the customer has no clear business activities that would justify its expected to use of the account.

EDD on the business activities and account use of business like DPMS and real estate sector participants can involve the following:

- Requiring the customer to provide invoices documenting incoming and outgoing transfers;
- Inspecting payroll documents and other business records;
- Visiting the customer's business premises and interviewing its personnel;
- Requesting a reference from a current customer or other well-known firm with which the new customer claims to do business, or which operates in the same sector as the new customer.

3.2.1.4 Ongoing Monitoring

All customers must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

3.2.1.4.1 CDD Updating

LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. This is particularly crucial in the context of customers that are companies, which, by their very nature, can change their fundamental identity overnight. With the stroke of a pen, a company engaged in a low-risk business and owned by reputable UAE residents can move its activities to a high-risk sector and can transfer ownership to nationals of a high-risk foreign jurisdiction. For example:

- Mr. Y and Sons is a highly-reputable dealer in uncut diamonds that has been banking with Bank C for more than 40 years. Bank C's account manager reads in the newspaper that Mr. Y has recently passed away and calls on Mr. Y's sons to express his condolences. During the course of the conversation, the account manager asks which son will be in charge of the business going forward. They inform him that they have just sold the business to a consortium of investors who wished to remain anonymous but who were represented by a global law firm with offices in the Free Zone. Once it has become aware of this fact, Bank C should rapidly identify the new beneficial owners of the customer. If it cannot do so promptly, it should suspend activity on the account.

LFIs should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular should ascertain that:

- The customer's beneficial owners remain the same;
- The customer continues to have an active status with a company registrar;
- The customer has the same legal form and is domiciled in the same jurisdiction;
- The customer is engaged in the same type of business, and in the same geographies;

In addition to a review of the customer's CDD file, the LFI should also review the customer's transactions to determine whether they continue to fit the customer's profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established. This type of transaction review is distinct from the ongoing transaction monitoring discussed in section 3.2.1.4.2 below. The purpose of the review is to complement transaction monitoring by identifying behaviours, trends, or patterns that are not necessarily subject to transaction monitoring rules. For example:

- Bank C is conducting its scheduled CDD review for Company A, a commercial real estate brokerage firm. When reviewing the customer's transactions over the past year, Bank C notices that Company A has begun making fairly regular payments to a counterparty in Country 1. Previously, Company A had engaged in extremely limited cross-border activity. The payments do not exhibit any red flags and therefore were not flagged by Bank C's automated transaction monitoring system. Bank C contacts Company A and learns that it is has recently entered into a referral agreement with a private bank in Country 1. The bank refers customers looking to invest in the real estate sector, in Country 2, to Company A and in return receives a percentage of any commission Company A makes on a resulting sale. Bank C decides to conduct additional due diligence to learn more about the customer base referred to Company A by the bank in Country 1.

The techniques used for transaction review will vary depending on the client. For lower-risk clients, a review of alerts, if any, is likely to be sufficient. For higher risk clients, a more intensive review may be necessary. For clients with a large volume of transactions, LFIs may use data analysis techniques to identify unusual behaviour.

If the review finds that the customer's behaviour or information has materially changed, the LFI should risk- rate the customer again. New information gained during this process may cause the LFI to believe that EDD is necessary, or may bring the customer into the category of customers for which EDD is mandatory (i.e. customers that are PEPs, or owned or controlled by PEPs, or their family members or associates; and customers that are based in high-risk jurisdictions).

LFIs may consider requiring that the customer update them as to any changes in its beneficial ownership or business activities. Even if this requirement is in place, however, LFIs should not rely on the customer to notify it of a change, but should still update CDD on a schedule appropriate to the customer's risk rating.

3.2.1.4.2 Transaction Monitoring

LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of an STR (see section 3.3 below). As with all customer types, LFIs that use automated monitoring systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. For example, a series of transactions between two unconnected companies may not be cause for an alert. But if the companies are all owned or controlled by the same individual(s), the LFI should investigate to make sure that the transactions have a legitimate economic purpose.

Where possible, monitoring systems should also flag unusual behaviour that may indicate that a customer's business has changed—for example, a first transfer to or from a high-risk jurisdiction, or a large transaction involving a new counterparty. LFIs should follow up on such transactions with the customer to discover whether the customer has changed its business activities in such a way as to require a higher risk rating.

Sample red flags for illicit behaviour involving DPMS and the real estate sector are provided in the Annex to this Guidance.

3.2.1.4.3 EDD: Ongoing Monitoring

When customers are higher risk, monitoring should be more frequent, intensive, and intrusive. LFIs should review the CDD files of higher risk customers on a frequent basis, , such as every six or nine months for very high-risk customers. The methods LFIs use to review the account should also be more intense and should not rely solely on information supplied for the customer. For example, LFIs should consider:

- Manually reviewing all transactions on the account on a quarterly basis, rather than a sample of transactions (as discussed above, such manual review should be in addition to automated transaction monitoring). Manual review can take the form of reviewing individual transactions, or of using data analysis to determine information about the customer's activity (e.g., overall percentage of counterparties in high-risk jurisdictions; new jurisdictions of activity compared to last quarter; overall percentage of transactions that are round numbers, etc.) that would not be apparent to automated transaction monitoring systems;

- Conducting site visits at the customer's premises and requesting a meeting with the customer's managing director or Chief Financial Officer;

- Conducting searches of public databases, including news and government databases, to independently identify material changes in a customer's ownership or business activities or to identify adverse media reports. Searches for adverse media should include relevant key words, including, but not limited to, allegation, fraud, corruption, and laundering.

In addition, higher-risk customers should be subject to more stringent transaction monitoring, such as lower thresholds for alerts and more intensive investigation.

3.2.2 Key Considerations for DPMS

All of the requirements above apply fully to DPMS customers. This section describes specific or additional considerations that LFIs should have in mind when carrying out CDD on such customers.

- **Nature of the Customer's Business:** Understanding the nature of the customer's business is particularly important in the context of DPMS, as risk is largely driven by the nature of the entity's business activities. LFIs should consider factors such as:

    - Whether the customer qualifies as a DNFBP, and, if so, whether it is registered as such with the appropriate authority in its home jurisdiction (in the UAE, this is the Ministry of Economy, see section 2.2.4);

    - The DPMS-specific risks of the countries where the customer does business (see section 3.1.1.2 (i)). Certain countries that may not be considered extremely high risk in other contexts may be very high risk in the DPMS sector, such as countries where illegal mining takes place on a significant scale, or countries were smuggling of gold and precious stones is particularly common;

    - The products and services the customer provides, and their attractiveness to illicit actors.

    - **Example:** Customer, a large Abu Dhabi luxury goods store, seeks to establish a general purpose business account with Bank B, an LFI. Customer sells fine jewelry to a clientele that includes a number of PEPs. Bank B collects additional information about sales and policies from Customer, and determines that all purchases of fine jewelry must be made using a credit card, and that fine jewelry accounts for less than 10% of Customer's annual turnover. Bank B decides that EDD is not necessary at this point, but decides to review activity on the account after six months to determine whether it presents any red flags.

- **Ongoing Monitoring:** Because DPMS risk varies with their business activities, it is particularly important that LFIs monitor DPMS accounts for any unexpected changes in activity. A change in activity is not necessarily a sign of illicit behaviour, but it may indicate that a DPMS has changed its activity profile in ways that affect its risk rating.

    - **Example:** When conducting its scheduled review of activity on the account of Customer, a large Abu Dhabi luxury goods store, Bank B notices that Customer has recently begun to receive large transfers from Iraq. When Bank B contacts Customer, the store explains that they've just begun conducting 'trunk shows' of fashion and fine jewelry for customers in Iraq and as a result have substantially increased the business they do with customers there. Based on this information, Bank B increases Customer's risk rating and considers placing other controls on the relationship.

3.2.3 Key Considerations for the Real Estate Sector

Customers that are overall low-risk, and whose business is unrelated to the real estate sector, can nonetheless engage in high-risk transactions related to the sector. For example, a retired businesswoman who has been a customer of an LFI for twenty years may sell her luxury villa to a foreign PEP. In such cases, the CDD that has been performed on the customer may not be sufficient to manage the risk of this particular transaction, and LFIs may need to perform additional transactional due diligence. Transactional due diligence may also be necessary to comply with the requirements of Article 7.1 of AML-CFT Decision, which requires LFIs to audit transactions carried out throughout the business relationship to ensure that the transactions are consistent with the customer's risk profile.

Transactional due diligence should at least involve collecting additional information about the underlying activity and the customer's counterparty. Information that an LFI may request in the context of transactional due diligence on real

estate transactions includes:

- Sufficient information about the property to support an assessment that the purchase/sale price is reasonable and generally consistent with values for similar properties. This may include its official valuation for property tax purposes (where one exists); cadastral maps for the area where the property is located; floor plans; photographs; and recent sales information for similar properties. Where the LFI is financing a purchase, or has previously financed the purchase of the same property, it likely has this information on hand already.

- Information about the customer's counterparty. Where the counterparty is an individual, this should include sufficient information to perform adverse media, sanctions and PEP screening. Adverse media searches should include searches of public records and databases using relevant key words, including but not limited to, allegation, fraud, corruption, laundering.

- Where the counterparty is a legal person, it should include the jurisdiction in which the counterparty is registered/headquartered; identifying information on the counterparty's beneficial owners and line of business.

- Information on source of funds and source of wealth. LFIs should be able to identify the source of funds for every large transaction related to the real estate sector. Where a transaction is financed, the source of funds will often be a bank loan, but for unfinanced transactions the determination may be more difficult. For high-risk customers or counterparties, such as PEPs, LFIs should also understand the source of overall wealth, in addition to the source of the specific funds used to purchase the property.

3.3 STR Reporting

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file a STR with the UAE Financial Intelligence Unit (UAE FIU) when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, the proceeds of crime, is related to a crime, or is intended to be used in a crime. **STR filing is a legal obligation and a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system.** By filing STRs with the UAE FIU, LFIs help to alert law enforcement about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations:

- A potential customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current customer cannot provide required information about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty; or
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the LFI should not establish the business relationship, or continue an existing business relationship.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[9] for further information.

[9] Available at centralbank.ae/en/cbuae-amlcft

3.4 Governance and Training

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. **The core of an effective risk-based program is an appropriately experienced AML/CFT compliance officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective.**

As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of DPMS and real estate sector customers, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For example, an LFI that has a large number of DPMS customers should offer training that includes an in-depth discussion of risk factors and red flags related to such customers.

Annex 1. Red Flags

Red Flags for DPMS

Trade practices

- Precious metals and stones originate from a country where there is limited production or no mines at all.
- Trade in large volumes conducted with countries which are not part of a specific precious metals and stones pipeline.
- An increase of the volume of the activity in a DPMS account despite a significant decrease in the industry-wide volume.
- Selling or buying precious metals and stones between two local companies through an intermediary located abroad (lack of business justification. uncertainty as to actual passage of goods between the companies).
- Volume of purchases and/or imports that grossly exceed the expected sales amount.
- Sale of gold bars, coins, and loose diamonds from a jewelry store (retail).
- Payments related to the appearance of rare or unique precious stones in the international market outside of known trading procedures (e.g., Argyle's rare pink diamond appearing in the international marketplace outside of the annual tender process). This to the best knowledge of the financial institution.
- A single bank account is used by multiple businesses.

Transactions/financing of precious metals and stones trade

- Unusual forms of payment in the trade, for example, use of travelers cheques (all stages according to the accepted forms of payments).
- Date of payment not customary in the trade, (e.g. receiving/sending funds for a precious metal and stone deal conducted a very long time ago (outside accepted payment terms). Or, a customer paying upfront where the customary payment date is within a 120 days term.
- Financial activity is inconsistent with practices in the precious metal and stone trade. For example,

- Foreign currency deposits followed by currency conversion and cash withdrawal in local currency.
- Cheque deposits followed by immediate cash withdrawals in slightly lower amounts (possible use of the DPMS account for cheques discounting).
- Transfers of foreign currency and/or foreign currency cheques deposits, followed by currency conversion and immediate withdrawal from the account (possible use of the DPMS account for exchange services)

- No economic rationale for transactions involving an individual or company in the precious metal and stone industry.
- Deposits immediately followed by withdrawals, atypical of practices in the precious metal and stone trade, including but not limited to:|
  - Circular transaction related to import/export of precious metals and stones.
  - Circular transactions related to local trade (between local bank accounts).
  - Circular financial transactions between a precious metal and stone company's account and the private account of the company's shareholder/director, without business or economic reason.
  - High turnover of funds through an account with a low end of day balance.
- Deposits or transfers to a precious metal and stone dealer's account from foreign companies followed by immediate transfer of similar amounts to another jurisdiction.
- Immediately after a precious metal and stone dealer's related account is opened, high-volume and high-value account activity is observed.
- Transactions between accounts of different companies which are affiliated with the same customer, particularly to or from Free Trade Zones or countries with tax leniencies 119 (may be an indication of transfer pricing or trade mispricing).
- Open export is settled by offsetting to, and receiving payment from, a third party.
- Open export is settled abroad by offset in front of the importer.
- Settling an open export invoice with unrelated companies that engage in a specific precious metal and stone and not through value/return from abroad or return of goods to the precious metal and stone merchant.
- Details of the transaction are different from the details of the commercial invoice presented by the DPMS to the bank (name of importer/exporter, sum, place etc.)
- High-value funds deposited or transferred to an account described as short-term loans with no transactions showing repayment of loans.
- Early repayment of DPMS loan (a loan for 25 years is repaid after five month) with no reasonable explanation.
- Sale of diamonds and jewelry at small incremental amounts (retail).

- Multiple cheques drawn on the same DPMS' account on the same day.
- Origin/destination of funds is different from the destination/origin of the specific precious metal and/or stone.
- DPMS is credited by transactions with no evidence of sales.
- Numerous returns of advanced payments.

Customers

- Activity does not match KYC, for example:
    - Actual trade volumes are significantly larger than the expected volume.
    - Customers and/or suppliers of the customer do not correspond to the stage of the trade initially declared.
- DPMS is not familiar with trade practices.
- DPMS maintains high level of secrecy.
- DPMS conducting activity in a branch not specializing in precious metals and stones (where such branches exist).
- Use of a bank account in the name of a charity to transfer funds to/from DPMS.
- Frequent changes in company name and contact person for a business in the industry (mainly wholesale)

Use of third parties

- Customer consults a third party while conducting transactions.
- Receiving/transferring funds for import/export activity to/from entities that are not known to be involved in the precious metals and stones trade (either an individual or a legal entity).
- Return of an advanced payment from a third party.
- Receiving/transferring funds for import/export where the ordering customer/beneficiary is an MSB.
- Use of third parties to deposit funds into single or multiple DPMS' accounts.
- Return of an advanced payment from a third party.
- Name of sender in the payment transfer to the DPMS is not the importer/buyer (mainly rough and polished trade).
- Name of receiver in the payment from the DPMS is not the exporter/supplier.
- A single bank account with multiple deposit handlers (retail and wholesale).

Use of missing/suspicious/falsified documents

- For diamond dealers, Kimberly Process (KP) certificate is or seems to be forged.
- Long validity of a KP certificate
- Transfers of funds or an attempt to transfer funds through a DPMS company's account without producing appropriate documentation.
- DPMS claims funds received/transferred are an advanced payment without producing any appropriate export/import invoice to support it.
- Transfers between a DPMS and a private account that are reported to the bank as precious metal and/or stone transactions, without presenting appropriate documentation.
- Invoice presented by the DPMS appears to the bank as unreliable/fake.
- Failing to provide a customs declaration in relation to a foreign currency cash deposit resulting from selling precious stones abroad.

Red Flags for the Real Estate Sector

Natural persons

- Transactions involving individuals residing in tax havens or risk territories, when the characteristics of the transactions match any of those included in the list of indicators.
- Transactions carried out on behalf of minors, incapacitated persons or other persons who, although not included in these categories, appear to lack the economic capacity to make such purchases.
- Transactions involving persons who are being tried or have been sentenced for crimes or who are publicly known to be linked to criminal activities involving illegal enrichment, or there are suspicions of involvement in such activities and that these activities may be considered to underlie money laundering
- Transactions involving persons who are in some way associated with the foregoing (for example, through family or business ties, common origins, where they share an address or have the same representatives or attorneys, etc.).
- Transactions involving an individual whose address is unknown or is merely a correspondence address (for example, a PO Box, shared office or shared business address, etc.), or where the details are believed or likely to be false.
- Several transactions involving the same party or those undertaken by groups of persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Individuals who unexpectedly repay problematic loans or mortgages or who repeatedly pay off large loans or mortgages early, particularly if they do so in cash.

Legal persons

- Transactions involving legal persons or legal arrangements domiciled in tax havens or risk territories, when the characteristics of the transaction match any of those included in the list of indicators.
- Transactions involving recently created legal persons, when the amount is large compared to their assets.
- Transactions involving legal persons or legal arrangements, when there does not seem to be any relationship between the transaction and the activity carried out by the buying company, or when the company has no business activity.
- Transactions involving foundations, cultural or leisure associations, or non-profit-making entities in general, when the characteristics of the transaction do not match the goals of the entity.

- Transactions involving legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Transactions involving legal persons whose addresses are unknown or are merely correspondence addresses (for example, a PO Box number, shared office or shared business address, etc.), or where the details are believed false or likely to be false.
- Various transactions involving the same party. Similarly, transactions carried out by groups of legal persons that may be related (for example, through family ties between owners or representatives, business links, sharing the same nationality as the legal person or its owners or representatives, sharing an address, in the case of legal persons or their owners or representatives, having a common owner, representative or attorney, entities with similar names, etc.).
- Formation of a legal person or increases to its capital in the form of non-monetary contributions of real estate, the value of which does not take into account the increase in market value of the properties used.
- Formation of legal persons to hold properties with the sole purpose of placing a front man or straw man between the property and the true owner.
- Contribution of real estate to the share capital of a company which has no registered address or permanent establishment which is open to the public in the country.
- Transactions in which unusual or unnecessarily complex legal structures are used without any economic logic. Natural and legal persons
- Transactions in which there are signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.
- Transactions which are begun in one individual's name and finally completed in another's without a logical explanation for the name change. (For example, the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed over to the owner, reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.).
- Transactions in which the parties:
    - Do not show particular interest in the characteristics of the property (e.g. quality of construction, location, date on which it will be handed over, etc.) which is the object of the transaction.
    - Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
    - Show a strong interest in completing the transaction quickly, without there being good cause.
    - Show considerable interest in transactions relating to buildings in particular areas, without caring about the price they have to pay.
    - Transactions in which the parties are foreign or non-resident for tax purposes and: o Their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying, even temporarily, etc.).
    - o They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).

- Transactions in which any of the payments are made by a third party, other than the parties involved. Cases where the payment is made by a credit institution registered in the country at the time of signing the property transfer, due to the granting of a mortgage loan, may be excluded. Intermediaries
- Transactions performed through intermediaries, when they act on behalf of groups of potentially associated individuals (for example, through family or business ties, shared nationality, persons living at the same address, etc.).
- Transactions carried out through intermediaries acting on behalf of groups of potentially affiliated legal persons (for example, through family ties between their owners or representatives, business links, the fact that the legal entity or its owners or representatives are of the same nationality, that the legal entities or their owners or representatives use the same address, that the entities have a common owner, representative or attorney, or in the case of entities with similar names, etc.).
- Transactions taking place through intermediaries who are foreign nationals or individuals who are non-resident for tax purposes.

Means of Payment

- Transactions involving payments in cash or in negotiable instruments which do not state the true payer (for example, bank drafts), where the accumulated amount is considered to be significant in relation to the total amount of the transaction.
- Transactions in which the party asks for the payment to be divided in to smaller parts with a short interval between them.
- Transactions where there are doubts as to the validity of the documents submitted with loan applications.
- Transactions in which a loan granted, or an attempt was made to obtain a loan, using cash collateral or where this collateral is deposited abroad.
- Transactions in which payment is made in cash, bank notes, bearer cheques or other anonymous instruments, or where payment is made by endorsing a third-party's cheque.
- Transactions with funds from countries considered to be tax havens or risk territories, according to anti-money laundering legislation, regardless of whether the customer is resident in the country or territory concerned or not.
- Transactions in which the buyer takes on debt which is considered significant in relation to the value of the property. Transactions involving the subrogation of mortgages granted through institutions registered in the country may be excluded. Nature of the Transaction
- Transactions in the form of a private contract, where there is no intention to notarise the contract, or where this intention is expressed, it does not finally take place.
- Transactions which are not completed in seeming disregard of a contract clause penalising the buyer with loss of the deposit if the sale does not go ahead.
- Transactions relating to the same property or rights that follow in rapid succession (for example, purchase and immediate sale of property) and which entail a significant increase or decrease in the price compared with the purchase price. Transactions entered into at a value significantly different (much higher or much lower) from the real value of the property or differing markedly from market values.
- Transactions relating to property development in high-risk urban areas, in the judgement of the company (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).
- Recording of the sale of a building plot followed by the recording of the declaration of a completely finished new building at the location at an interval less than the minimum time needed to complete the construction, bearing in mind its characteristics.
- Recording of the declaration of a completed new building by a non-resident legal person having no permanent domicile indicating that the construction work was completed at its own expense without any subcontracting or supply of materials.
- Transactions relating to property development in high-risk urban areas based on other variables determined by the institution (for example, because there is a high percentage of residents of foreign origin, a new urban development plan has been approved, the number of buildings under construction is high relative to the number of inhabitants, etc.).

Annex 2. Synopsis of the Guidance

Purpose of this Guidance (1)	Purpose	The purpose of this Guidance is to help Licensed Financial Institutions (LFIs) understand and mitigate risks when providing services to the dealers in precious metals and stones (DPMS) and real estate (RE) sectors, and to guide them in fulfilling their AML/CFT obligations. The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the two sectors are weighted as highly important in terms of risk and materiality in the UAE.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories:

		▪ national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers and other LFIs; and ▪ insurance companies, agencies, and brokers.
Understanding and Assessing the Risks of DPMS(2.1)	ML/TF Risks of DPMS	DPMS present higher risks to LFIs because their services and products are attractive to illicit actors as the trade in precious metals and stones permits illicit actors to move large quantities of value in a liquid, fungible format across borders outside of the traditional financial system.
	Features of DPMS that Increase Risk	Not all DPMS pose equal risk to LFIs. DPMS with the following characteristics may be higher risk: ▪ Operating in jurisdictions with lax or non-existent regulation or that are high risk for crime and terrorism; ▪ Offer products and services—such as the sale of gold bullion or of uncut stones—that allow customers to access a widely traded, fungible, anonymous form of value; or ▪ Serve a high-risk customer base, such as a high proportion of PEPs.
	Supervision of DPMS in the UAE	DPMS in the UAE may qualify as DNFBPs when they carry out any single monetary transaction or several transactions that appear to be interrelated or equal to more than AED 55,000. If so, they are required to apply AML/CFT controls like those used by LFIs. They are supervised by the Ministry of Economy, which has issued guidelines for supervised entities describing their AML/CFT compliance obligations.
Understanding and Assessing the Risks of the RE sector (2.2)	ML/TF Risks of the RE Sector	The RE sector presents a higher risk to LFIs because the sector offers an attractive way for illicit actors, criminals, and corrupt officials to move and store value while hiding their identity.
	Features of RE Sectors that Increase Risk	Not all customers and transactions related to the RE sector (in the UAE or elsewhere) pose equal risk to LFIs. Sectors with the following characteristics may be higher risk: ▪ Weak regulation and/or supervision of real estate brokers and agents; ▪ Widespread use of cash to purchase real property; ▪ Lack of transparency on beneficial owners of real estate; ▪ Openness to foreign purchasers, including 'golden visa' programs; and ▪ High liquidity and rising prices.
	Supervision of the RE Sector in the UAE	Real estate agents and brokers qualify as DNFBPs when they conclude operations for the benefit of their customers with respect to the purchase and sale of real estate. When they qualify, they are required to apply AML/CFT controls like those used by LFIs. They are supervised by the Ministry of Economy, which has issued guidelines for supervised entities describing their AML/CFT compliance obligations.
Mitigating Risk: Requirements for LFIs (3)	Risk-Based Approach	LFIs must take a **risk-based approach** in their AML programs and to individual customers. This means that they should assess all customers, including DPMS and RE sector customers, to determine their degree of risk. In assessing the risk of a DPMS and RE sector customers, LFIs should consider at least the following factors: ▪ The jurisdiction(s) in which the customer is based or does business, including both the jurisdictional risk of crime and terrorism but also

		the regulation in place on the DPMS and real estate sectors; ▪ The products and services the customer supplies to its customers; ▪ The customer's customer base; ▪ The quality of the customer's AML/CFT controls, where they exist.
	Customer Due Diligence	For all customers, including DPMS and RE Sector customers, LFIs must perform Customer Due Diligence with the following components:
		Customer Identification: DPMs and RE sector customers will often be businesses, and LFIs should ensure that their customer has the required licenses.
		Identification of Beneficial Owners: DPMs and RE sector customers will often be legal persons. For all legal person customers, LFIs must identify all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more. If no individual can be identified, the LFI must identify the individual(s) holding the senior management position(s) within the legal person customer.
		Understand the Purpose of the Account and the Nature of the Customer's Business: The purpose of the account and the nature of the customer's business are critical drivers of risk for DPMS and RE sector customers. LFIs should fully understand how their customer makes money and what types of transactions it expect to carry out through the LFI's account. As they seek to understand the customer's business, LFIs should collect all information necessary to assess customer risk.
		Perform Ongoing Monitoring: For all customers, LFIs must ensure that the customer information on file is up to date and accurate, and that the customer's activities are in line with the expectations set at onboarding. If not, the customer risk rating may need to be changed.
		Special Considerations for RE transactions: Many transactions related to the RE sector will be between persons who are not themselves members of the sector. LFIs should perform due diligence on all transactions that are outside of a customer's normal behavioral profile. If LFIs discover that a transaction is related to the purchase or sale of real estate, it may be necessary to perform additional due diligence.
	Suspicious Transaction Reporting	For customers of all types, LFIs must report any behavior that they reasonably suspect may be linked to money laundering, the financing of terrorism, or a criminal offence. Please consult the CBUAE's *Guidance on Suspicious Transaction Reporting* for further information.
	Governance and Training	The measures discussed above should be supported by a larger AML/CFT program with effective governance arrangements, including a sufficiently empowered Compliance Officer, and training that educates LFI staff on the risks of these sectors.

Guidance for Registered Hawala Providers and Licensed Financial Institutions Providing Services to Registered Hawala Providers

Effective from 15/8/2021 **Status:** In-Force

Part I: Registered Hawala Providers and Licensed Financial Institutions

1 Introduction

1.1 Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions...with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at centralbank.ae/en/cbuae-amlcft.

1.2 Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons which are licensed and/or supervised by the CBUAE in the following categories:

- Registered Hawala Providers ("RHP");
- National banks, branches of foreign banks; and
- Exchange houses.

Key Definitions and Acronyms

AML/CFT: Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.

Beneficial owner: The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client; or the natural person on whose behalf a transaction is being conducted; or the natural person who exercises

effective ultimate control over a legal person or legal arrangement.

Beneficiary Hawala Provider: The beneficiary's Hawala Provider, or receiving Hawala Provider, that receives the funds or equivalent value from the Originating Hawala Provider.

CBUAE Regulations: Any resolution, regulation, circular, rule, instruction, standard or notice issued by the CBUAE.

Hawala Activity: The arrangements for transfer and receipt of funds or equivalent value and settlement through trade and cash.

Hawala Provider Certificate: The Certificate issued by the CBUAE for carrying on Hawala activity in the UAE.

Legal person: Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.

Money or Value Transfer Service (MVTS): financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.

Originating Hawala Provider: The originator's Hawala Provider, or sending Hawala Provider, that initiates and carries out the transfer of funds or equivalent value to the Beneficiary Hawala Provider.

Registered Hawala Provider: Any natural person holding a valid residency visa or Legal Person, who is registered in the CBUAE's Hawala Providers Register in accordance with the provisions of its Circular No. 24/2019, including its agents or a network of agents.

Registered Hawala Provider Agent: Any natural or legal person carrying out activity outside the UAE on behalf of a Registered Hawala Provider.

1.3 Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions ("Cabinet Decision 74").
- Registered Hawala Providers Regulation issued by the CBUAE ("Circular No. 24/2019").

Under Articles 4 and 5 of Circular No. 24/2019, RHP and their customers and agents must strictly abide by all UAE laws, including civil laws, Commercial Companies' Law, federal laws on AML/CFT, and any Regulations and directions issued by the CBUAE ("the legal and regulatory framework in the UAE"). RHP may be guided by the FATF standards on AML/CFT and Proliferation and must abide by guidance issued by the CBUAE in this regard.

1.4 Organization of this Guidance

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the MVTS sector, including the Hawala service providers, is weighted as highly important in terms of risk and materiality in the UAE. This Guidance is addressed to the i) RHP and ii) LFIs that provide accounts or financial services to RHP. Part I of this Guidance applies to both RHP and LFIs, whereas Part II applies specifically to RHP and Part III specifically to LFIs.

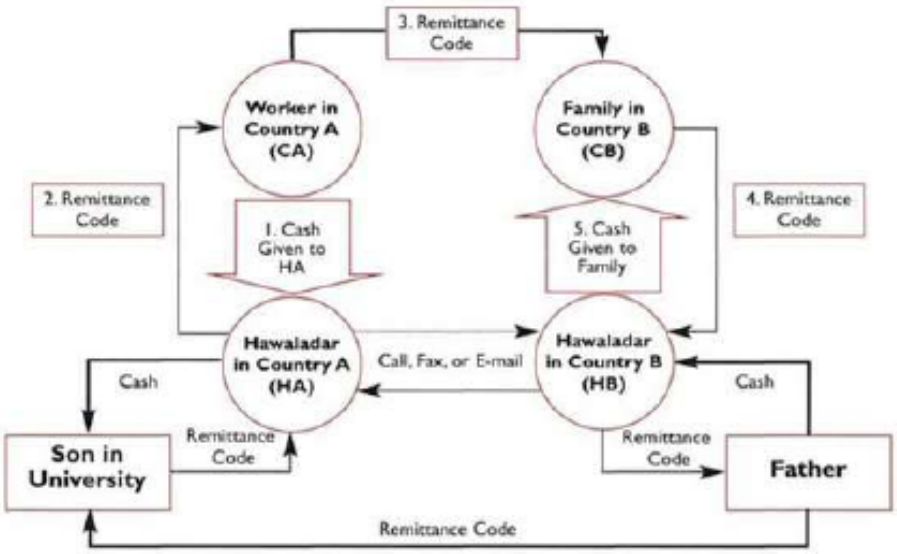
2 Overview of Hawala activity

The FATF defines hawala providers (and other similar service providers) as money transmitters, particularly with ties to specific geographic regions or ethnic communities, that arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. While hawala providers-also known as hawaladars-often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement.[2] Hawala is an activity based on trust and was established to avoid high charges by people who cannot afford them, the ability to reach beneficiaries in remote places quickly where banks do not operate, and the existence of strict currency controls in some countries. Because communication is often by text message and there is no need for funds to clear, hawala transfers may also be available faster than the ones made using the formal financial system. Although hawala providers generally specialize in transferring money between certain jurisdictions, they are also part of larger networks that can arrange transfers to almost any part of the world. Such transfers are likely to be slower and more expensive than transfers within the corridors in which the provider specializes. Although the hawala system minimizes use of the formal financial system, including use of international wires, it is important to note that almost all hawaladars will ultimately seek to conduct transfers, particularly international transfers through LFIs, and possibly to use other financial services. In doing so, they could expose the LFI with which they do business with to the risks of their own business activities and customers.

Common Attributes of Hawala Providers

- Fees for funds transfers are less than other channels and funds are available faster.
- Operates in communities in which the Hawala Provider is known, visible and accessible to the customers.
- Operates in areas with high numbers of expatriates/migrant workers of a specific ethnic group by providing cultural convenience with absence of language barriers, trust among community members, and solidarity among migrants with limited education levels and literacy.
- Operates with jurisdictions and regions underserved by other types of financial service providers, such as high-risk areas experiencing wars, civil unrest, conflicts, economic crisis, or weak or non-existent banking systems.
- Operates as a hawala provider to facilitate remittance services as a side business to other business activities.
- Provides one-off remittance services and communicates with the customer only as much as needed to conduct the transaction.

Sample Hawala Transaction:[3]



[2] See also the FATF report The Role of *Hawala* and Other Similar Service Providers in ML/TF (fatf-gafi.org)
[3] Source: IMF III Features of the Informal Hawala System : Informal Funds Transfer Systems : An Analysis of the Informal Hawala System: (imf.org)

3 Global risks of Hawala activity

Hawaladars' business model is built around satisfying customers' needs to move money rapidly across borders, a service that may also be misused by criminals as is to individuals seeking to conduct legitimate personal remittances. In recent years hawala providers have been repeatedly abused to transfer illicit funds, including funds involved in terrorist financing. Certain providers have been found to be fully complicit in these schemes, and even to operate as professional money launderers. In addition, hawala providers generally have the greatest competitive advantage in areas where more formal MVTS providers do not operate or have limited infrastructure, often because these jurisdictions are remote or classified as very high risk. Although this certainly does not mean that every transaction to those areas is illicit, it does suggest that the institutional risk profile of the average hawala provider is likely to be higher than that of other MVTS providers. In many jurisdictions, hawala providers operate *underground,* because they are providing an illegal service or because they and their customers don't want to be required to comply with rules related to taxes, currency controls, and AML/CFT compliance. This is especially common among hawala providers operating in jurisdictions where hawala is prohibited, unregulated, or illegal.

The inherent risk of hawala providers is influenced primarily by the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide, and their customer base:

1. Regulatory Environment

The regulatory environment for hawala providers clearly varies across jurisdictions. In some jurisdictions, they are not able to maintain a license or registration and therefore operate entirely underground. While operating underground is generally prohibited under the laws of the country where the hawala provider operates, it does not necessarily mean that a provider is a money launderer. Still, underground providers will seek to conceal their activities from financial institutions, and are extremely unlikely to comply with any AML/CFT obligations. Such entities may present themselves to LFIs as "general trading companies" or describe other business types that can justify regular international transfers, including dealing in precious metals or stones, trading in used cars, or in high value carpets.

Even in jurisdictions where hawala is legal and regulated such as the UAE, hawala providers may have only a basic understanding of their financial crime risks and obligations, and may not use systems and technologies that support compliance with those obligations. Furthermore, because hawaladars may lack strong AML/CFT preventive measures, they may be sought out by customers specifically hoping to take advantage of this possible weakness. As a result, hawala providers are almost always found to be classified as very high-risk customers by banks. A hawala

provider can strive to manage this risk by applying strong, targeted controls and maintaining an effective AML/CFT program that meets or exceeds UAE requirements and global standards (see Part II section 3 below).

2. Geography

Hawala providers, like all financial institutions, are heavily exposed to the risks prevalent in the geographies where they operate. The risk of a hawala provider, therefore, will depend in part on the illicit finance risks--including ML/TF and sanctions evasion--in the jurisdictions where it is established or has subsidiaries. In addition, a provider's risk will also be impacted by the jurisdictions with which it most frequently does business. For example, the risk of a hawaladar operating in the UAE and primarily executing transfers to and from Country X should be assessed based on the illicit finance risk in both the UAE and Country X.

3. Products, Services, and Delivery Channels

Hawala providers, by definition, all provide money or value transfer services using hawala networks, which is subject to higher risks. The risk of hawala transactions may be increased or decreased by the size and purpose of the transaction. Some hawaladars only carry out low-value personal remittances, while others service businesses by supporting commercial operations, which may involve relatively high-value transactions. Low-value personal remittances may be considered lower-risk, although low-value remittances to jurisdictions at high-risk for terrorist financing should be treated as equally high risk. **RHP in the UAE may perform only limited services (listed in section 4.1 below), but hawala providers established elsewhere may not have such restrictions on their activity.**

The risk involved in providing the hawala service is further impacted by the delivery channels through which it is offered. Channels that promote anonymity (accepting transaction orders by text or telephone; accepting cash; allowing agents or third parties to order transactions on behalf of the originator) increase the risk of the service. Some international law enforcement agencies have reported cases of hawala providers operating in virtual currencies; although still rare, such a delivery channel would be extremely high risk, as it would combine the general risks of hawala providers with those of virtual currencies, which offer illicit actors anonymity and access to a practically unregulated financial sector.

In addition, hawala services may not be the only financial product hawala providers offer. In many jurisdictions providers also offer small loans (often with pawned items as security) and sell stored value cards, or provide safekeeping services for cash. They may also engage in non-financial lines of business such as selling calling cards, mobile phones and SIM cards. All of these lines of business are cash intensive[4] and high-risk, and are generally not subject to AML/CFT controls. Even in a jurisdiction where hawala providers are regulated, they may commingle cash proceeds of these other services with hawala funds. This means that a hawala provider with an account at an LFI could use that account to support all aspects of its business, not simply provision of hawala services.

4. Customer Base

Most hawala providers are likely to serve a customer base made up of lower-income individuals seeking to conduct or receive fairly low-value transfers. Such a customer base is not necessarily low-risk, especially when customers have ties to jurisdictions that are at high risk for terrorist financing. The risk of the provider's customer base, however, will be further increased if the provider conducts larger transfers on behalf of business entities (e.g. trade-based transactions), if it has a high proportion of legal person customers, or if its customers include politically exposed persons.

---

[4] The CBUAE will issue Guidance for LFIs providing services to Cash Intensive Businesses.

4 Regulation and Supervision of RHP in the UAE

The CBUAE permits legitimate Hawala Activity as an important element of its continuous efforts to support financial inclusion and bring the unbanked population into the regulated financial system. To this end, Hawala is regulated by the Registered Hawala Providers Regulation issued by the CBUAE (``Circular No. 24/2019"). As per its articles 2.1

and 7.1 and Article 26 of the AML-CFT Decision, **all providers carrying on Hawala Activity in the UAE must hold a Hawala Provider Certificate issued by the CBUAE**; it is not permitted to carry on Hawala Activity without being registered with the CBUAE.

RHP are supervised by the CBUAE, who has the right to examine the business of RHP and their agents and customers whenever it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations. Similar to its all LFIs, the CBUAE applies the principle of proportionality in its supervision and enforcement process, whereby small RHP may demonstrate to the CBUAE that the objectives are met without necessarily addressing all of the specifics cited in the legal and regulatory framework in the UAE.

4.1 Permitted and non-permitted services by RHP

RHP are only permitted to provide well-defined services, which include non-commercial personal remittances and money transfer services to support commercial operations (such as trade transactions with jurisdictional corridors serviced by the hawala community).

RHP are not permitted to engage in any of the following transactions:

- Take deposits, exchange currencies or sell and purchase travellers' cheques;
- Provide any financial services other than money transfers (e.g. exchange of virtual assets/cryptocurrencies, loans, purchase of debts); or
- Execute transactions involving or on behalf of any other hawala provider in the UAE (as they are required by Circular No. 24/2019 to manage their business personally and never assign such task to another person, also known as "*nesting*"). This excludes the agents of the RHP in a foreign country (see also Part II section 3.3.5 below).

Part II: Guidance for RHP

1 Sanctions Obligations and Freezing Without Delay

Targeted Financial Sanctions (TFS) are legal restrictions on financial activity imposed by the United Nations Security Council (UNSC) or the UAE. An individual or legal person subject to TFS cannot send or receive money, or engage in any other kind of financial activity, without specific permission from the government of the UAE. The names of individuals or legal persons that are subject to TFS are included in lists published by the UN and the UAE (also known as "*listed persons*" or "*sanctioned persons*.")

RHP are required to fully comply with the obligation to implement all necessary measures without delay as described in the Cabinet Decision No. (74) of 2020, the "*Guidance on TFS for FIs and Designated Non-Financial Business and Professions (DNFBPs)*" issued by the Executive Office of the Committee for Goods & Material Subject to Import and Export Control ("Executive Office"), the "*Guidance for LFIs on the implementation of TFS*" issued by the CBUAE, the CBUAE Notice No. 3895/2021, and any of their amendments or updates thereof.[5] RHP should be aware that it is a crime in the UAE to provide funds or financial services, including money transmissions services, to a person subject to TFS. This means that if a person is subject to TFS, the RHP cannot do any of the following:

- Send that person money on behalf of a customer, no matter where in the world they are;
- Provide that person with money that another person has sent them; or
- Carry out a transaction of any kind for that person.

Appropriate implementation of TFS has four key steps, which RHP must follow to ensure they are compliant:

1. **Maintain awareness of UNSC and UAE sanctions lists, and rapidly become informed of changes to these lists.**

RHP should rely on the official website of the UNSC for the most updated UN Consolidated List:

- un.org/securitycouncil/content/un-sc-consolidated-list

RHP should rely on the official website of the Executive Office to obtain the most recent publication of the UAE sanctions List (Local Terrorist List) List issued by the UAE Cabinet:

- uaeiec.gov.ae/en-us/un-page
- uaeiec.gov.ae/ar-ae/un-page

In addition, under Article 21 of Cabinet Decision 74, RHP must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.

2. **Check the names of customers against the lists of sanctioned persons.**

Every time an RHP carries out a transaction, it must check before it sends or receives any money to make sure its customer, counterparty, or anyone else involved in the transaction is not listed on the UN or UAE sanctions lists. This process is known as 'screening process.' The RHP must screen the customer and the person to or from whom the customer is sending or receiving money. Where the customer is a legal person, it must screen the customer's beneficial owners (see section 3.3.3 below) and senior managing official. The RHP must also screen its counterparty who is executing the transaction at the other end. The result of the screening process can have the following results:

- A "confirmed match"; i.e. a customer or a customer's counterparty has the same full name as a sanctioned person; or
- A "potential match"; i.e. a customer or a customer's counterparty has a similar or partially matching name as a sanctioned person; in those cases, the RHP should use additional information, such as the person's date of birth, address, and nationality, to distinguish the two persons.

In addition, every time there is a change to the sanctions lists, the RHP must compare the newly listed persons against its list of past customers. If an RHP finds that it previously carried out a transaction involving a person who was not listed at the time but is now listed, it has not done anything wrong. But it must report the transaction so that the authorities are aware (see step 4 below).

3. **Immediately freeze any funds in the possession or under the control of the RHP that may belong to a listed person and cancel (where possible) any transactions involving a listed person.**

When a "confirmed match" is found through the screening process, RHP must immediately, without delay and without prior notice, freeze all funds.

i. "Freeze all funds" means that you must hold the funds. You cannot send them or give them to anyone except to a UAE authority. You cannot return them to the person who gave them to you. If the funds are cash, you should place the funds in a safe place, separate from other funds, until the authorities can collect them. If the funds are held in a financial institution, such as a bank, you should notify the financial institution, who will place them in a special account. If an RHP has recently completed a transaction that involves a listed person, the RHP should notify its counterparty so that they can freeze the funds at the other end if possible. It must keep records of the information that it used to confirm this.
ii. "Without delay" means within 24 hours of the listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be. This means that you must take active efforts to become aware of changes to the sanctions lists by registering on the Executive Office's website in order to receive

automated email notifications, and that once a change has been made, you must immediately put it into effect by refusing to carry out any transactions for or with a listed person.

iii. "Without prior notice" means that you must not tell the customer, or the person whose funds are being frozen, what the RHP is going to do.

When a "potential match" is found through the screening process, the RHP must suspend without delay any transaction and refrain from offering any funds or services. It must keep records of the information that it used to confirm this.

4. **Report any listed persons and the actions the RHP has taken to the appropriate authorities**

With regards to LFIs obligation for TFS reporting, the CBUAE in coordination with the Executive Office, has established a unified mechanism to report TFS obligations utilizing the UAE Financial Intelligence Unit's (FIU) online reporting platform (goAML).

In case of any "confirmed match" to a listing of names of individuals or legal persons to the Local Terrorist List and the UN Consolidated List, the RHP are required to report any freezing measures, prohibition to provide funds or services or any attempted transactions via the goAML platform within two business days by selecting the Fund Freeze Report (FFR). The RHP must also ensure all the necessary information and documents are submitted.

In case of any "potential match" to a listing of names of individuals or legal persons to the Local Terrorist List or UN Consolidated List, the RHP are required to report the potential match via the goAML Platform by selecting the Partial Name Match Report (PMNR). The RHP must also ensure all the necessary information and documents are submitted. In addition, the RHP must uphold suspension measures related to the "potential match" until further instructions are received via the goAML Platform on whether to cancel the suspension or implement freezing measures.

The TFS related reports (FFR or PMNR) submitted via the goAML Platform will be received simultaneously by the CBUAE and the Executive Office. RHP should also consult the CBUAE's[6] and the Executive Office's[7] websites respectively as updated from time to time.

---

[5] Available at centralbank.ae/en/cbuae-amlcft.
[6] Available at: centralbank.ae/en/cbuae-amlcft
[7] Available at: uaeiec.gov.ae/en-us/un-page

2 Registration and other Requirements

2.1 Registration

Under Article 2 of Circular No. 24/2019, **a resident natural person or legal person may not carry on Hawala Activity in the UAE unless the applicant holds a Hawala Provider Certificate issued by the CBUAE** and registered in the CBUAE Hawala Providers Register. Any resident natural person or legal person may apply for registration and obtain a Hawala Provider Certificate from the CBUAE. The applicant should not be of UAE nationality, should be legally competent, and officially residing in the UAE. The said application shall be made on the CBUAE's prescribed forms on the CBUAE's website.[8]

---

[8] Available at centralbank.ae/en/cbuae-amlcft.

2.2 CBUAE Notification of Approval/Rejection

Under Article 3 of Circular No. 24/2019, the CBUAE may agree or decline an application for a Hawala Provider Certificate. In case of approval, the CBUAE shall issue a Hawala Provider Certificate valid for one year, renewable for similar periods. The CBUAE shall notify the applicant in writing, and may include in the Hawala Provider Certificate

whatever terms and conditions it deems appropriate. In case of rejection, the CBUAE shall notify the applicant in writing indicating reasons for rejection.

2.3 Re-Registration

Under Articles 2 and 4 of Circular No. 24/2019, RHP should submit to the CBUAE an application for renewal of the Hawala Provider Certificate within a period of not less than two months from the date of expiry of the original certificate or any renewals thereof. The said application should be made on the CBUAE's prescribed form titled "*Application to Re-register Hawala Providers*" on the CBUAE's website.

2.4 Requirements for Trade License, Security and Reporting Systems

As per Article 2 of Circular No. 24/2019 and the respective application requirements, RHP must complete the following requirements within 90 days from the date mentioned in the final registration certificate as well as submit proof of completion to the Licensing Division of the CBUAE:

- Add Hawala Activity to the commercial trade license.
- Install security systems; i.e. CCTV and police connections.
- Register in the relevant Services Access Control Manager (SACM) and subsequently to the UAE FIU's goAML portal by following the steps in the registration guides issued by the FIU previously sent to RHP. Registration on SACM is a prerequisite for goAML registration;
- Register in the relevant SACM and subsequently to the CBUAE's Remittance Reporting System (RRS) for the daily reporting and Integrated Regulatory Reporting System (IRR) for the quarterly reporting (see Part II section 4 below). Registration in SACM is a prerequisite for RRS & IRR registration. In order to register in SACM, RHP will be required to provide the following information to the CBUAE via e-mail on hawala@cbuae.gov.ae:
- Trade name of the RHP;
- First and last name of the user;
- Emirates ID number and copy of Emirates ID;
- Email address; and
- Mobile phone number.
- RHP should register for the Integrated Enquiries Management System (IEMS) by referring to the IEMS User Guide available at the relevant link in FIU's website.[9]

Failure to submit the above within the specified period may result in a registration certificate withdrawal.

[9] Available at: uaefiu.gov.ae.

2.5 Requirement for a Bank Account

As per Article 2 of Circular No. 24/2019 the RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with details of such account. In addition, they should inform their account manager at the bank of their intention to use the account to carry out Hawala Activity.

3 AML/CFT Program

As per Articles 4, 20, 21 and 26 of the AML-CFT Decision, RHP are required to establish and maintain effective AML/CFT compliance programs designed to prevent them from being misused to facilitate money laundering or terrorist financing (ML/TF). The program must be risk-based and appropriate to the risk of the RHP, taking into consideration its:

- Size;
- Volume of transactions;
- Types of remittances offered (personal only or personal and commercial);
- Complexity;
- The nature and volume of its Hawala Activity;
- The nature of its customer base; and
- The geographic areas in which it operates.

This means that where an RHP engages in higher-risk activities (as discussed below in section 3.2), or does a higher volume of business, it must have a more sophisticated AML/CFT program and employ more intensive measures to manage this risk. The section that follows discusses the **mandatory minimum elements** of an AML/CFT program under the legal and regulatory framework in the UAE as well as ways that RHP can make adjustments to respond to their risk. It is divided into four parts, as follows:

1. **The AML/CFT Program and the Compliance Officer**. This part discusses the content of the AML/CFT program and how it should be implemented by the RHP.
2. **Understanding Risks**. This section discusses how to identify the RHP's ML/TF risks so that the RHP can build an appropriate AML/CFT program.
3. **Customer Due Diligence**. This section discusses the mandatory procedures for identifying and understanding the RHP's customers and counterparties.
4. **Record Keeping**. This section discusses the records of activity that the RHP must maintain and provide to law enforcement authorities and counterparties.

3.1 The AML/CFT Program and the Compliance Officer

As per Article 21 of the AML-CFT Decision, each RHP must have a specific person, the Compliance Officer, who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT program. This person must be an employee, manager, or owner of the RHP. **In large RHP**, with multiple employees and substantial revenues from Hawala Activity, the CBUAE expects that the Compliance Officer will be a full-time position without any other responsibilities for managing the business. **In small RHP**, however, the CBUAE recognizes that the Compliance Officer is likely to have other responsibilities beyond management of the compliance program. If the RHP is owned and operated by a single person, that person will be the Compliance Officer.

The Compliance Officer is responsible for the following:

- Ensure full compliance with the legal and regulatory framework in the UAE and this Guidance.
- Making sure that other employees of the RHP (where relevant) comply with the legal and regulatory framework in the UAE and this Guidance, and abide by the RHP's own policies and procedures; and
- Implementing the compliance program elements described in this Guidance, including conducting the risk assessment.

The RHP's AML/CFT compliance program must include all the measures discussed in the following sections as well as the following components:

- **Provide education and training to appropriate personnel.** RHP employees who participate in Hawala Activity must be trained to understand how to comply with the legal and regulatory framework in the UAE and this Guidance, and abide by the RHP's policies and procedures. It is not acceptable for an untrained employee to have responsibility for collecting or disbursing customer funds and initiating transactions.
- **Conduct a periodic audit of the AML/CFT program.** RHP are required to arrange for a regular independent audit of their program by hiring an external qualified independent auditor approved by the CBUAE. **Small RHP** should be audited once every two or three years, while **large RHP** once every year. It

is important to note that the audit must be independent; i.e. an RHP may not audit itself.

3.2 Understanding Risks

According to Article 16 of the AML-CFT Law and Article 4 of the AML-CFT Decision, RHP must identify, assess and understand the ML/TF risks to which they are exposed, and how they may be affected by those risks, in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. The sophistication of an RHP's risk assessment process depends on the RHP's size and operations. A **large RHP** is expected to produce an extensive risk assessment that complies fully with the standards outlined in the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof. This assessment may be done by an external consultant, but the RHP retains ultimate responsibility for its content and its compliance with the standard set in the Guidelines. The CBUAE recognizes, however, that a **small RHP** has limited services and resources. RHP of this type can follow the risk assessment process discussed below. All RHP must document their risk assessment, even if it is in the form of notes, to demonstrate that they have thoughtfully completed this process. They must be able to understand their findings and explain them if called upon to the CBUAE.

The Compliance Officer should begin the risk assessment process by carefully reading and understanding Parts I and II of this Guidance, which contain essential information about the risks faced by an RHP. The Compliance Officer should then consider the RHP's risk in the following risk categories. The discussion below does not cover every factor that increases or decreases risk and RHP should consider any other factors based on their knowledge and experience.

1. **Customer Risk.** This is the risk that your customers may be involved in ML/TF. By receiving money from a customer who is involved in illegal activities, the RHP itself can unwittingly become involved in those activities. Some examples of questions that RHP can use to assess customer risk include:

    a. *Are my customers mostly individuals, or do I have many customers that are legal persons?* When you provide services to a company, you don't always know who you're really dealing with. So having many legal person customers may increase your risk.

    b. *Are my customers only sending remittances to family, or are they engaging in business*? Business activities are generally considered to be higher risk for ML/TF because amounts are higher and it's harder for the RHP to understand the true purpose of the transaction.

2. **Geographic Risk.** Some countries are high risk for illicit activity, whether because they have a high volume of crime and terrorism, or because their financial sector doesn't have controls to prevent the movement of illicit funds. If an RHP operates in those countries, either because it has agents there or because it frequently sends or receives money there, then it is exposed to that risk. Questions an RHP can ask to assess its geographic risk include:

    a. *Do I regularly do business in or with countries that have an ongoing insurgency? Where terrorist attacks are frequent*? These countries will be very high risk.

    b. *Do I regularly do business in or with countries listed on the FATF list of monitored jurisdictions?*[10]

3. **Products and Services Risk.** RHP are permitted to offer only limited products and services (see Part I section 4.1 above). Within the group of permitted products, transfers connected to commercial activity are generally considered to be higher risk than those connected to personal remittances.

4. **Delivery Channel Risk.** The way an RHP delivers its products and services will also impact its risk, because some delivery channels make it difficult to understand and observe the customer. For example, if an RHP

accepts orders for remittances via text message or phone call, or allows customers to initiate a transaction by giving money to an associate, who then delivers it to the RHP, this will make their activities higher risk.

Based on the considerations above, RHP should give themselves an overall score of Low, Medium, or High risk. **RHP should complete the risk assessment process at least once a year**. RHP should understand their risk assessment, its findings, and what it means for their business. They should consider their risk assessment when designing and implementing their AML/CFT program. Where they assess themselves as higher risk, they should take additional precautions.

---

[10] The FATF list can be found at fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate).

3.3 Customer Due Diligence

Customer due diligence ("CDD") is the process by which an RHP identifies and understands its customer. CDD is required by Article 5 of the AML-CFT Decision and is essential to protecting the RHP from abuse, and to deterring and detecting ML/TF schemes. In specific cases outlined below, and whenever the RHP believes that higher risks are present, the RHP must perform Enhanced Due Diligence ("EDD"). EDD involves more intensive measures to discover information about the customer.

The RHP must perform Customer Identification Diligence ("CID"), CDD or EDD prior to conducting each and every transaction, even if the customer is a repeat customer (see sections 3.3.1 to 3.3.4 below for their details)**. An RHP must not conduct a transaction if the appropriate diligence has not been performed or completed.**

When to Use CID, CDD and EDD	
Transaction	**What is Required**
A natural person sends or receives a transfer between AED 1 and AED 3,499	CID, unless higher risks are present, in which case CDD & EDD as well.
A natural person sends or receives a transfer of between AED 3,500 to AED.54,999	CDD, unless higher risks are present, in which case EDD as well.
A natural person sends or receives a transfer of AED 55,000 or greater.	CDD and EDD
A natural person from a high-risk jurisdiction sends or receives a transfer of any value.	CDD and EDD
A natural person who is a politically exposed person sends or receives a transfer of any value.	CDD and EDD
A legal person sends or receives a transfer of any value.	CDD and EDD

3.3.1 Customer Identification Diligence

The CID process must be applied for a natural person who sends or receives a transfer between AED 1 and AED 3,499. The CID process is the verification of the original identification documents of the customer who is a natural person and the systematic recording of basic customer information in the point of sale system without the need to retain copies of the identification documents. The customer's full name, address, mobile number, nationality, date of birth, ID type (Emirates ID, or passport number when Emirates ID is not available) and ID number must be recorded in the point of sale system and printed on receipts.

3.3.2 Customer Due Diligence for Natural Persons

Article 4 of Circular No. 24/2019 requires RHP to identify and verify the identity of their customers, including remitters and beneficiaries, by using Emirates ID, or passport when Emirates ID is not available. **RHP must collect at least the following information for each customer:**

- Name,
- Emirates ID number or passport number when Emirates ID is not available;
- Date of birth and nationality;
- Address;
- Mobile number;
- Occupation; and
- The name of the person from whom the customer is receiving money, or the person to whom the customer is sending money and their country.

This information must be printed on customer receipts. RHP must record this information and store it in their files for five years. RHP must also take a clear photo or photocopy of the customer's identification document and retain it for five years.

The CDD process should also be applied when it appears that a natural person may be deliberately splitting up a larger transfer to evade the CDD requirement (for example by repeatedly once in a week transfer value below AED 3,500 per transaction).

Using this information, as discussed in Part II section 1 above on sanctions obligations, RHP should screen their customers, including the sender/beneficiary as appropriate, and the transaction against the UN Consolidated List and the Local UAE Terrorist List. Screening must be performed before carrying out any transaction for the customer. If there is a match, the RHP should carefully consider whether the other data collected (date of birth, country of birth) match the information available for the listed person in question. The RHP may continue with the transaction only if it is confident that its customer or the person on the other end of the transaction is not a listed person. In addition, if the RHP discovers that any party to the transaction is listed on the UN Consolidated List and the Local Terrorist List, it must not return the customer's funds or provide the customer with funds that have been sent to him, but must instead freeze the funds.

Furthemore, RHP should obtain a clear understanding of the intended purpose and nature of the transaction and ensure that it does not breach the permitted services by RHP listed in Part I section 4 above. RHP should consider whether it is consistent with what they know about the customer. Some examples of transactions that may require further investigation include:

- A customer who says he works as a labourer wishes to transfer a sum that is greater than the average yearly income for someone in his position.

- A customer visits the RHP on a regular basis and makes small or moderate-sized transfers, but the sum of the amounts he transfers over the course of the year is greater than the yearly income for someone in his position.

- A customer says that he has no occupation, but continues to make transfers or transfers a large sum.

- A customer who is from country A states that he is sending funds to a family member, but the beneficiary is located in country B.

- A customer from country A makes regular transfers to people he says are family members in that country, but they appear to live in different regions of country A and their relationship to the customer is not clear.

These transactions are not necessarily illicit, but they suggest that the RHP needs to collect additional information. For example, a customer may actually be acting on behalf of a business. In that case, the RHP's customer is actually

the business, and it must perform CDD on the business as described in section 3.3.3 below. If the RHP has any additional concerns, it should follow the EDD procedures discussed in section 3.3.4 below.

RHP must cease and reject any transaction if they cannot collect any of the information required above, or if they cannot comply with any of the above requirements.

3.3.3 Customer Due Diligence for Legal Persons

When a legal person like a company uses an RHP to conduct a transaction, the RHP's customer is the company itself, not the individual representing the company. A legal person conducts a transaction when the funds involved belong to the legal person, and when the transaction is made as part of carrying out the legal person's business. If the customer is a legal person, it must be registered and based in the UAE to carry out transactions through a RHP. Legal persons such as companies, bodies corporate, foundations, partnerships, or associations, along with similar entities do not have bio-data like individuals and can transact under their own names while being controlled by other individuals. This means that they require specific CDD procedures. As per Articles 8 and 9 of the AML-CFT Decision **RHP must perform the following actions for a legal person customer:**

1. Collecting and recording the following information about the legal person customer:
    a. The legal person's name;
    b. The legal person's legal form (e.g., limited liability company);
    c. The address of the legal person's main office or headquarters;
    d. The legal person's trade license; and
    e. The name of the legal person's senior managing official.
2. Conducting CDD as described in section 3.3.2 above on the individual representing the customer (the individual who is directly ordering the transaction).
3. Determining that the representative is authorized to conduct the transaction via a valid authorization, such as the trade license and/or a letter from the legal person customer's management on its letterhead.
4. Identifying and verifying the identity of the customer's beneficial owners.
    a. Beneficial owners are the individuals who own and control the legal person. In many cases, the managing director or other similar top official will also be the beneficial owner, but not always.
    b. RHP must identify every individual who owns 25% or more of the legal person customer. They must collect their names, and then perform CDD on them as required by section 3.3.2 above.
    c. RHP can collect the names of beneficial owners, and thus determine who to perform CDD on, by asking the customer's representative. If they are concerned about the information provided by the representative, they should ask for documentation to prove ownership.
    d. If no individual owns 25% of the legal person customer, RHP must identify, and conduct CDD on the individual who is the customer's senior managing official.
    e. Beneficial owners cannot be other legal persons. If a legal person customer is owned by other legal persons, the RHP must understand their ownership as well until it identifies all individuals owning at least 25% of its customer.
5. Understanding the customer's ownership and control structure. The RHP must understand who owns the customer, who exercises control over it and how.
6. Understanding the nature of the customer business. The RHP must understand what sort of business the customer engages in and how the customer makes its money. If the customer's business doesn't make sense, or if the customer has no apparent business activities, that calls into question whether the funds involved in the transaction actually came from legitimate business activities.

- Conducting sanctions screening on all related parties. The RHP must at least screen the following names against sanctions lists:
    a. The name of the legal person customer;
    b. The name of the customer's representative;
    c. The name of the beneficial owner(s);
    d. The name of the customer's senior managing official; and

e. The customer's address.

As with CDD for natural persons, RHP must take a clear, readable photo or photocopy of documents obtained from the customer during CDD, and must retain those documents for five years after the transaction.

3.3.4 Enhanced Due Diligence

Sometimes CDD alone as described above is not sufficient to fully understand a customer. In addition, for certain customers, an extra level of due diligence is required. In those cases, the RHP must perform EDD in the following circumstances:

1. The customer is a legal person. In these cases, the RHP must perform all the steps listed in section 3.3.3 above, plus additional due diligence as described here.

2. The customer is a natural person carrying out a transfer worth AED 55,000 or above. In those cases, the RHP must perform all the steps listed in section 3.3.2 above, plus additional due diligence as described in this section below.

3. The customer is a politically exposed person. During CDD, the RHP must collect information regarding the occupation of a natural person customer, and the beneficial owners of a legal person customer. If the customer, or the beneficial owners of a legal person customer, indicates that he or she is a government official with any government, the RHP must ask additional questions to understand that individual's rank and status. If the individual holds a high-ranking position in any government, then EDD is required for the customer. This is to make sure that the funds involved are not related to corruption or abuse of the customer's position.

4. The customer is from, or is sending a remittance to, a high-risk jurisdiction. As discussed in section 3.2 above, high-risk jurisdictions are those with a higher risk of ML/TF.

RHP should **consider** performing EDD when there are other high risks associated with the transaction, such as concerns about the customer's behaviour or about the source of the funds involved in the transaction.

When performing EDD, RHP must follow the following mandatory steps:

- Seek approval from the manager of the RHP to carry out the transaction. If the RHP is owned and operated by a single person, this step is not necessary.
- Collect additional information to understand the source of funds involved in the transaction and the customer's overall source of funds (i.e. source of wealth). For instance, the RHP may ask for a pay slip to verify the customer's income.
- Collect additional information about the customer's business. For example, if a transaction is linked to the sale of goods, the RHP may request to see the invoice.

3.3.5 Agent Due Diligence

RHP may use agents in a foreign country to carry out activity on their behalf in that foreign country. This generally entails the corresponding agent in the foreign country executing payments on instructions from the RHP, or the agent sending instructions to the RHP to execute payments domestically. It should be noted that **RHP are not permitted to use agents to carry out activity on their behalf in the UAE** (as they are required by Circular No. 24/2019 to manage their business personally and never assign such task to another person, also known as "*nesting*".)

RHP are exposed to risks when their agents engage in transactions that create risks for ML or TF. RHP must identify and assess the ML/TF risks they may be exposed to from the use of agents to provide activity on their behalf in a foreign country. RHP should ensure that they understand who their agents are, and that they are not breaching any

applicable AML/CFT laws and regulations. In order to reduce their exposure to ML/TF risks, RHP are required to perform appropriate due diligence on their agents, to ensure they thoroughly know their agents and monitor their transactions to ensure that they are legitimate. **The required elements of due diligence on agents are as follows:**

- When entering into a business relationship with an agent, as a first step, the RHP should identify and verify the identity of the agent, using reliable, independent source documents, data or information.
- RHP should also identify and take reasonable measures to verify the identity of the beneficial owner(s) and understand the ownership and control structure of the agent, such that the RHP is satisfied that it knows the beneficial owner(s) and that the agent is not a shell bank.
- RHP should gather sufficient information to understand the purpose and intended nature of the business relationship, which includes understanding what types of customers the agent intends to service through the business relationship, how it will offer services, the transaction volume and value, and the extent to which any of these are assessed as high risk.
- RHP should also gather sufficient information and determine from publicly available information the reputation of the agent, including whether it has been subject to a ML/TF investigation or regulatory action. In addition, RHP should ensure that the agent has proper AML/CFT controls.
- RHP should conduct ongoing due diligence of the business relationship, including periodical reviews of the CDD information on the agent, and ongoing monitoring to detect any changes in the agents' activity pattern that may indicate unusual activity.

RHP should keep up-to-date agent lists and retain them for a period of five years. RHP must provide the CBUAE current lists of their agents and the countries in which they operate. In addition, RHP should make current lists of their agents available to the relevant authorities within the country in which they operate. RHP should ensure that their agents fully adhere to the procedures of record keeping as described in this Guidance and that they make those records available to the RHP immediately upon request.

3.4 Record Keeping

Under Article 16 of AML-CFT Law and Article 24 of the AML-CFT Decision, RHP, as remittance providers, have very important obligations relating to the records they maintain about the remittances they execute.

3.4.1 Record Keeping Related to Remittances

1. Sending a Remittance

When the RHP's customer is the person originating a transaction, the RHP must collect the following information through the CID and CDD process:

- The sending customer's name;
- His or her Emirates ID, or passport number when Emirates ID is not available;
- His or her date and nationality;
- His or her address;
- Mobile number;
- Occupation; and
- The name of the beneficiary of the transaction and the country it is sent to.

The RHP must assign the transaction a unique ID number that allows the RHP to quickly identify and track the transaction. The RHP must provide all of this information to the hawala provider at the other end of the transaction and keep the relevant record. **The RHP must not carry out the transaction if it has not supplied this information.**

2. Receiving a Remittance

When the RHP's customer is the person receiving the remittance, the RHP must conduct CDD on the beneficiary and make sure that its customer's information matches that of the beneficiary identified in the information provided by the Originating Hawala Provider and keep the relevant record. The information must include:

- The receiving customer's name;
- His or her Emirates ID, or passport number when Emirates ID is not available;
- His or her date and nationality;
- His or her address;
- Mobile number;
- Occupation; and
- The name of the sender of the transaction and the country it is sent from.

**The RHP's partners and agents outside the UAE should comply with the requirements under ``*Sending a Remittance"* above even though they are not subject to UAE laws.** If a RHP receives a transaction order from a hawala provider outside the UAE that does not contain the information required under ``Sending a Remittance" above, it cannot perform required sanctions screening or identify whether the transaction is suspicious and needs to be reported to the FIU. Therefore, the RHP should require its agent or counterpart to provide the information listed before it releases the funds to the beneficiary.

3.4.2 Other Types of Record Keeping

According to the AML-CFT Law and the AML-CFT Decision, RHP must keep all records obtained through the CDD process; copies of personal identification documents provided during CDD; and copies of Suspicious Transaction Reports (STR) filed with the FIU. Under Article 4 of Circular No. 24/2019, RHP are required to have forms in which the customers fills in the necessary information to originate the transaction; RHP must retain these forms as well.

RHP must also maintain records of transactions. These records must be sufficiently detailed to allow authorities to reconstruct and understand the transaction. They must at least include the names of the sender and beneficiary, the date of the transaction, and the amount of the transaction, and be organized in such a way so that the RHP and authorities can easily find the records they need for a specific transaction.

RHP must make the records described here, or any other records, available to the competent authorities immediately upon request. All the records described in this section must be kept for at least five (5) years, from the date of completion of the transaction, or for longer if directed by the CBUAE or other authority.

4 Reporting Obligations

4.1 Daily Reporting

Under Article 4 of Circular No. 24/2019, RHP are required on a daily basis to upload electronically to the CBUAE, via its Remittance Reporting System ("RRS") and/or other applicable system, the data and details of all transfers, remitters and beneficiaries as per the forms prepared by the CBUAE for this purpose.

4.2 Quarterly Settlement Statements

Under Article 4 of Circular No. 24/2019, RHP should submit to the CBUAE statements of their settlement accounts on a quarterly basis along with other required forms, as well as provide the CBUAE with any data, information, or statistics it may require at any time and for any specific period.

4.3 Reporting Suspicious Transactions and Registration to GoAML

RHP must monitor transactions that they carry out to identify those that may be suspicious and where a Suspicious Transaction Report (``STR"), or suspicious activity report ("SAR") or other report types may need to be filed with the FIU. Monitoring begins at the CDD stage, but does not end there. RHP must keep records of customer activity so that they can examine it to identify patterns over time that may be cause concern. RHP must take into account all information available, including regarding the originator and beneficiary(ies) of a transaction, in order to determine whether an STR is to be filed.

Situations in which it may be necessary to file an STR/ SAR include:

- A customer begins the CDD process, but cancels the transaction and leaves when he discovers the information that the RHP is required to collect.
- The RHP completes CDD on a customer, but still has doubts as to whether the transaction was legitimate or whether the customer's stated reason for the transaction was the true one.
- A customer carries out transactions larger than his stated income without providing a valid justification.
- A natural person customer regularly orders transactions just below the AED 55,000 threshold for when EDD is required (i.e. either tied to the threshold or if there are other risk factors that may trigger EDD).
- Multiple customers send money to, or receive money from, the same person, and there is no clear connection between the customers.
- The RHP suspects that a customer is carrying out transactions that are disallowed under Part I, section 4.1 of this guidance.

Under Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, if the RHP suspects that a transaction, attempted transaction, activity, or funds (including agents' transactions), constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime, they must submit an STR, SAR or other report types to the FIU using the ``goAML" portal. RHP must submit this report without delay, meaning as soon as reasonably possible after the transaction takes place or their suspicions develop. All RHP must register with the goAML portal so that they can easily file these reports.

Reporting a suspicious transaction is not an admission of guilt or wrongdoing. STRs filed by RHP help law enforcement authorities identify and track potential criminal behaviour. As long as the RHP complies with the procedures in this guidance document, it will not generally be held responsible for a transaction that turns out to have been involved in a crime. But a failure to report a transaction that an RHP should know to be suspicious can result in penalties.

For more detail and information, please refer to the "*CBUAE Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting.*"

5 Penalties

Under Article 7 of Circular No. 24/2019, violation of any provision may be subject to supervisory action as deemed appropriate by the CBUAE. In addition, without prejudice to other sanctions stated in other laws in the UAE, the CBUAE may impose administrative and financial sanctions and penalties in accordance with the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities and the CBUAE Regulations issued in implementation thereof.

Part III: Guidance for LFIs

1 Understanding Risks

Please refer to Part I, Section 3 for a description of the risks of Hawala Activity.

The Circular No. 24/2019 requires that RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with details of such account. **The CBUAE expects LFIs to accept RHP customers**, but LFIs must manage the risk that these transactions create through the use of appropriate controls (see Part III, section 2 below). **LFIs must not accept as customers *unregistered* hawala providers based in the UAE, and must immediately report an STR to the FIU, inform CBUAE when they are detected, and closely monitor the relationship.** Please see Part III, sections 2.2 and 2.3 below for guidance on detecting *unregistered* MVTS.

2 Mitigating Risks

The sections below elaborate on how LFIs can apply specific preventive measures to identify, manage, and mitigate the risks associated with hawala providers customers. These are not exhaustive and LFIs should consult the legal and regulatory framework in force in the UAE for the measures to be taken. The controls mentioned below should be **at the minimum** integrated into the LFI's larger AML/CFT compliance program, and supported with appropriate governance and training.

2.1 Risk-Based Approach

LFIs should take a risk-based approach to the preventive measures they put in place for all customers, including hawala providers. **The risk-based approach has three principal components:**

2.1.1 Conducting an Enterprise Risk Assessment

As required by Article 4.1 of the AML-CFT Decision, the enterprise risk assessment should reflect the presence of higher-risk customers, including hawala providers, in an LFI's customer base. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the LFI's controls risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its hawala providers customers, including the preventive measures discussed below.

2.1.2 Identifying and Assessing the Risks Associated with Specific Customers

The LFI should assess the risk of each customer to identify those that require EDD and to support its entity risk assessment. As discussed in Part I section 3 above, the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide and its customer base, are critical determinants of a hawala provider's inherent risk. In assessing the risks of a hawala provider customer, LFIs should consider:

i. **Controls Risk:** LFIs should seek to understand the regulatory requirements in place for the customer, as well as how well they are enforced. The regulatory requirements placed on hawala providers vary markedly across jurisdictions.

ii. **Geographic Risk:** The risks associated with the jurisdictions in which the provider lives (for individuals) or is registered/established (for legal persons) and where it operates, including the jurisdictions where its main counterparties are based and where it has subsidiaries.

iii. **Product, Service, and Delivery Channel Risk:** LFIs should assess risk in this category on two dimensions:

    a. The products and services that the hawala provider offers to its customers, and

b. The delivery channels through which it offers these products and services.

Products, services, and delivery channels that promote the rapid, anonymous transfer of high values are particularly attractive to illicit actors.

iv. **Customer Risks**: For hawala provider customers, customer risk can be assessed as the proportion of higher-risk customer types (e.g. politically exposed persons, legal persons, and customers from high-risk jurisdictions) within the provider's customer base.

Questions that an LFI may ask to determine the risk profile of a hawala provider customer include, but are not limited to:

- *Where is the provider incorporated? Where does it operate? Are these high-risk jurisdictions?*
- *What products and services does the provider offer its customers?*
- *What volume of transactions does the provider carry out?*
- *What customer base does the provider serve?*
- *What is the regulatory environment in the jurisdiction(s) where the provider is incorporated/has operations?*
- *Is there an authority that actively enforces the requirements?*
- *Does the provider perform appropriate CDD, transaction monitoring, record keeping, and sanctions screening?*
- *Does the provider intend to use its account to execute transactions on behalf of its customers?*

In addition to risk rating hawala providers, LFIs should also consider the risks of specific transactions, especially high-value transactions, those involving high-risk jurisdictions, and those that represent departures from a customer's standard or expected behaviour.

2.1.3 Applying EDD and Other Preventive Measures

Where the LFI determines a customer to be higher-risk, Article 4.2(b) of the AML-CFT Decision requires that the LFI apply EDD. Specific EDD steps are also required for hawala providers customers that are politically exposed persons, or are owned or controlled by a politically exposed person, or are based in a higher-risk jurisdiction.

2.2 Customer Due Diligence and Enhanced Due Diligence

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFI's services. **Where an LFI cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LFI should not continue it.** LFIs should also consider filing an STR, SAR or other report types to the FIU as discussed in section 2.3.2 below. This guidance is not an exhaustive list of LFIs' CDD obligations and LFIs should consult the legal and regulatory framework in force in the UAE for the measures to be taken.

2.2.1 Customer Identification and Verification

Under Article 8 of AML-CFT Decision, LFIs are required to identify and verify the identity of all customers. Please see also the AML/CFT Guidelines for Financial Institutions for full information on customer identification. In particular, when verifying the Emirates ID card, LFIs must use the online validation gateway of the Federal Authority for Identity & Citizenship and keep a copy of the Emirates ID and its digital verification.

Hawala providers based in the UAE are required to have an active registration certificate issued by the CBUAE and a commercial trade license that includes Hawala Activity. In particular, when opening any accounts for hawala providers, LFIs must physically check the original hawala provider registration certificate issued by the CBUAE and keep a copy thereof. LFIs should not form business relationships or conduct transactions with hawala providers

without an active registration certificate issued by the CBUAE (unregistered hawala providers). In addition, if an LFI determines that a customer or prospective customer has materially misrepresented itself or its business, it must not accept the customer, must exit the relationship if one has been established, should add the customer, its beneficial owners, directors and managers to its internal watchlists, and should file an STR with the FIU.

2.2.2 Beneficial Owner Identification

Where the hawala provider customers is a legal person, please consult the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements* for details on the identification of beneficial owners.[11]

[11] Available at centralbank.ae/en/cbuae-amlcft.

2.2.3 Customer's Business and Business Relationship

For all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This element of CDD will have important implications for the customer risk rating. This is particularly true of the purpose of the account, which will likely be an essential determinant of risk for hawala provider customers. It is critical that LFIs have processes and controls in place to ensure that they are able to identify hawala customers. LFIs must ensure that they fully understand their customers' source of funds and the business in which they are engaged. In addition to interviewing the customer, requesting financial records, and reviewing invoices, LFIs should also search company databases and consider visiting the customer's business premises.

Underground hawala providers often try to evade detection by creating new companies and/or frequently switching to new financial institutions. In addition, even those that operate legally, may seek to misrepresent the purpose of the relationship in order to evade scrutiny and controls imposed by the LFI. It can be particularly difficult for an LFI to establish the bona fides and business activities of a newly established company, which is likely to not have any customers or inventory, especially when that company's line of business (e.g. import/export) is vague. LFIs should screen the names of new customer's beneficial owners, directors, and managers against its internal watchlists of customers previously exited by the LFI.

When a customer provides information indicating it is a hawala provider, LFIs must collect sufficient information during the CDD process to understand the full scope of the customer's business, including not only its provision of hawala services but also any other business activities in which the customer engages. LFIs should pay particular attention to the jurisdictions with which their hawala provider customers does business, and must understand whether their customer offers financial services to other hawala providers (e.g. participates in clearing networks or makes transfers on behalf of the customers of another provider who lacks a network in certain jurisdictions). Furthermore, LFIs must fully understand the intended use of the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. This may be many small cash deposits followed by large cross-border transfers or volume of activity that does not fit the customer's business. They must also understand whether the hawala provider may be using the LFI's accounts to conduct business and to move funds on behalf of customers while attempting to conceal this activity from the LFI. Section 2.3.1 contains red flags for concealed activity.

2.2.4 Ongoing Monitoring

All customers must be subject to ongoing monitoring throughout the business relationship to ensure that transactions are reasonable, and legitimate. Ongoing monitoring is particularly important in the context of business relationships with hawala providers, where the risks these relationships create for the LFI can change significantly based on the hawala provider's business activities. LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. LFIs should update CDD for all customers on a risk-based

schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

In addition to a review of the customer's CDD file, the LFI should also review the customer's transactions to determine whether they continue to fit the customer's profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established. This type of transaction review is distinct from the ongoing transaction monitoring discussed in 2.3.1 below. The purpose of the review is to complement ongoing transaction monitoring by identifying behaviours, trends, or patterns that are not necessarily subject to transaction monitoring rules. For example:

- Company M, a hawala provider, opens an account with Bank B, an LFI. At onboarding, Company M tells Bank B that it operates as a money transfer service to Country X. A year after the account is opened, Bank B conducts a scheduled CDD review and discovers that, six months after onboarding, Company M began to make and receive periodic transfers to and from Country Y. Bank B makes inquiries and discovers that Company M is now providing money transfer services to Country Y as well. Bank B decides to put a restriction on the account requiring prior authorization to make transfers beyond Country X and Country Y, requires Company M to sign a warrant that it will inform Bank B in advance of any future changes to its business model, and raises the customer risk-rating.

When customers are higher risk, including hawala provider customers, monitoring should be more frequent, intensive, and intrusive. LFIs should review the CDD files of higher risk customers on a frequent basis, such as twice a year. The methods LFIs use to review the account should also be more intense and should not rely solely on information supplied for the customer. For example, LFIs should consider:

- Reviewing all transactions on the account, rather than a sample of transactions;
- Conducting site visits at the customer's premises and requesting a meeting with the customer;
- Conducting searches of public databases, including news and government databases in order to independently identify material changes in a customer's ownership or business activities. Such searches should include adverse media searches of public records and databases, using relevant key words, including but not limited to, allegation, fraud, corruption, laundering.

2.3 Transaction Monitoring and STR Reporting

2.3.1 Transaction Monitoring

Where possible, transaction monitoring systems used to monitor activity in the accounts of the RHP should also be equipped to identify breaches of the permitted services by RHP listed in Part I section 4.1. The transaction monitoring system used by LFIs should also be equipped to identify RHP that are using the LFI's accounts to conduct their business and to move funds on behalf of customers while attempting to conceal this activity from the LFI. Red flags for concealed activity appear below. If an LFI's automated transaction monitoring system is not capable of alerting on these red flags, LFIs should have in place manual monitoring, such as management information systems that are capable of doing so. Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.

- Money being transferred at regular intervals to international locations known to be clearing houses for remittances.
- An account being used as a temporary repository with the funds quickly transferred.
- Usage of third-party accounts to disguise and to avoid detection by authorities.
- Wire transfers frequently sent by traders to foreign countries that do not seem to have any business connection to the destination countries.

- Business accounts used to receive or disburse large sums of money but show virtually no reasonable business-related activities such as payment of payrolls, invoices etc.
- Frequent deposits of third-party checks and money orders into business or personal accounts.
- Frequent international wire transfers from bank accounts that appear inconsistent with stated business activities.
- Sudden change in pattern of financial transactions from low value international fund transfers to large value transfers.

2.3.2 STR Reporting

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file an STR, or SAR or other report types with the FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. **STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system.** STR filings are essential to assist concerned UAE authorities, such as law enforcement, in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations:

- A potential customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current customer cannot provide required information about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the LFI should not establish the business relationship, or continue an existing business relationship; or
- If the LFI believes that a customer may be acting as an unregistered hawaladar.

Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.

2.4 Governance and Training

The specific preventive measures mentioned above must take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. The core of an effective risk-based program is an appropriately experienced AML/CFT compliance officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. As with all risks to which the LFI is exposed, the AML/CFT training program must ensure that employees are aware of the risks of hawala provider customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For example, an LFI that has a large number of hawala provider customers should offer training that includes an in-depth discussion of risk factors and red flags related to such customers.

Annex 1. Synopsis of the Guidance

PART I: REGISTERED HAWALA PROVIDERS AND LICENSED FINANCIAL INSTITUTIONS		
Introduction	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by the Registered Hawala Providers and other Licensed Financial Institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.

	Applicability	This Guidance applies to all natural and legal persons which are licensed and/or supervised by the CBUAE in the following categories: Registered Hawala Providers ("RHP"), National banks, branches of foreign banks, and Exchange houses.
	Legal Basis	This Guidance builds upon the provisions of UAE laws and regulations, including the AML-CFT Law, the AML-CFT Decision, the Cabinet Decision 74 of 2020 and the Registered Hawala Providers Regulation issued by the CBUAE ("Circular No. 24/2019").
Overview of Hawala activity	Hawala is an activity based on trust and was established to avoid high charges by people who cannot afford them, the ability to reach beneficiaries in remote places quickly where banks do not operate, and the existence of strict currency controls in some countries. While hawala providers, also known as hawaladars, often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement.	
Global risks of Hawala Activity	Hawaladars' business model is built around satisfying customers' needs to move money rapidly across borders, a service that may also be misused by criminals as it is to individuals seeking to conduct legitimate personal remittances. The risk of a hawala provider is influenced by the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide, and their customer base.	
Regulation in the UAE	The CBUAE permits legitimate Hawala Activity as an important element of its continuous efforts to support financial inclusion and bring the unbanked population into the regulated financial system. To this end, Hawala is regulated by the Registered Hawala Providers Regulation issued by the CBUAE. All providers **carrying on Hawala Activity in the UAE must hold a Hawala Provider Certificate issued by the CBUAE;** it is not permitted to carry on Hawala Activity without being registered with the CBUAE. Registered Hawala Providers (RHP) are only permitted to provide well-defined services that include non- commercial personal remittances and money transfer services to support commercial operations. RHP are not permitted to engage in any of the following transactions: Take deposits, exchange currencies or sell and purchase travellers' cheques; Provide any financial services other than money transfers (e.g. exchange of virtual assets/cryptocurrencies, loans, purchase of debts); or Execute transactions involving or on behalf of any other hawala provider in the UAE. This excludes the agents of the RHP in a foreign country.	
PART II: GUIDANCE FOR REGISTERED HAWALA PROVIDERS		
Sanctions Obligations	Targeted Financial Sanctions (TFS)are legal restrictions on financial activity imposed by the United Nations Security Council (UNSC) or the UAE. RHP are required to fully comply with the obligation to implement all necessary measures without delay as described in the Cabinet Decision 74 of 2020, the *"Guidance on TFS for FIs and Designated Non-Financial Business and Professions (DNFBPs)'* issued by the Executive Office of the Committee for Goods & Material Subject to Import and Export Control, the *CBUAE's Guidance for LFIs on the implementation of TFS*, the CBUAE Notice No. 3895/2021, and any of their amendments or updates thereof. RHP should be aware that it is a crime in the UAE to provide funds or financial services, including money transmissions services, to a person subject to TFS. Appropriate implementation of TFS has four key steps, which RHP must follow to ensure they are compliant: 1. Maintain awareness of UNSC and UAE sanctions lists, and rapidly becoming informed of changes to these lists. 2. Check the names of customers against the lists of sanctioned persons. 3. Immediately freeze any funds in the possession or under the control of the RHP that may belong to a listed person, and cancelling (where possible) any transactions involving a listed person.	

	4. Report any listed persons and the actions the RHP has taken to the appropriate authorities (via the goAML Portal).	
Registration and other Requirements	Registration	A resident natural person or legal person may not carry on Hawala Activity in the UAE unless the applicant holds a Hawala Provider Certificate issued by the CBUAE and is registered in the CBUAE Hawala Providers Register.
	CBUAE Notification of Approval/Rejection	The CBUAE may agree or decline an application for a Hawala Provider Certificate and will notify the applicant in writing of its decision.
	Re-Registration	RHP should submit to the CBUAE an application for renewal of the Hawala Provider Certificate within a period not less than two months from the date of expiry of the original certificate or any renewals thereof.
	Requirements for Trade License, Security and Reporting Systems	RHP are required to complete the following requirements within 90 days from the date mentioned in the final registration certificate as well as submit proof of completion to the Licensing Division of the CBUAE: ▪ Add Hawala Activity to the commercial trade license. ▪ Install security systems i.e. CCTV and police connections. ▪ Register o the UAE Financial Intelligence Unit's (FIU)goAML portal. ▪ Register to the CBUAE's Systems for the daily and quarterly reporting. ▪ RHP should register for the FIU's Integrated Enquiries Management System.
	Requirement for a Bank Account	RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with its details. In addition, they should inform their account manager at the bank of their intention to use the account to carry out Hawala Activity.
AML/CFT program	AML/CFT Program and Compliance Officer	RHP are required to establish and maintain effective AML/CFT compliance programs designed to prevent them from being misused to facilitate money laundering or terrorist financing. The program must be risk-based and appropriate to the risk of the RHP, taking into consideration its size, volume of transactions, types of remittances offered (personal only or personal and commercial), complexity, the nature and volume of its Hawala Activity, the nature of its customer base and the geographic areas in which it operates. Each RHP must have a specific person, the Compliance Officer, who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT program. This person must bean employee, manager, or owner of the RHP depending on the size of the RHP. They should also provide education and training to appropriate personnel and conduct a periodic audit of the AML/CFT program.
	Understanding Risks	The Compliance Officer should begin the risk assessment process by carefully reading and understanding Parts 1 and II of this Guidance, which contain essential information about the risks faced by an RHP and consider the customer, geographic, products and services, and delivery channel risks. RHP should complete this risk assessment process at least once a year. Where they assess themselves as higher risk, they should take additional precautions.
AML/CFT Program	Customer and Agent Due Diligence	Customer due diligence ("CDD") is the process by which an RHP identifies and understands its customer; it is required by law. The RHP must perform Customer Identification Diligence ("CID"), CDD or

		Enhanced Due Diligence ("EDD") prior to conducting each and every transaction, even if the customer is a repeat customer. An RHP must not conduct a transaction if the appropriate diligence has not been performed or completed depending on their nature as follows: ▪ CID: When natural persons sends or receives a transfer between AED 1-3, 499 and no higher risks are present. ▪ CDD: In all other cases between AED 3,500-54,999. ▪ EDD: When the customer is a natural person carrying out a transfer above ED 55,000, or when the customer is from/sending a remittance to a high-risk jurisdiction, or when the customer is a politically exposed person or a legal person, or when other higher risks are present. RHP may use agents in a foreign country to carry out activity on their behalf in that foreign country. RHP are not permitted to use agents to carry out activity on their behalf in the UAE (also known as *"nesting"*). RHP are required to perform appropriate due diligence on their agents and monitor their transactions to ensure that they are legitimate, keep up-to-date agent lists for a period of five years and provide them upon request to the CBUAE and/or to relevant authorities within the country in which they operate.
	Transaction Monitoring and Record Keeping	When an RHP's customer is originating a transaction, the RHP must collect and keep certain information for every transaction. When RHP's customer is receiving the remittance, they must in addition conduct CDD on the beneficiary and make sure that its customer's information matches that of the beneficiary identified in the information provided by the originating hawala provider. RHP must keep all records obtained through the CDD process and maintain records of all transactions for at least five years from the date of completion of the transaction or longer if directed by the CBUAE or any other authority.
Reporting Obligations	Daily Reporting	RHP must upload electronically to the CBUAE's reporting systems on a daily basis the data and details of all transfers, remitters and beneficiaries as per the forms prepared by the CBUAE for this purpose.
	Quarterly Settlement Statements	RHP must further submit to the CBUAE statements of their settlement accounts on a quarterly basis along with other required forms, as well as provide the CBUAE with any data, information, or statistics it may require.
	Reporting Suspicious Transactions to the FIU	If the RHP suspects that a transaction, attempted transaction, activity, or funds (including agents' transactions), constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime, they must submit a Suspicious Transaction Report (STR), Suspicious Activity Report (SAR) or other report types to the FIU using the goAML portal. RHP must submit this report without delay, meaning as soon as reasonably possible after the transaction takes place or their suspicions develop. Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* fox further information.
Penalties	Violation of any statutory obligations may be subject to supervisory action, administrative and financial sanctions and penalties as deemed appropriate by the CBUAE.	
PART III: GUIDANCE FOR LFIs		

Understanding Risks	Circular 24/2019 requires that RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with its details. **The CBUAE expects LFIs to accept RHP customers,** but LFIs must manage the risk that these transactions create through the use of appropriate controls. LFIs must not accept as customers unregistered hawala providers based in the UAE, and must immediately report an STR to the FIU, inform CBUAE when they are detected, and closely monitor the relationship.	
Mitigating Risks	Risk-Based Approach	LFIs should take a risk-based approach to the preventive measures they put in place for all customers, including hawala providers. The approach should include at the minimum the conduct of an enterprise risk assessment, identification and assessment of the risks associated with specific customers, and the application of EDD and other preventive measures.
	CDD and EDD	Customer Identification and verification: LFIs are required to identify and verify the identity of all customers. Among other requirements, LFIs must physically check the original hawala provider registration certificate issued by the CBUAE and keep a copy thereof. LFIs should not form business relationships or conduct transactions with hawala providers without a valid registration certificate issued by the CBUAE (unregistered hawala providers).
		Beneficial Owner Identification: Where the hawala provider customers is a legal person, please consult the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements* for details on the identification of beneficial owners.
		Customer's Business and Business Relationship: It is critical that LFIs have processes and controls in place to ensure that they are able to identify hawaladar customers. LFIs must ensure that they fully understand their customers' source of funds and the business in which they are engaged, the intended use and expected activity on the account, to the extent that they can generally predict and identify activity that does not fit the profile.
		Ongoing Monitoring: All customers must be subjectto ongoing monitoring throughout the business relationship to ensure that transactions are reasonable and legitimate. LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to- date. When customers are higher risk, including hawala provider customers, monitoring should be more frequent, intensive, and intrusive.
	Transaction Monitoring and Suspicious Transaction Reporting	Where possible, transaction monitoring systems used to monitor activity of the RHP should also be equipped to identify breaches of the permitted services by RHP. The transaction monitoring system used by LFIs should also be equipped to identify RHP that attempt to conceal activity from the LFI. LFIs must file a Suspicious Transaction Report, Suspicious Activity Report or other report types with the FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.
	Governance and Training	The specific preventive measures mentioned in this Guidance must take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. As

		with all risks to which the LFI is exposed, a training program must ensure that employees are aware of the risks of hawala provider customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls.

Guidance for Licensed Financial Institutions on the Risks Relating to Payments

Effective from 1/8/2022 **Status:** In-Force

1. Introduction

1.1. Purpose of the Guidance

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance [2] issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at centralbank.ae/en/cbuae-amlcft.

[2] FATF: *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services, 2013,* fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, and *Correspondent Banking Services, 2016*, fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies; and
- Stored value facilities, retail payment service providers, and card schemes.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws:

- Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended by Decree Federal Law No. (26) of 2021 ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended by Cabinet Decision No. (24) of 2022 ("AML-CFT Decision").
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74").

1.4. Acronyms and Definitions

Card Scheme: a single set of rules, practices and standards that enable a holder of a payment instrument to effect the execution of card-based payment transactions within the UAE which is separated from any infrastructure of payment system that supports its operation, and includes the card scheme governing body. For the avoidance of doubt, a card scheme may be operated by a private or public sector entity.

Correspondent Banking Relationship: the relationship between a correspondent financial institution and a respondent one through a current account or any other type of account(s) or through a service related to such an account and includes a corresponding relationship established for the purpose of securities transactions or transfer of funds.

Nesting: defined by the FATF as the use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

New Payment Products and Services (NPPS): defined by the FATF as new and innovative payment products and services that offer an alternative to traditional financial services.

Payment Sector: refers to different forms of payment that are transmitted and exchanged across various delivery channels, frequently utilizing digital platforms, systems, services and products.

PPS: Payment Products and Services.

Retail Payment Services: any of the following services: payment account issuance; payment instrument issuance; merchant acquiring; payment aggregation; domestic fund transfer; cross-border fund transfer; payment token; payment initiation; and payment account information.

Stored Value Facility (SVF): a facility (other than cash) for or in relation to which a customer, or another person on the customer's behalf, pays a sum of money (including money's worth such as values, reward points, crypto-assets or virtual assets) to the issuer, whether directly or indirectly, in exchange for: (a) the storage of the value of that money (including money's worth such as values, reward points, crypto-assets or virtual assets) whether in whole or in part, on the facility; and (b) the relevant undertaking. SVF includes device based SVF and non-device based SVF.

2. Understanding Risks

There is no uniform global approach to regulation of the Payment Sector and participants may be classified as different types of entities in different regulatory regimes. Some types of participants may be regulated as financial institutions in some jurisdictions but not in others. Operating within a global financial center, LFIs in the UAE may be exposed not just to participants licensed by the CBUAE, but also to those operating globally. This exposure can be direct (i.e., providing financial services directly to a participant), or indirect (e.g., when a customer initiates a withdrawal from his checking account using a foreign smartphone-based app that he has linked to that account).

The Payment Sector is becoming increasingly diverse, and payment processes more complex. The Payment Sector is no longer solely dominated by traditional financial institutions like banks and exchange houses, which also offer new and innovative methods using the internet or mobile phone technology. A variety of new types of Payment Sector participants, such as companies that offer internet-or smartphone-based payment applications and providers of prepaid cards and devices, are involved in a growing percentage of all payment transactions. These entities allow almost anyone to accept and originate payments using a wide variety of techniques and payment routes. Whenever a customer makes a purchase or pays a bill online, these new participants are likely to be involved. These entities may also be used outside commercial contexts, such as by crowdfunding platforms or charitable organizations.

Furthermore, as innovative technologies emerge and commerce and economic activity increasingly grows online, merchants and consumers are relying on a diverse array of New Payment Products and Services (NPPS). The FATF defines NPPS as "*new and innovative payment products and services that offer an alternative to traditional financial services*." Examples of NPPS include prepaid cards, mobile payments, and internet-based payment services; these are neither exhaustive, nor exclusive as a provider of mobile money, for instance, may utilize prepaid cards or provide internet-based payment services. In contrast, payment methods such as credit cards and cheques, and bulk funds transfer systems such as national payment systems, would generally not qualify as NPPS. Because NPPS are so diverse, they do not share a single risk profile and pose money laundering and financing of terrorism (ML/FT) risks for financial institutions when they do not understand the operation or the vulnerabilities in the NPSS operational models. The provision of these NPPS is frequently implemented or facilitated by a group or network of different companies, some of them invisible to the consumer or even all the participants in the network, given the presence of multiple participants in the chain with whom not all participants will have a contractual relationship.

The vast majority of payment transactions carried out each year across the globe are legitimate. But the Payment Sector—and NPPS in particular—has characteristics that make it both attractive and vulnerable to illicit actors. As LFIs are increasingly exposed to new participants in this sector, they must remain alert to and understand the risks this exposure creates.

Section 2.1 below discusses the ML/FT risks of the Payment Sector with a focus on risks related to NPPS. It applies to financial institutions that are directly involved in the provision of such products and services, which includes both traditional LFIs and those that are solely engaged in providing payments. Section 2.2 discusses risks specific to LFIs that provide services to other Payment Sector participants.

2.1. ML/FT Risks of the Payment Sector

2.1.1. Characteristics of the Movement of Funds

PPS, and NPPS in particular, are extremely attractive to illicit actors because of the rapid movement of funds between Payment Sector participants and across borders. The risks of a specific payment network or application however can vary based on the features that make it more or less attractive to illicit actors, such as:

- **Transaction speed.** Are transactions instantaneous, or do they take hours or days? The quicker the transaction, the easier it is for illicit actors to conduct multiple transfers, further obscuring the origin of the

funds, before coming to the attention of the authorities.

- **Transaction limits**. Does the PPS have transaction caps or limits? Smaller-value payments are not without risk, especially in the terrorist financing context, but they do make it more difficult to move illicit funds on a large scale.

- **Closed vs open loop system**. PPS, primarily SVF, can be "closed" or "open" loop. In a closed loop system, the payment method can only be used for payments to a specific payee. Examples include transit passes and store gift cards. In an open loop system, the payment method can be used to pay a wide variety of payees, and can be linked to other payment methods that further expand its reach. Although it is certainly possible to use closed loop systems for ML/FT (for instance, if a terrorist group collects store gift cards and uses them to purchase equipment), the restrictions on their use makes them less attractive to illicit actors.

- **Methods of funding and access to cash**.[3] The methods by which a PPS can be funded (such as by cash, through another payment service, a prepaid model, or by third-party funding from anonymous sources) may increase risk. The inputs and outputs of a given PPS are therefore an important consideration when assessing risk, including whether the funding source is located internationally such as a high-risk country. For example, illicit actors may seek to place cash in the financial system or to obscure transaction trails by converting funds in and out of cash. PPS that permit users to fund their accounts with cash, or that allow users to withdraw cash, may be higher risk. In addition, as discussed above in the context of open loop systems, the more open and porous the PPS, the higher the risk it may present. PPS that allow users to fund accounts from multiple sources, and to withdraw funds using multiple methods, are likely to be more attractive to illicit actors, and will be harder to effectively monitor.

- **Payment transparency**. NPPS often have aggregated payments and settlement accounts involving multiple parties and long payment chains thereby potentially causing LFIs to have reduced visibility into payment activity taking place through the PPS as well as obscuring an LFI's ability to identify the ultimate payer and payee for all transactions.

- **Ability for one person to create multiple accounts.** Some PPS allow customers to create multiple accounts using the same ID. These may be individual accounts or created on behalf of minors or other family members. Illicit actors may seek to rapidly cycle funds through accounts (whether or not these take the form of virtual 'wallets' or other SVF) in order to obscure payment trails. They may also seek to open multiple accounts to facilitate fraud and other criminal activity. Restricting a customer to one account does not eliminate risk, since illicit actors often work in groups, but it makes it more difficult for a single person to launder funds by conducting a self-transfer.

- **Non-face-to-face relationships**. Does the payment method allow for a non-face-to-face business relationship? What are the payment method's characteristics? Can the relationship be established through agents, online or through a mobile payment system? The absence of contact and/or anonymity may increase the risk of identity fraud or customers providing inaccurate information.

- **Use of virtual assets.**[4] As interest in virtual assets grows, more and more payment methods and schemes are integrating with virtual assets. For example, a global payments firm allow users in some countries to purchase virtual assets using the funds in their account, although not to use them directly for payments. Payment methods and schemes that integrate virtual assets could expose financial institutions to the specific risks of this sector.

---

[3] For details on the vulnerabilities of cash and alternatives to cash, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to Cash-Intensive Businesses*

[4] Please note that the risks relating to Virtual Assets/Virtual Assets Service Providers are out of the scope of this guidance and addressed in a separate guidance to be issued by the CBUAE.

2.1.2. Peer-to-Peer Payments

NPPS have revolutionized the ability to make payments or transfer funds. Where cash transactions previously required face-to-face interaction and bank transfers involved transactions' fees and an execution time in the past, NPPS allow participants to send money that will be instantly available to the beneficiary, reducing the need for trust in the relationship. As a result, the availability of convenient, inexpensive PPS has led to a decreasing use of cash, particularly in highly developed countries. **Bringing transactions into the formal financial system has many advantages from the perspective of combating illicit finance.** These transactions can flow through third parties that are in many cases subject to AML/CFT requirements. In most cases, the payments that involve such third parties include information on the payer and the payee and are permanently recorded by a financial institution, making it easier for law enforcement to track transactions. But the use of PPS for peer-to-peer payments also creates risk for financial institutions because it means that many smaller illicit transactions that once took place in cash are now being conducted via PPS, particularly NPPS.

2.1.3. Cross-Border Movement

One of the principal features of many NPPS is that they can be used globally for making payments or transferring funds. While the usefulness of cash and cheques is limited outside the jurisdiction where they were issued, many PPS are internet-based services and specialize in conducting transfers between countries and currencies. For example, a UAE bank that offers checking accounts to UAE residents may have no ATMs or branches outside the UAE. But, if users link their accounts to global or regional payment apps, they can conduct transactions with persons over the world and can use their smartphone as a payment instrument in countries where the bank has no presence, thus introducing new geographical exposure potentially to high-risk countries. And **unlike cross-border wires, which carry full identifying information,** the bank will frequently only see the customer's transactions with the payment network itself, rather than their location or ultimate destination. Many illicit finance schemes involve the cross-border movement of funds. Criminals may seek to finance terrorism in other countries, move funds out of sanctioned jurisdictions, or evade the attention of law enforcement in the jurisdiction where a proceeds-generating offense was committed. PPS that allow or facilitate cross-border movement of funds may therefore be particularly attractive to illicit actors.

2.1.4. Global Regulatory Gaps

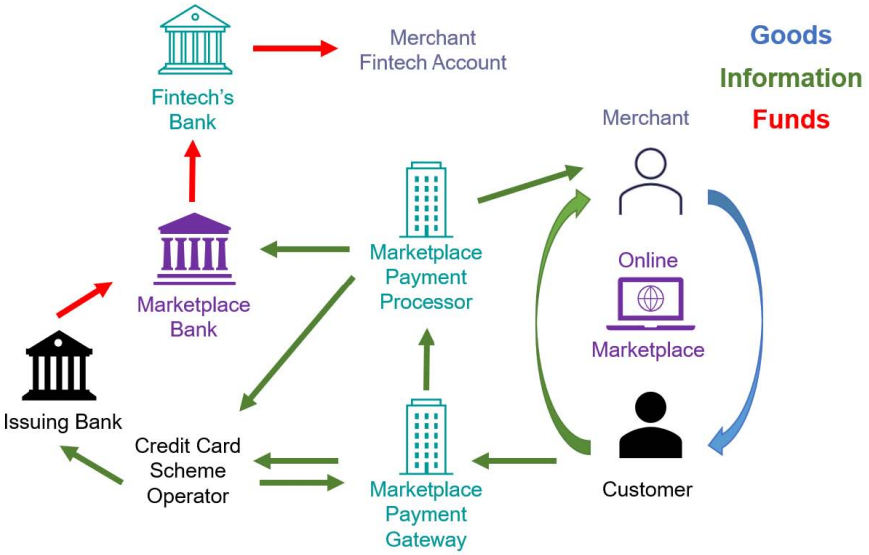
Countries take a variety of approaches to regulating the Payment Sector and there is no one widely accepted classification of participants. As a result, two regulators in two different jurisdictions may subject a single company to very different requirements based on each jurisdiction's regulatory framework. The company may be regulated as a financial institution in one jurisdiction, and thus subject to AML/CFT requirements, but treated as a tech company in another with no requirement to apply preventive measures. Companies may provide services to customers in a given country without being regulated in that country at all. Even where Payment Sector participants are fully regulated and subject to stringent AML/CFT requirements, supervisors' expectations for this sector may be lower than for traditional financial institutions such as banks. And participants, as relatively new market entrants, may lack the experience, expertise, or commitment to apply fully effective preventive measures. These entities may be less able to protect themselves and their partners, and thus vulnerable to abuse by illicit actors.

2.1.5. Intermediation

The Payment Sector may be complex with a number of participants potentially involved in a single transaction. As a result, many payment transactions will be highly intermediated, with multiple financial institutions involved in a funds transfer. Additional entities (some of which may not be financial institutions) can potentially facilitate the transaction through the exchange of information. Intermediated transactions create risk because no regulated entity

participating in the transaction has the visibility necessary to fully understand the transaction and the participants. Illicit transactions may have red flags when viewed as a whole, but may appear legitimate when seen from the perspective of each of the financial institutions involved. This creates a vulnerability that illicit actors can exploit.

For example, consider the hypothetical transaction below, a purchase on an online marketplace that allows individual sellers to sell items directly to customers:



In this transaction, the customer is using a credit card to purchase goods from the merchant, but the merchant is not a participant in the credit card scheme. A number of Payment Sector participants help to bridge this gap and facilitate the transaction:

- The marketplace uses a payment gateway that accepts the customer's credit card credentials, encrypts them, and validates them against data held by the credit card scheme operator. The marketplace may also integrate with providers that provide 'one-click' payment information to the payment gateway without requiring the customer to enter his or her credit card details. In the UAE, these providers would be classified as conducting payment account information services, but in many other jurisdictions they are not regulated as financial institutions.

- The credit card scheme operator validates the customer information provided by the payment gateway, conducts initial fraud checks, and informs the payment gateway that the credit account is in good standing and the credit limit has not been exceeded.

- The payment gateway informs the marketplace's payment processor that a transaction of an identified value can proceed using the customer's credit card details.

- The marketplace payment processor informs the merchant that the transaction has been confirmed and instructs the credit card scheme operator to debit the customer's account for the purchase price, in favor of the marketplace.

- The credit card scheme operator passes this payment instruction on to the bank that issued the customer's credit card (the issuing bank). Meanwhile, the merchant ships the customer the merchandise purchased.

- The issuing bank transfers funds in the purchase value to the marketplace's bank (this transfer may in fact go through the marketplace payment processor's account at the same bank).

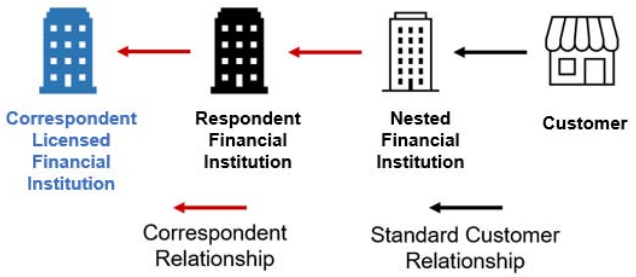
- The marketplace bank transfers the purchase funds to the merchant's fintech (likely a provider of SVF), which in turn transfers the funds to the merchant's account. The marketplace's payment processor likely

facilitates this transaction by instructing the bank where to send the funds.

It is unlikely that any of the Payment Sector participants in this transaction have full visibility into the funds transfer chain. The banks are unlikely to have information on anyone other than their immediate customers or correspondents. The payment gateway likely does not identify the merchant. The fintech likely does not identify the customer. The marketplace payment processor is likely aware that the customer and merchant are engaging in a transaction, but may not know where the customer's funds are coming from or where the merchant's funds are going. And because the marketplace payment processor does not hold funds at any point in the transaction, it may not be regulated as a financial institution in all jurisdictions. In this instance, a marketplace payment processor may apply certain conditions on what types of customers and merchants it engages. For more information on how LFIs can mitigate and manage ML/FT risks related to this sector, including the risks arising from the use of NPPS, please see section 3 "Mitigating Risks."

2.1.6. Nesting

Nesting is a form of intermediation that presents specific risks. In most Correspondent Banking Relationships that involve nesting, the respondent financial institution is not aware of individual transactions ordered by the ultimate customer; instead, the respondent sees bulk activity in the correspondent's account that represents aggregate customer orders and perhaps also proprietary transactions by the correspondent. As a result, the transaction is intermediated because the respondent cannot see—nor assess the risk of— the original customer.



Although nesting can occur in the context of any financial service, some features of the Payment Sector— the long payment chains and the involvement of multiple parties—can increase the likelihood that nesting will take place. In particular, some Payment Sector participants specialize in providing financial services to dubious merchants or customers who would be rejected by larger financial institutions. A participant servicing these customers, frequently offering merchant acquiring or payment aggregation services, will establish a nested relationship with a third participant that in turn has a Correspondent Banking Relationship with a bank. Although all the parties involved must and may claim to perform appropriate merchant due diligence, in practice, the risk may be that the bank is relying on its correspondent, which is in turn relying on the nested financial institution, with the first two parties not having full visibility into the nested financial institution's customer base or due diligence practices.

2.1.7. Use of Agents and Affiliates

Payment Sector participants often interact in a dense web of agency and affiliate relationships, with each participant playing a defined role. A large number of entities involved in the NPPS, in particular when involving several countries, may increase the ML/FT risk.

For example, entities involved in the provision of SVF through a prepaid card scheme could include:[5]

- The issuer of the SVF, such as the issuer of prepaid cards, who is accountable to the customer for holding the funds they have loaded into the SVF (issuers are often banks that maintain program funds in a single program account);
- The merchant acquirer (or acquirers), who establishes a direct relationship with merchants, distributes and maintains the payment gateway, collect funds on their behalf, and distributes them to merchants;

- The program manager, who operates the network and provides services to the issuer (because all program funds are generally maintained in a single account, program managers often maintain the electronic records that track the "movement" of funds into and out of customer's individual wallets);
- The retailer, who sells SVF devices like prepaid cards to customers;
- The network operator, who maintains the link between merchants' point of sale devices, or other payment gateways, and the program manager; and
- Persons, who act as agents for the scheme, such as by accepting cash in exchange for topping up wallet balance.

Another example includes the provision of mobile payment services. The roles of Payment Sector participants depend largely on the business model of the mobile payment service. Furthermore, various roles may be carried out by a single entity or through agents. Entities involved in the provision of mobile payments may include the following:

- The network operator, who provides the platform to allow access to the funds through a mobile phone.
- The distributor (including retailer), who sells or arranges for the issuance of funds on behalf of the issuer to customers.
- The issuer of the SVF, or the electronic money issuer, who issues electronic money, which is defined here as a record of funds or value available to a customer stored on a payment device, such as a prepaid card or mobile phone.

This interplay between different entities can lead to risks resulting from intermediation as discussed above. But it can also give rise to risks when the participating entities have not assigned clear responsibility for compliance with AML/CFT requirements. The PPS risk's exposure may then be dependent on multiple actors who may have a deficient understanding of AML/CFT obligations. For example, in the prepaid card scheme described above agents could facilitate money laundering by accepting large volumes of cash and breaking the value of the deposit up across several wallets, thus avoiding scrutiny related to large cash deposits. The entities acting as merchant acquirers could be aware that the merchants are providing illegal goods or services or are fraudulent, but conceal this knowledge in order to continue to receive fees related to transactions involving the merchants in its network.

The risks created by the use of agents and affiliates increase when agents and affiliates are responsible for sensitive steps in the system (customer or merchant onboarding, or cash acceptance) and when there are multiple agents or affiliates between the customer and the ultimate provider of payment services. For example in card schemes, merchant acquirers will frequently work with contractors who identify merchants and bring them to the acquirer in return for a fee. Depending on the relationships involved, the financial institution that maintains the merchant accounts may not have any actual direct contact with and have a limited visibility of the merchant, as the relationship is intermediated through the merchant acquirer and also the merchant acquirer's contractor. Since contractors do not get paid unless the financial institution accepts the merchant as a customer, they may be incentivized to help the merchant conceal the true nature of its business.

---

[5] Please note that one entity can hold various roles related to the provision of SVF (e.g., an issuer of the SVF can also be a program manager). The risk is extended where different agents are involved in the provisioning of a prepaid card.

2.1.8. Merchant Risks

All merchants accept payments in one form or another, and most merchants today are at least considering integrating NPPS into their financial arrangements. On the other end of the spectrum, NPPS lower the barriers for merchants to access financial services, making it easier to start and operate a small business, particularly in the e-commerce sector. These lower barriers to entry however can also create risks when merchants are not properly vetted. Globally, Payment Sector participants including providers of NPPS have been abused by or directly complicit with merchants who offer fraudulent or illegal goods or services, or whose business models pose reputational risks to financial institutions. These can for example include traffickers in narcotics who disguise their transactions as

financial activity related to a supposedly legitimate small business. They can also include businesses that are legal in some jurisdictions but not others (such as gambling websites) and seek to accept payments from customers resident in jurisdictions where the business is illegal. Finally, they may include sites that are legal in many jurisdictions but that pose reputational risk, and that are therefore outside a financial institution's risk appetite, or online marketplaces that do not thoroughly police their merchants and thus could themselves be abused by illicit actors.

Any factors—particularly intermediation, nesting, and the use of agents and affiliates—that prevent a financial institution from understanding exactly what merchants or what types of merchants it is serving when it provides a PPS, increase the risks. Risks may be higher in cross-border networks, as businesses may be legal in some jurisdictions and illegal in others, while customers can use the PPS to purchase services that would be illegal in their jurisdiction. Relying on third parties to conduct customer due diligence (CDD) on merchants can also increase risk if the relationship is not well-governed.

2.2. ML/FT Risks for LFIs Providing Services to Payment Sector Participants

Many traditional LFIs, including banks, are full participants in the Payment Sector. Banks serve for example as issuers and acquirers in credit, debit, and prepaid card schemes, and are actively involved in developing new payment methods to better serve their customers. When banks play such roles, they are directly exposed to the determinants of risk discussed in section 2.1 above, and should thus conduct appropriate CDD on all Payment Sector participants. Banks and any other LFIs that offer services to other Payment Sector participants, or have customers who use these services, are exposed to specific forms of risk that include:

2.2.1. Correspondent and Correspondent-Type Risk

Because large-scale national clearing and settlement systems are often opened only to banks and other depository institutions, the majority of retail payments will ultimately pass through a bank generally as part of batch settlement. In order to facilitate this activity, non-bank financial institutions involved in payments, as well as unregulated Payment Sector participants, generally maintain deposit accounts with banks. These accounts can be used to safeguard customer funds (for example funds that have been deposited with a prepaid scheme) or to aggregate customer funds before disbursing them directly to customer's account (for example when a merchant acquirer aggregates multiple payments to a merchant partner before disbursing them in a single transfer). Correspondent Banking Relationships in which the correspondent's customers' funds flow through an account held at the respondent financial institution are particularly high risk, because they expose the respondent institution directly to any potentially illicit activity in which the correspondent's customers are engaged. Because banks that offer services to correspondents have limited information on these transactions, they are reliant on the correspondent to implement an effective AML/CFT program. Please see section 3.4.2 for the respective preventive measures.

2.2.2. Other Risks Related to Intermediation

Even banks that view themselves as having limited to no exposure to NPPS may in fact have indirect exposure through customers who link their bank accounts to payment apps, or use their bank accounts to fund SVF accounts or wallets (or withdraw funds received in such wallets to their accounts), or withdraw funds as cash and use it to purchase other prepaid instruments. Account activity of this type poses unique challenges for account and customer surveillance, because frequently the bank will be aware only of the immediate source or destination for the transaction, rather than the entire transaction chain. This can allow customers to deliberately thwart transaction monitoring programs and prevent the bank from understanding and assessing the activity on the customer's account to determine whether it is in fact in line with the customer profile. Examples of how intermediation can limit a bank's ability to identify suspicious or unusual behavior include:

- Many banks have automated transaction rules designed to identify possible unlicensed money transfer activity by alerting on accounts that receive multiple small deposits from different sources, followed by a

single large cross-border transaction. A customer could thwart this surveillance by having associates deposit the funds to be transferred in an SVF wallet, and then moving those funds to a linked bank account in order to execute the cross-border transfer. From the bank's perspective, it would appear that the customer received only one deposit. Relatedly, the provider of SVF could not know that the funds were ultimately transferred across borders.

- Many banks use watchlists to identify transactions that may be illegal or in violation of bank policy, such as the use of gambling websites. A customer seeking to evade these restrictions could use a foreign payment app linked to their account to purchase the assets; this transfer would likely appear on the bank's records as a debit in favor of the operator of the payment app. The operator, in turn, may not be responsible for enforcing the laws of the jurisdictions where its foreign customers are based. It is therefore important for banks to identify foreign payment apps in order to appropriately assess the risks of the transactional activity.
- A customer that generates a high quantity of illicit proceeds in cash can evade surveillance the bank applies to cash deposits by depositing the cash with a provider of NPPS (including both SVF and any other payment app that accepts cash inputs) and then withdrawing the funds from the payment service to his/her linked bank account.

2.2.3. Risks Related to Outsourcing

Banks often serve as the backbones of PPS such as credit, debit, and prepaid schemes without serving as the administrator or governing body of the scheme. In these situations, banks provide their reputation, stability, ability to hold deposits, and access to national payment systems while program administrators actually manage the movement of funds throughout the scheme. Because program operators have more direct contact with customers and more insights into the movement of funds, banks involved in these schemes often outsource CDD and other elements of the AML/CFT program to the program operators. But **as banks continue to be exposed to funds involved in the program, they remain responsible for implementing an effective and compliant AML/CFT program, even if transactions flow through third parties** that may or may not be subject to AML/CFT requirements. LFIs should therefore adopt policies to mitigate risks arising from reliance on outside service providers, including ones that operate in high-risk countries. Where roles and responsibilities are not clearly assigned, or where the program administrator does not implement an effective program, illicit actors can exploit the cracks in the program, and the bank and the program operator together will likely be less effective than if either party were operating alone. In such cases, LFIs should maintain a contingency arrangement as necessary.

3. Mitigating Risks

LFIs, whether they are primarily Payment Sector participants or have more limited exposure, are expected to take a risk-based approach to mitigating and managing ML/FT risks related to this sector, including the risks arising from the use of NPPS. A risk-based approach means that risk mitigation should begin with, and be based on, an appropriate assessment of the LFI's payments-related risks. This assessment should in turn be reflected in the design and operation of the LFI's AML/CFT program, including but not limited to the particular program elements discussed below, so that the LFI devotes greater resources and attention where risks are higher.

The sections below discuss how LFIs can apply specific preventive measures to mitigate and manage their payments-related risk. Sections 3.1-2 and 3.5-7 apply to all LFIs. Section 3.3 describes preventive measures recommended for LFIs that provide PPS directly to customers (including both consumers and merchants, or payers and payees), and section 3.4 for LFIs that provide services to other Payment Sector participants. The controls discussed should be integrated into the LFI's larger AML/CFT compliance program and supported with appropriate governance and training. It is not an exhaustive discussion of all AML/CFT requirements and LFIs should continuously consult the UAE legal and regulatory framework currently in force.

3.1. AML/CFT Obligations under CBUAE Regulations

The CBUAE regulatory framework clearly state expectations for compliance with AML/CFT obligations. In addition to this guidance, LFIs including non-bank payment service providers should carefully review all the relevant regulations issued by the CBUAE, which provide a comprehensive coverage of all payment products, services, and systems that are issued, provided and/or operated in the UAE, to ensure they fully understand and comply with their obligations.

3.1.1. Providers of Stored Value Facilities

In November 2020 the CBUAE issued the *Stored Value Facilities (SVF) Regulation* (Circular No. 6/2020 issued by Notice 4834/2020). Under its Article 14, all licensees must comply with the existing legal obligations and regulatory requirements for AML/CFT of the CBUAE and address ML/FT risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, detect ML/FT activities, and report any suspicious transactions to the UAE Financial intelligence Unit (UAE FIU). Among their detailed regulatory obligations, the licensees must assess the risk level of business relationships and undertake periodic risk profiling and assessment of products based on the AML/CFT requirements.

3.1.2. Retail Payment Services and Card Schemes Regulation

In July 2021 the CBUAE issued the *Retail Payment Services and Card Schemes Regulation* (Circular No. 15/2021 issued by Notice 3603/2021). Under its Article 12, payment service providers must comply with the relevant UAE AML/CFT laws and regulations and address ML/FT risks through appropriate preventive measures to deter abuse of the sector as a conduit for illicit funds, detect ML/FT activities, and report any suspicious transactions to the UAE FIU. Among their detailed regulatory obligations, the licensees must conduct business relationship-specific risk assessments and undertake periodic risk profiling and assessment of retail payment service users based on AML/CFT requirements. In addition, under Article 18.14, card schemes must report transactions to the UAE FIU when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

3.1.3. Large Value and Retail Payment Systems Regulations

In March 2021 the CBUAE issued the *Large Value Payment Systems Regulation* (Circular No 9/2020 issued by Notice 1410/2021) which covers clearing and settlement systems designated primarily to process large-value and/or wholesale payments typically among financial market participants or involving money market, foreign exchange or many commercial transactions. In tandem, the CBUAE issued the *Retail Payment Systems Regulation* (Circular No. 10/2020 issued by Notice 1408/2021) which covers fund transfer systems and related instruments, mechanisms, and arrangements that typically handle a large volume of relatively low-value payments in such forms as cheques, credit transfers, direct debit, card payment transactions or a regulated medium of exchange. Among their detailed regulatory obligations, all licensees are required to comply with any instructions issued by the CBUAE and any relevant international standards.

3.2. Risk Assessment

Under Article 4 of the AML-CFT Decision, LFIs are required to identify, assess, and understand the ML/FT risks to which they are exposed and how they may be affected by those risks, in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. In addition, under Article 23 of the Decision, LFIs are required to identify and assess the ML/FT risks of that may arise when developing new products and new professional practices, including means of providing new services and using new or under-development techniques for both new and existing products. **An appropriate risk assessment should consider all the PPS that an LFI provides, and the LFI's direct relationships to Payment Sector participants, both domestic and foreign.**

When assessing its direct exposure to the Payment Sector, whether in the form of PPS it offers, or relationships it maintains with other participants, the LFI should consider the risk factors discussed in section 2 above. The risk assessment should take into consideration:

- **Movement of Funds.** What are the financial flows through the PPS and through the LFI's accounts? What is the speed of transactions? Is there a cap on transaction value? Is there a daily, weekly, or monthly cap on the volume of transactions? Is the payment service in question closed loop or open loop? Can single users open multiple accounts?

- **Mode of Funding:** How do users fund their accounts and make withdrawals, and is funding permitted prior to customer verification?

- **Peer-to-Peer Payments.** Does the PPS allow users to conduct peer-to-peer transfers, or can they only send transfers to merchants/from customers? How is this restriction implemented and enforced?

- **Cross-Border Movement.** Does the PPS permit funds to move across borders and to high-risk countries through relationships with foreign financial institutions? Can users access the PPS when they are outside the UAE? Does the service support multiple currencies?

- **Regulatory Status.** Is the PPS that the LFI provides a regulated activity in the UAE and in all jurisdictions where it is provided?

- **Use of Agents and Affiliates**. How many entities are involved in delivering the PPS? How open is the network supporting the PPS? Does it include entities that are not regulated as LFIs—for example convenience stores that accept cash in return for topping up account balance? What is the role of each player in the system, and are responsibilities clearly defined in governance documents?

- **Intermediation.** How much visibility does the LFI have into payment activity taking place through the PPS? Can the LFI identify the ultimate payer and payee for all transactions? How many entities are in the payment chain?

- **Controls.** Does the PPS integrate appropriate features that contribute to managing the risk created by the factors listed above, such as by performing a robust customer verification process? These can include both the AML/CFT-specific features discussed in section 3.3 below and measures related to cybersecurity and counter-fraud.

Where LFIs, particularly banks, provide services such as deposit accounts to Payment Sector participants, they should also consider the following in assessing the risk of the relationship:

- **Nature of the Relationship:** What products or services does the LFI provide to the participant? Does the relationship involve direct exposure to the funds of the participant's customers? Is the sector participant using the relationship to facilitate activity by other Payment Sector participants?

- **Regulatory Status:** Is the participant required to be licensed in the UAE, its home jurisdiction, and all jurisdictions where it operates? Is it subject to AML/CFT requirements in all jurisdictions that are at least as stringent as those imposed in the UAE?

- **Relationship Governance:** Are AML/CFT responsibilities within the relationship clearly defined? Does the LFI outsource some aspects of AML/CFT program implementation to the Payment Sector participant?

The risk assessment should also consider the LFI's indirect exposure to the Payment Sector through its customers, who may connect their account with an LFI to a variety of PPS, or may fund their account by using such PPS. Because many payment service providers use existing domestic or international payment systems to execute transfers on behalf of their customers, an LFI may not be aware that its customers are using such services nor able to prohibit their use or detect payments activity in customer's accounts. LFIs should therefore consider a variety of tools to assess their indirect exposure to this sector. These may include:

- applying appropriate level of due diligence and asking questions during the CDD process to obtain all relevant information;

- administering customer surveys to better understand customer's interest in and use of payment services; and

- utilizing watchlist-based screening over a sample period.

When LFIs have a sense of the most common PPS their customers use, they should assess the risk these services and products pose, considering the factors discussed above, including the involvement of high-risk countries and the extent of exposure. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the LFI's controls risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed.

3.3. Preventive Measures for LFIs Providing Products and Services Directly to Customers

Under Article 4(2) of the AML-CFT Decision, all LFIs must implement an AML/CFT program designed to manage the risks identified in their risk assessment that should include:

3.3.1. Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring

Under Article 5 of the AML-CFT Decision, LFIs should conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. Payment Sector participants, including providers of SVF, retail payment services, and card schemes, generally establish relationships with their customers rather than treat all customers as occasional or walk-in customers. In these scenarios, **LFIs must perform, no matter the customer type, all the elements of CDD required under sections 2 and 3 of the AML-CFT Decision**, which include customer identification and verification, beneficial owner identification, understanding of the nature of the customer's business and purpose of the business relationship, and ongoing monitoring. CDD, and where necessary enhanced due diligence (EDD), are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers.

In addition to these mandatory elements, LFIs should consider the following additional elements of CDD that are particularly important in the context of NPPS:

- **User identification and verification.** Many, if not most, NPPS involve the use of digital as opposed to face-to-face methods of onboarding and identifying customers (a.k.a. "electronic Know Your Customer," or "e-KYC"). Digital delivery of services is increasingly common, but can present higher risks when LFIs do not take appropriate steps to ensure that they fully understand the customer and that the person using the services is in fact the identified customer. In particular, when verifying the Emirates ID card (either physically or by way of digital or e-KYC solutions) LFIs must use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE-Pass Application, or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than the Emirates ID are used in the KYC process, a copy must be physically obtained from the original passport which must be certified (i.e. certified copy) as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.

- **Use of IP addresses and geographical (spatial and temporal) locators**. As discussed above, payment services that are internet-based or accessible through smartphones can allow customers to access financial services no matter where they are in the world. LFIs are of course free to allow their customers to access their services while outside the UAE, but should take advantage of geographical location tools at

both the onboarding and the ongoing monitoring stages to ensure that they understand the geographic risk they might be exposed to by their customers. This can include:

  - Requiring additional authentication or verification when a customer accesses the service from an IP address or device different from the one used at onboarding, or from a different country and/or time zone than the customer's stated country of residence.

  - Reviewing the customer's log-in locations during CDD refresh to identify any suspicious log-in or movement patterns (for example, high numbers of transactions taking place when the customer is near a border with a high-risk country where the PPS is blocked).

- **SVF due diligence**: Risk mitigating measures should include as per Article 14.4 of the SVF Regulation: (a) the application of limits on the maximum storage values, cumulative turnover or transaction amounts; (b) disallowing higher risk funding sources; (c) restricting the SVF product being used for higher risk activities; (d) restricting higher risk functions such as cash access; and (e) implementing measures to detect multiple SVF accounts/cards held by the same Customer or group of Customers.

- **Merchant due diligence.** Payment Sector participants that deal directly with merchants (whether as providers of SVF or card schemes, or conducting merchant acquisition or payment aggregation) may have two main classes of customers: consumers and merchants. It is important to remember that merchants who use the service are customers of the LFI and that merchants that may engage in deceptive or fraudulent business practices or use their legitimate business as a cover for criminal activities, can expose the LFI to extremely high ML/FT risk. Merchants should therefore be subject to CDD designed to understand the nature of their business and the expected transaction volumes. LFIs should understand the merchant's current financial and payments operations and in particular ascertain why the merchant is seeking a new provider of financial services, as fraudulent merchants may move from LFI to LFI seeking to conceal their activities. Merchants operating in higher-risk sectors, and those that are cash-intensive businesses, are likely to require EDD that could involve performing a periodic site visit of the merchant's place of business. For more information, please consult the CBUAE's *Guidance for LFIs providing services to the Real Estate and Precious Metals and Stones sectors,* and *Guidance for LFIs providing services to Cash-Intensive Businesses*.

As per Article 7 of the AML-CFT Decision, all customers must be subject to ongoing monitoring to make sure that CDD information on file is accurate, complete and up-to-date and to ensure that transactions conducted are consistent with the expected customer profile. To support this process, LFIs should apply solutions that ensure the accuracy and completeness of their data. It also may be appropriate to include non-standard elements of monitoring to reflect the risks of payments customers, such as geographic and IP-address monitoring discussed above, and the monitoring of the balance between peer-to-peer and merchant payments in a customer's account. For merchant relationships, ongoing monitoring should include an examination of the number of 'chargebacks' or refunds the LFI has had to award to customers of the merchant, as well as any customer complaints the LFI has received. Where a merchant generates a large number of customer complaints or refund requests, or none at all, it may be a sign that it is operating a fraudulent business.

3.3.2. Controls

In line with their risk appetite and AML/CFT program, LFIs should develop controls that are commensurate with the nature and size of their business to enable them to manage the risks identified. Effective controls are those designed to minimize or eliminate those aspects of the PPS and NPPS that make them most attractive to illicit actors as discussed in section 2 above. LFIs should in particular consider:

- **Geographical limits.** LFIs should strongly consider using IP addresses and smartphone geolocation capabilities to prevent customers accessing PPS from high-risk countries. There are a number of sources that LFIs can use to develop a list of high-risk countries, jurisdictions, or regions. LFIs should consult any publications issued by the National Anti-Money Laundering and Combating the Financing of Terrorism and

financing of Illegal Organizations Committee (NAMLCFTC)[6], the UAE Financial Intelligence Unit (UAE FIU), and the FATF. LFIs may also use public free databases such as, for example, the Basel AML Index[7] or the Transparency International Corruption Perceptions Index.[8] LFIs should not solely rely on public lists, however, and should consider their own experiences and the nature of their exposure to each jurisdiction when assessing the risk of that jurisdiction. LFIs should be aware, however, that given the widespread availability of Virtual Private Network (VPN) services, simply using IP address-based screening is not likely to be effective in preventing access to their service from specified areas. LFIs that use this control should make sure their systems are designed to detect VPN usage.

- **Transaction limits.** Smaller transactions are not without illicit finance risk, but from the perspective of materiality, transaction and volume limits (daily, weekly, monthly, etc.) can decrease an LFI's exposure to illicit payments and also make the PPS overall less attractive to illicit actors.

- **Funding constraints.** Requiring customers to fund their accounts and to withdraw funds using only transfers from regulated domestic financial institutions can help protect PPS from the risks related to cash and ensure that the customer will be subject to CDD and monitoring.

- **Multi-factor authentication.** Requiring customers to provide a One-Time Password (OTP), or answer a phone call, or prompt on their smartphone when logging into an internet-based PPS can help prevent the misappropriation of customer funds by hackers. With regard to the OTP, all banks are required to include specific information in the messages that contain an OTP (full transaction amount, detailed beneficiary merchant name and website and a dedicated telephone number for customers to report suspected fraudulent activity). Banks are also required to ensure that card acquirers and issuers assist them to provide the additional OTP information as needed.[9]

---

[6] Available at: namlcftc.gov.ae/en/more/jurisdictions/
[7] Available at: baselgovernance.org/basel-aml-index
[8] Available at: transparency.org/en/cpi/2020/index/nzl
[9] Notice 4892/2021 issued by the CBUAE to all Banks in October 2021 regarding *"One-Time Password (OTP) for card transactions".*

3.3.3. Wire Transfers Requirements

Articles 27-29 of the AML-CFT Decision contain specific requirements with regard to information that LFIs must collect, and transmit with the wire transfer, when conducting an international wire transfers as well as specific obligations related to domestic wire transfers. In addition, Guidance on CDD measures concerning wire transfers is laid down in section 6.3.2 of the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions.* It is important to note that since many Payment Sector participants qualify as financial institutions, the applicability of these requirements is wide-ranging.

3.4. Preventive Measures for LFIs Providing Services to other Payment Sector Participants

3.4.1. Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring

As mentioned above, LFIs must conduct appropriate CDD on all customers, regardless of their type or sector. The majority, if not all, of Payment Sector participant customers will be legal persons for which LFIs should conduct CDD as required by Articles 8 and 9 of the AML-CFT Decision. In particular, under Article 9 of the AML-CFT Decision, LFIs

are required to identify the beneficial owners of a legal person customer by obtaining and verifying the identity of all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25% or more, and where no such individual meets this description, the LFI must identify and verify the identity of the relevant individual(s) holding the senior management position in the entity. For more information, please consult the CBUAE's *Guidance for Licensed Financial Institutions providing services to Legal Persons and Arrangements*. LFIs should ensure that their contractual agreements with Payment Sector participant customers ensure that the LFI can access necessary information in a timely fashion. **If LFIs cannot access this information in accordance with timelines laid out in its policies, they should consider restricting and ultimately terminating the relationship**.

Furthermore, as per Articles 8.3 and 4 of AML-CFT Decision, for all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This step requires the LFI to collect information that allows it to create a profile of the customer and of the expected uses to which the customer will put the LFI's products and services. In the context of payments, the LFI must understand whether and how its services are being used by its Payment Sector participant customer to facilitate provision of the PPS to its customer (Payment Sector participant customers may also be transacting on a proprietary basis). This should include a determination of whether nesting will take place. If the LFI prohibits nesting, it should make that prohibition clear to the customer.

In addition to the standard required CDD elements of Sections 2 and 3 of the AML-CFT Decision, LFIs should collect all the information necessary to risk-rate the Payment Sector participant customer considering the risk factors described in section 3.2 above and whether aspects of the customer profile require EDD. LFIs should also consider the following steps to gain a more detailed understanding of the customer's business in order to be sure that they fully understand it:

- Review the customer's promotional materials, including its website, to understand its target customers and the services it purports to offer.
- Understand how the customer provides payment services, the other participants it works with to do so, and whether it uses agents or affiliates.
- Requiring the customer to identify its major merchant customers by providing information such as the merchant's name, principal business activity, geographic location, and transaction volume, and use public records searches or information provided by the customer to determine whether these merchants are operating a legitimate business.
- Visiting the customer's headquarters and business operations center and evaluating the customer's AML/CFT controls.
- Reviewing public databases to ensure that the customer, its beneficial owners, and its senior management have not been subject to law enforcement actions.

Under Article 7 of the AML-CFT Decision, all customers must also be subject to ongoing monitoring throughout the business relationship. Changes in the design or structure of a PPS, as well as changes in a Payment Sector participant's customer base (including both the consumer and merchant customer base), can have a major impact on the overall risk associated with the Payment Sector participant. Ongoing monitoring of the customer relationship should be sufficiently rigorous to identify when such changes have taken place, as well as any other changes that impact the customer's risk rating, and should be conducted at a frequency appropriate to the customer's risk and the materiality of its transactions. Ongoing monitoring should also include a review of the customer's transactional activity to determine whether it is in line with expectations established at onboarding and with activity during the previous review period. Sharp or substantial changes in activity may have a fully legitimate cause, such as growth in the customer's user base, but LFIs should still ensure they understand the reasons for these changes.

3.4.2. Correspondent Due Diligence

Article 25 of the AML-CFT Decision sets out specific mandatory requirements for LFIs entering into a Correspondent Banking Relationship or any similar relationship, no matter the nature of their customer, which include the following:

- Refrain from entering into or maintaining a Correspondent Banking Relationship with shell banks or an institution that allows their accounts to be used by shell banks;
- Collect sufficient information about any receiving correspondent banking institution for the purpose of identifying and achieving a full understanding of the nature of its business and to make available, trough publicly available information, its reputation and level of control, including whether it has been investigated;
- Evaluate the AML/CFT controls applied by the receiving institution;
- Obtain approval from senior management before establishing new Correspondent Banking Relationship; and
- Understand each institution's AML/CFT responsibilities.

In the context of Correspondent Banking Relationships with Payment Sector participants, LFIs should conduct correspondent due diligence that reflects the unique risks and features of those relationships. As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, **each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it.** Thus, LFIs should be aware of intermediated risk posed by Payment Sector participants—including providers of SVF, retail payment services, and card schemes—that access banking services through their accounts with an LFI. As a result, LFIs should in particular consider:

- **Regulatory status**. As discussed above in section 2.1.4, jurisdictions take different approaches to regulating the Payment Sector, and not all Payment Sector participants that would qualify as financial institutions under the UAE's legal and regulatory framework are required to be licensed and regulated in their home jurisdiction. When offering services to a foreign entity, LFIs should consider not just its licensing status under its home jurisdiction's laws, but its licensing status should it carry out those same activities in the UAE. Where a foreign entity would require a license in the UAE, LFIs should treat it as a financial institution and subject it to correspondent due diligence. In these cases, LFIs should be particularly cautious to ensure that their correspondent implements an AML/CFT program that at least meets the requirements of the AML-CFT Law and Decision, and be aware that the correspondent is likely not supervised to ensure effective implementation of this program, increasing its risk.
- **Merchant Due Diligence.** LFIs should ensure that their Payment Sector participant customers conduct appropriate due diligence not just on customers but on merchants as well. LFIs should request and review the correspondent's due diligence policies, procedures, and processes to determine the adequacy of its due diligence standards for merchant and consumer customers.
- **Controls related to nesting.** When an LFI offers services to a correspondent without knowing that nesting is taking place, it is unable to take appropriate measures to manage the risk of the nested relationship and, thus, likely to be exposed to higher risks. LFIs should therefore always understand all purposes for which the correspondent account will be used and ensure that the CDD and monitoring applied to the relationship will assess whether nesting is taking place.
- **Testing and auditing.** On a risk-basis, LFIs should consider taking active measures to test the correspondent's AML/CFT program. This can include, at a minimum, reviewing the correspondent's internal audit reports and can extend to requiring the correspondent to hire an external auditor, conducting on-site reviews and discussions at the correspondent's premises.

3.5. Targeted Financial Sanctions

Article 16.1 of the AML-CFT Law and Article 60 of the AML-CFT Decision require LFIs to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, the Cabinet Decision 74 of 2020 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List. For more information, please consult the Executive Office of the Committee for Goods and Material Subjected to Import and Export Control's *Guidance on TFS for Financial Institutions and Designated Non-financial Business and Professions and Virtual Assets Service Providers*[10], the CBUAE's *Guidance for LFIs on the Implementation of TFS,* and *Guidance for LFIs on Transaction monitoring and Sanctions screening*[11].

LFIs should take appropriate steps to develop, implement and regularly update an appropriate Sanctions Compliance Program in order to fulfil their obligation to comply with the related requirements that includes screening of customers and transactions. LFIs should be aware that, for all PPS they offer, they should have in place operational systems that ensure they can appropriately screen transactions related to those products or services. If they cannot conduct appropriate screening, they should not offer that product or service. **LFIs should also ensure that the required information fields are created and duly transmitted throughout the payment cycle across the different PPS**. LFIs should screen all information they have about a transaction, including any messages between users engaging in a peer-to-peer transfer that may have a non-uniform number of characters, use special characters, or present other challenges to screening systems.

An LFI that does not wish to have any exposure to high-risk countries will need to take additional measures to control where its customers use its products or services. Furthermore, sanctions risk assessments can change from time to time depending on where a customer is currently located. In intermediated correspondent relationships, LFIs should ensure that they fully understand their correspondents' sanctions screening approaches, and **should not process any payments for a correspondent unless they are entirely confident that the correspondent conducts appropriate screening**. LFIs cannot rely on another LFI to fulfill screening obligations related to transactions on their own accounts or systems.

Furthermore, LFIs must sign up for the Integrated Enquiries Management System ("IEMS") introduced by the UAE FIU to automate and facilitate the execution process of requests for information, implementing decisions of public prosecutions and any other type of ML/FT requests. Via this system, the FIU can make requests to all LFIs simultaneously with the goal of processing requests and providing results to law enforcement authorities more efficiently. For more information, please consult the *IEMS User Guide* published by the UAE FIU.[12]

---

[10] Available at uaeiec.gov.ae/en-us/un-page#
[11] Available at centralbank.ae/en/cbuae-amlcft
[12] Available at uaefiu.gov.ae/media/jtdnttby/integrated-enquiry-management-system.pdf

3.6. Transaction Monitoring and Suspicious Transaction Reporting

Under Article 16 of the AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of a Suspicious Transaction Report (STR), a Suspicious Activity report (SAR) or other report types. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/FT risks of the institution's customers, products and services, delivery channels, and geographic exposure. For more information, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*.

As required by Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, LFIs must file a STR, a SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, is related to a crime, or is intended to be used in a crime. STR filing is not sim ply a legal obligation; it is a critical element

of the UAE's effort to combat financial crime and protect the integrity of its financial system. By filing STRs with the UAE FIU, LFIs alert law enforcement authorities about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs.

As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, **each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it.** Although LFIs cannot outsource their responsibility to report suspicious activity, they can outsource certain aspects of transaction monitoring. In the prepaid card scheme described in section 2.1.7, for example, the bank that offers the prepaid cards may outsource automated transaction monitoring to the program manager, which has more direct insight into individual transactions. The bank in this situation, and any LFI that outsources any elements of transaction monitoring, nevertheless retains ultimate responsibility for identifying and reporting suspicious transactions.

3.7. Governance and Training

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. Therefore, in addition to the mandatory governance and training requirements set forth in the AML-CFT Law and Decision, Payment Sector participants and LFIs providing them services should endeavor to incorporate the following considerations into the design of their governance frameworks and their training programs.

- **Clear allocation of AML/CFT responsibilities among LFIs.** When a network of Payment Sector participants combine to deliver a payment service and execute transactions, risks arise when they do not have a clear understanding of each participant's AML/CFT responsibilities. Allocating responsibilities is particularly important when some LFIs involved in a payment will not form a relationship with the ultimate customer or beneficiary. Card schemes should have a governing body, but this may not be a requirement for other Payment Sector participants depending on their role in processing payments. LFIs should understand the parties and their roles and responsibilities in the scheme and manage risks accordingly. **Any LFI that provides payment services as part of a network should assume full responsibility for CDD**. Furthermore, LFIs cannot rely on any other entities to implement elements of the AML/CFT program, such as the appointment of a compliance officer and the reporting suspicious transactions. **Similarly, when a LFI provides services to a Payment Sector participant as part of a Correspondent Banking Relationship, they should also understand each party's AML/CFT responsibilities and document them in the contract or other program documents**. Understanding the parties' respective AML/CFT responsibilities is a mandatory element of correspondent CDD under Article 25 of the AML-CFT Decision.

- **Agent Governance and Training.** Where a payment service or product relies on the use of agents for delivery, it is critical that they are appropriately trained to recognize red flags for illicit activity, and to carry out the elements of the AML/CFT program for which they are responsible. LFIs that use agents should have appropriate programs in place to manage them through effective governance arrangements that, among other measures, set clear requirements for terminating relationships if agents do not comply with the LFI's policy. LFIs should provide training directly to agents and test their compliance on a regular basis. Where agents participate in sensitive activities, such as cash acceptance or onboarding, they should receive increased training and be subject to additional controls and testing.

- **Employee Training.** As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of PPS, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For Payment Sector participants that offer PPS as their primary business, employee training should be focused on payments-related risks. For LFIs that offer services to Payment Sector participants, employee training should cover payment risks as appropriate to the employee's role and responsibilities as well as the LFI's overall exposure to the sector.

Annex 1. Synopsis of the Guidance

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by Licensed Financial Institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, stored value facilities, retail payment service providers, and card schemes.
Understanding Risks	ML/FT Risks of the Payment Sector	**Characteristics of the Movement of Funds:** Products and Services (PPS) and New Payment Products and Services (NPPS)in particular are extremely attractive to illicit actors because of the rapid movement of funds between Payment Sector participants and across borders. The risks vary based on transaction speed, transaction limits, closed vs. open loop system, methods of funding and access to cash, payment transparency, ability for one person to create multiple accounts, non-face-to-face relationships, and use of virtual assets (the latter is addressed in a separate guidance to be issued by CBUAE).
		Peer-to-Peer Payments: NPPS allow participants to send money that will be instantly available to the beneficiary, reducing the need for trust in the relationship. The use of PPS for peer-to-peer payments creates risk for financial institutions because transactions can flow through third parties that may not be subject to AML/CFT requirements.
		Cross-Border Movement: Many NPPS can be used globally for making payments or transferring funds, thus introducing banks to new geographical exposure. Unlike cross-border wires, which carry full identifying information, banks will frequently only see the customer's transactions with the payment network itself, rather than their location or ultimate destination.
		Global Regulatory Gaps: Countries take a variety of approaches to regulating the Payment Sector and there is no one widely accepted classification of participants. And participants, as relatively new market entrants, may lack the experience, expertise, or commitment to apply fully effective preventive measures.
		Intermediation: A number of participants potentially involved in a single transaction. Intermediated transactions create risk because no regulated entity participating in the transaction has the visibility necessary to fully understand the transaction and the participants.
		Nesting: Nesting is a form of intermediation that presents specific risks. In most Correspondent Banking Relationships that involve nesting, the respondent financial institution is not aware of individual transactions ordered by the ultimate customer.
		Use of Agents and Affiliates: Payment Sector participants often interact in a dense web of agency and affiliate relationships. A large number of entities involved in the NPPS, in particular when involving several countries, may increase the ML/FT risk. The interplay between different entities can lead to risks from intermediation and also when

		the participating entities have not assigned clear responsibility for compliance with AML/CFT requirements.
		Merchant Risks: Globally, Payment Sector participants including providers of NPPS have been abused by or directly complicit with merchants who offer fraudulent or illegal goods or services, or whose business models pose reputational risks to financial institutions. Relying on third parties to conduct customer due diligence (CDD) on merchants can also increase risk if the relationship is not well-governed.
	ML/FT Risks for LFIs Providing Services to Payment Sector Participants	**Correspondent and Correspondent-Type Risk:** Correspondent Banking Relationships in which the correspondenfs customers' funds flow through an account held at the respondent financial institution are particularly high risk, because they expose the respondent institution directly to any potentially illicit activity in which the correspondent's customers are engaged. Because banks that offer services to correspondents have limited information on these transactions, they are reliant on the correspondent to implement an effective AML/CFT program.
		Other Risks Related to Intermediation: Even banks that view themselves as having limited to no exposure to NPPS may have indirect exposure through customers who link their bank accounts to payment apps, or use their bank accounts to fund stored value facilities (SVF) accounts or wallets, or withdraw funds as cash and use it to purchase other prepaid instruments.
		Risks Related to Outsourcing: Banks often serve as the backbones of PPS such as credit, debit, and prepaid schemes without serving as the administrator or governing body of the scheme. Banks involved in these schemes often outsource CDD and other elements of the AML/CFT program to the program operators who have more direct contact with customers and insight to movement of funds. But Banks remain responsible for implementing an effective and compliant AML/CFT program.
Mitigating Risks	AML/CFT obligations under CBUAE Regulations	In addition to this guidance, LFIs including non-bank payment service providers should carefully review all the relevant regulations issued by the CBUAE, which provide a comprehensive coverage of all payment products, services, and systems that are issued, provided and/or operated in the UAE, to ensure they fully understand and comply with their AML/CFT obligations. In 2020-2021 the CBUAE issued the SVF Regulation, the Retail Payment Services and Card Schemes Regulation, the Large Value Payment Systems Regulation, and the Retail Payment Systems Regulation.
	Risk Assessment	An appropriate risk assessment should consider all the PPS that an LFI provides, and the LFI's direct relationships to Payment Sector participants, both domestic and foreign. When assessing an LFI's direct exposure to the Payment Sector, the LFI should consider the risk factors discussed in section 2 of the Guidance, such as the movement of funds, mode offunding, and peer-to-peer payments among others. Where LFIs provide services to Payment Sector participants, they should also assess the risk of the relationship as well as their indirect exposure to the Payment Sector through their customers.

	Preventive Measures for LFIs Providing Products and Services directly to Customers	**Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring:** LFIs must perform all the elements of CDD, which include customer identification and verification, beneficial owner identification, understanding of the nature of the customer's business and purpose of the relationship, and ongoing monitoring. In addition to these mandatory elements, LFIs should consider the following elements that are particularly important in the context of NPPS: user identification and verification, use of IP addresses and geographical (spatial and temporal) locators, and SVF and merchant due diligence.
		Controls: LFIs should develop controls that are commensurate with the nature and size of their business to manage the risks identified. LFIs should in particular consider geographical limits, transaction limits, funding constraints, and multi-factor authentication to minimize or eliminate those aspects of the PPS and NPPS that make them most attractive to illicit actors.
		Wire Transfers Requirements: The AML-CFT Decision contain specific requirements with regard to information that LFIs must collect, and transmit with the wire transfer, when conducting an international wire transfers as well as specific obligations related to domestic wire transfers (the Guidelines further contain CDD measures). Since many Payment Sector participants qualify as financial institutions, the applicability of these requirements is wide-ranging.
	Preventive Measures for LFIs Providing Services to other Payment Sector Participants	**Customer Due Diligence, Enhanced Due Diligence and Ongoing Monitoring:** LFIs must conduct appropriate ODD on all customers, regardless of their type or sector (the majority, if not all, of Payment Sector participant customers will be legal persons). In this context, the LFIs should also consider a determination of whether nesting will take place. In addition to the standard required ODD elements, LFIs should collect all the information necessary to risk-rate the Payment Sector participant customer and evaluate whether aspects of the customer profile require EDD. All customers must also be subject to ongoing monitoring throughout the business relationship.
		Correspondent Due Diligence: In the context of Correspondent Banking Relationships with Payment Sector participants, LFIs should conduct correspondent due diligence that reflects the unique risks and features of those relationships. In the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it. LFIs should in particular consider regulatory status, merchant due diligence, controls relating to nesting, and testing and auditing of the correspondents AML/CFT program.
	Targeted Financial Sanctions	LFIs are required to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council under Chapter VII of the Charter of the United Nations and the requirements set by Cabinet Decision 74 of 2020 regarding Targeted Financial Sanctions. LFIs should be aware that, for all PPS they offer, they should have in place operational systems that ensure they can appropriately screen transactions related to those products or services. In intermediated correspondent relationships, LFIs should ensure that they fully

		understand their correspondents' sanctions screening approaches, and should not process any payments for a correspondent unless they are entirely confident that the correspondent conducts appropriate screening.
	Transaction Monitoring and Suspicious Transaction Reporting	LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of a Suspicious Transaction Report (STR), a Suspicious Activity report (SAR), or other report types. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of ODD. As discussed above, in the case of extended, intermediated transaction chains such as those frequently seen in the Payment Sector, each LFI involved is ultimately responsible for monitoring all transactions processed or conducted through the LFI, using the information available to it. Any LFI that outsources any elements of transaction monitoring retains ultimate responsibility for identifying and reporting suspicious transactions.
	Governance and Training	Payment Sector participants and LFIs providing them services should endeavor to incorporate the following considerations into the design of their governance frameworks and their training programs: clear allocation of AML/CFT responsibilities among LFIs, agent governance and training, and employee training. When a network of Payment Sector participants combine to deliver a payment service and execute transactions, risks arise when they do not have a clear understanding of each participant's AML/CFT responsibilities. Any LFI that provides payment services as part of a network should assume full responsibility for CDD. When a LFI provides services to a Payment Sector participant as part of a Correspondent Banking Relationship, they should also understand each party's AML/CFT responsibilities and document them in the contract or other program documents.

Guidance for Licensed Financial Institutions on the Risks Relating to Politically Exposed Persons

Effective from 1/8/2022 **Status:** In-Force

1. Introduction

1.1. Purpose of the Guidance

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or

supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators identified by the FATF. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, stored value facilities, retail payment service providers, card schemes, registered hawala providers and other LFIs; and
- Insurance and re-insurance companies, agencies, and brokers.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws:

- Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended by Federal Decree Law No. (26) of 2021 ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision").

1.4. Acronyms and Definitions

Heads of International Organizations (HIO): Natural persons who are or have been entrusted with the management or any prominent function within an international organization.

International Organizations: Entities established by formal political agreements between their Member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations; regional international organisations; military international organisations, and economic organisations.

Politically Exposed Persons (PEP): Natural persons who are or have been entrusted with a prominent public function in the UAE or any other foreign country such as heads of states or governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state owned corporations, and senior officials of political parties, and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:

- Direct family members (of the PEP who are spouses, children, spouses of children, parents)
- Associates known to be close to the PEP, which include:
  - Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP;
  - Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

Related Customers: Customers that are the direct family members of a PEP or the associates known to be close to a PEP.

2. Understanding Risks

Article 15 of the AML-CFT Decision and the FATF standards impose specific Customer Due Diligence (CDD) obligations on LFIs with respect to Customers that are Politically Exposed Persons (PEPs) which include the Direct Family Members or Associates Known to be Close to the PEPs. The AML-CFT Law and Decision give special attention to these customers because they are likely to expose LFIs to a heightened risk of money laundering, terrorism financing, and other illicit finance. **The special requirements related to PEPs are not an indication that LFIs should avoid dealing with such customers**. Instead, these requirements are meant to ensure that LFIs have done the due diligence necessary to fully identify, understand their customers and have made fully-informed decisions regarding whether or not to accept the customer or to continue the relationship. There are three sub-groups of PEPs:

- PEPs who are or have been entrusted with their prominent public position in the UAE are known as "**domestic PEPs**";
- PEPs who are or have been entrusted with their prominent public position in any other foreign country are known as "**foreign PEPs**"; and
- PEPs who are or have been entrusted with the management or any prominent function within an international organization are known as "**Heads of International Organizations (HIOs)".**

Customers that are PEPs, and transactions involving PEPs, receive special attention under the UAE legal and regulatory framework and the FATF standards because they bear a higher risk of involvement in certain proceeds-generating offenses: corruption, misuse or theft of public funds, and bribery. It is important to note that the majority of PEPs are law-abiding public servants and that no more than a small percentage of PEPs are involved in these offenses. Nevertheless, the risk is still higher than in the general population.

PEPs are at higher risk of involvement in these crimes because of the powers that come with their position or status. Most importantly, a PEP has **power or influence** over how government funds are spent, or over state action. PEPs may use their power or influence to directly enrich themselves, their family members, and their associates, by stealing or misdirecting government funds. Or they may sell their power or influence to illicit actors who are seeking to obtain a specific outcome, whether it is a lucrative contract, the passage of a regulation, or the transfer of government secrets.

The AML-CFT Decision also requires LFIs to perform the same specific due diligence on the direct family members and known close associates of a PEP. These individuals may not themselves have any direct power or influence over government actions, but they nevertheless present higher risks to LFIs as a result of their relationship with a PEP.

- PEPs, knowing that their financial transactions will be subject to scrutiny, may use family members or associates to carry out illicit transactions or collect illicit funds, in an attempt to hide their involvement in a transaction and their illicit gains. In many countries where corruption is an issue, PEPs themselves may nominally possess few assets, while their family members and associates openly display their wealth.
- Illicit actors seeking to persuade a PEP to take certain actions may seek to achieve this goal by paying off the people close to the PEP, the PEP's family members and close associates. For instance, a person seeking a government contract may pay a PEP's spouse to "put in a good word for him or her" with the PEP, or to gain

access to the PEP by inviting the contractor to the PEP's home. These payments may be made with or without the knowledge or consent of the PEP.

Article 15 of the AML-CFT Decision also requires LFIs to identify those legal person and legal arrangement customers that have at least one beneficial owner who is a PEP (see sections 3.2.1 and 3.2.2 below). In this Guidance, customers that are the direct family members of a PEP, the known close associates of a PEP, or that are legal persons or legal arrangements with at least one beneficial owner who is a PEP will be referred to as "**Related Customers**."

Although LFIs are required to apply special procedures for all PEPs and Related Customers, not all PEPs and Related Customers are equally high-risk. The sources of risk for a PEP are closely related to the risk that a PEP could have abused his or her position for financial gain. Some factors that can influence the risks of a particular PEP are:

- The PEP's ability to control highly consequential outcomes. Certain roles are more likely to attract large-scale corruption. For example, a judge in a traffic court may be offered bribes, but these are likely to be lower in value than the bribes potentially offered to a judge who presides over the trials of organized criminal groups.
- The authority and independence inherent in the PEP's role or function. Where a PEP has greater authority or independent decision-making authority, he or she is more likely to be able to achieve outcomes that are beneficial to him/herself or his/her family or associates.
- The access to funds inherent in the PEP's role. A PEP that can control the disbursement of funds is likely to have more opportunities for engaging in embezzlement and self-dealing.
- The nature of governance in the state or organization that has entrusted the PEP with a prominent function. Poor governance undermines transparency and accountability. Strong governance can help ensure that public officials are unable to use their office for gain, or are quickly caught if they do so. Governance is a broad category that includes the strength of anti-corruption laws, the vigor with which corruption is investigated and prosecuted, and the authority of independent public auditors.
- The overall level of corruption in the state or organization that has entrusted the PEP with a prominent function. Where corruption is rife, public officials are unlikely to be entirely immune.

The sources of risk for a Related Customer can be divided into two broad categories:

- The risk of the PEP to which the Related Customer is connected (i.e. understanding the risk of the PEP and its characteristics).
- The relationship between the Related Customer and the PEP (i.e. the type and strength of the relationship (e.g. the closer the relationship, the more likely the Related Customer is to share the PEP's risk)).

3. Mitigating Risks

The AML-CFT Decision contains specific, mandatory requirements for managing risks related to PEPs. **It is important for LFIs to be aware that the Decision imposes baseline requirements that are higher than for other types of customers**. LFIs cannot choose to omit these requirements even when they consider that risks associated with a specific customer or transaction are low. This does not mean, however, that LFIs are not expected to take a risk-based approach to these customers. LFIs should implement the baseline controls described below as well as consider whether additional controls are necessary when even higher risks are present.

Furthermore, the sections below discuss how LFIs can apply the required specific preventive measures to identify, manage, and mitigate the risks associated with PEPs. It is not a comprehensive discussion of all AML/CFT requirements imposed on LFIs. LFIs should consult the legal and regulatory framework currently in force, the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*, and the CBUAE issued Guidances for further information[2]. The controls discussed below should at the minimum be integrated into the LFI's larger AML/CFT compliance program and supported with appropriate governance and training.

[2] Available at centralbank.ae/en/cbuae-amlcft

3.1. Legal Requirements

Article 15 of the AML-CFT Decision requires LFIs to carry out specific mandatory due diligence measures on PEPs and Related Customers, in addition to the standard CDD required for all customers under its Section 3 (described in Articles 5-14). In line with FATF standards (Recommendation 12), Article 15 imposes on LFIs different requirements for foreign PEPs as opposed to domestic PEPs and HIOs. **For foreign PEPs and Related Customers, LFIs must:**

(a) Put in place suitable risk management systems to determine whether a Customer or the Beneficial Owner is considered a PEP (i.e. a foreign PEP, or the direct family member or known close associate of a PEP).
(b) Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP (i.e. foreign PEP and Related Customers).
(c) Take reasonable measures to establish the source of funds and wealth of Customers and Beneficial Owners identified as PEPs (i.e. foreign PEPs and Related Customers).
(d) Conduct enhanced ongoing monitoring over such relationship (i.e. the relationship with a foreign PEP or Related Customers).

For domestic PEPs and HIOs and their Related Customers, LFIs must:

(a) Take sufficient measures to identify whether the Customer or the Beneficial Owner is considered one of those persons (see section 3.2.4).
(b) Take the measures identified in (b), (c), and (d) when there is a high-risk business relationship accompanying such persons.

Like the FATF standards, article 15.2 of the AML-CFT Decision imposes special PEP-related requirements for certain insurance policies, although its requirements apply to a slightly broader range of policies. LFIs must take reasonable measures to determine whether the beneficiary, or the beneficial owner of a beneficiary, of a life insurance policy or of family takaful insurance is a PEP or a Related Customer. If identified as a PEP or Related Customer, LFIs must inform senior management before pay-out of those policies, or prior to the exercise of any rights related to them. LFIs must also thoroughly examine the overall business relationship, and consider filing a suspicious transaction report (STR), a suspicious activity report (SAR) or any other report types with the FIU where applicable (please see section 3.3.2 below).

3.2. Applying Legal Requirements

3.2.1. Classifying Customers as PEPs

The definition of PEP in the AML-CFT Decision specifically lists the following roles as persons who always qualify as PEPs:

- Heads of States or Governments;
- Senior politicians;
- Senior government officials;
- Judicial officials;
- Military officials;
- Senior executive managers of state-owned corporations;
- Senior officials of political parties; and
- Persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation.

However, as there is **no exhaustive list** of the positions that qualify an individual as a PEP globally, the above list is not exhaustive and LFIs should use their discretion in identifying PEPs, and develop **risk-based** policies and procedures

to ensure they appropriately identify customers who are PEPs, or the family members or close associates of PEPs.

For example, LFIs should use discretion in determining whether a customer who is government official or manager of a state-owned corporation is sufficiently "senior" to qualify as a PEP under the definition of the AML-CFT Decision. Not all public sector employees are PEPs. For example, a civil servant who sorts mail at the post office is unlikely to be a PEP, and although any public employee can carry some level of corruption risk, in such cases the risk is not sufficiently high to warrant special procedures. This distinction is captured in the AML-CFT Decision's definition of a PEP as a natural person who has been awarded a "**prominent public function**." At the same time, the decision whether or not to treat a customer as a PEP cannot be based solely on the customer's title, rank, civil service grade, or other similar factors. It is also important to be aware that "prominent" is not simply equivalent to 'famous' or 'well-known,' and that individuals may be "entrusted" with a public function in a wide variety of ways, including by appointment, election, and promotion through the civil service.

Furthermore, LFIs should also be aware that high risks of corruption can exist even when a customer is not immediately qualifying as a PEP per definition. For example, the heads of large trade unions and professional associations are likely to wield political power without having been appointed to those roles by a government or international organization. LFIs may decide, in terms of their own risk appetite, to treat such individuals as PEPs.

The determination of whether a customer is a PEP should therefore consider a number of factors, including, most importantly, whether the natural person currently holds, or has recently held, a role that gives him or her **power or influence** over decisions, policy or the disbursal of funds belonging to a government or an international organization. Factors to consider when making this determination include the nature of the political and governance system in the country or international organization where the customer holds his or her position; roles and responsibilities within that system; authority over government decisions and activities, and access to government funds and assets (whether directly or indirectly such as through the awarding of government contracts).

PEPs are always natural persons. However, LFIs should perform a PEP analysis on customers who are the beneficial owners of legal persons or legal arrangements. Depending on the customer's ownership and control structure, it may also be appropriate to perform a PEP analysis on the customer's senior managing officer or senior management. Where risks are higher, for example, in the case of companies with complex structure and complex trust arrangements, LFIs should consider identifying beneficial owners below the 25% threshold mandated by the AML-CFT Decision. For example, a PEP and his spouse and three children may each own 15% of a company. No single family member would have to be identified as a beneficial owner under UAE law, but when their ownership shares are added together the family clearly exercises control over the company. Such a company would likely need to be subjected to the EDD requirements discussed in section 3.2.6.

3.2.2. Classifying Customers as Related Customers

The AML-CFT Decision requires LFIs to treat the direct family members and close associates of PEPs as if they were PEPs themselves.

- Article 1 of the AML-CFT Decision defines direct family members of a PEP as the PEP's spouses, children, spouses of children, and parents.
- Article 1 of the AML-CFT Decision defines close associates of a PEP as:
    - Natural persons having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP; and
    - Natural persons having individual ownership rights in a legal person or arrangement established in favour of the PEP.

The above-mentioned relationships should be viewed as a mandatory minimum, not as an exhaustive list of all relationships that may justify to treat a customer as a PEP. The link between the family member or the close associate with the PEP determine the level of risk. LFIs should take a **risk-based approach** and consider whether a

relationship exists between their customer and the PEP that could be exploited or abused to obscure the PEP's connection to illicit funds.

For example, an LFI may choose to also define as a direct family members any person in a relationship with a PEP, and, as close associates, partners, prominent members of the same political party or civil organization as the PEP; close friends or advisors; business partners or associates, especially those that share (beneficial) ownership of legal entities with the PEP, or who are otherwise connected (e.g. through joint membership of a company board) in accordance with FATF Guidance and the above mentioned definition.

Once an LFI has established that a qualifying relationship exists between a customer (or the beneficial owner of a customer) and a PEP, the LFI must treat the customer as a PEP (or as owned by a PEP). There is one important distinction, however, between a PEP and the direct family member or close associate of a PEP: the latter cannot transfer their status to their own family members and close associates. For example:

- General A is the head of the Air Force of a country. Mr. B, her son, is married to Mrs. B, a private citizen who owns a grocery store. General A is a PEP, and Mr. B and Mrs. B must be treated as PEPs because they are direct family members of General A.

- Mrs. B is the daughter-in-law of General A. Her brother, Mr. C, a lawyer in private practice, is not required to be treated as a PEP. Mr. C's connection to the true PEP (General A) is too distant. Even though Mrs. B is treated as a PEP, Mr. C does not need to also be treated as a PEP merely because he is a sibling of Mrs. B.

  LFIs should, however, apply EDD requirements and/or enhanced monitoring of the relationship if they have identified any high risks, such as concerns that the more distant family members or business associates of a PEP may be involved in corruption or any other sort of illicit activity, whether or not it involves the PEP.

Similarly:

- Mr. X is a prominent politician in a country who recently left office, but who may run for office in the future. Following his departure from office, Mr. X and Mrs. Y became cofounders of a real estate development company, with each owning 50% of the company. Due to Mr. X's prominent function, the partnership has been extensively covered in the media. Mr. X is a PEP because of his recent past position. Mrs. Y must be treated as a PEP because she is a known close associate of Mr. X.

- Mrs. Y is also a 50% owner of an entirely separate business that manufactures cell phones. Mrs. Y's co-owner of that business, Mr. Z, does not need to be treated as a PEP. As the business partner of a business partner of a PEP, his connection to Mr. X is too distant. LFIs should, however, apply EDD requirements and/or enhanced monitoring of the relationship if they have any concerns that the more distant family members or business associates of a PEP are involved in corruption or any other sort of illicit activity, whether or not it involves the PEP.

3.2.3. Time Limits of PEP Status

The definition of PEP in the AML-CFT Decision makes clear that a PEP does not cease to qualify as a PEP simply because they no longer hold a prominent public function (i.e. "Natural persons who are *or have been* entrusted with prominent public functions"). Nor does a Related Customer cease to require PEP treatment simply because the PEP to whom they are related no longer holds that position. A PEP's risk (and, indirectly, the risk of a Related Customer) derives from the PEP's power or influence over decisions, funds, or policy. Therefore, it may not be appropriate to continue to treat a customer as a PEP long after they have lost such power or influence. On the other hand, if PEP has amassed funds through corruption during his or her period in office, the PEP is likely to wait until being out of office to access or enjoy those funds. This means that the corruption risk remains even if a PEP has been out of office for a certain time.

Because each case is different it would not be appropriate for LFIs to apply a universal rule for determining whether a customer is no longer a PEP (e.g. one year after relinquishing the public position). Therefore, while LFIs may set a schedule to review PEP status, they should make a risk-based decision as to when sufficient time has passed for a customer to no longer be classified as a PEP. Factors to consider when making such a determination include:

- The seniority, prominence, and power inherent in the customer's (or the customer's beneficial owner's) previous role.
- The corruption potential of the customer's previous role. Where there was greater opportunity for illicit gain, it is more likely that the customer's source of funds will continue to be corrupt proceeds for some time after the customer leaves office.
- Whether the customer still exercises informal influence over government decision-making through his or her current formal role (e.g. head of a prominent lobbying organization) or through informal relationships (e.g. the customer is an informal but widely accepted leader of a political party but has no official title).
- Whether the previous and current role of the customer are linked in any way;
- The customer's relationships to other PEPs (e.g., if the customer is a retired politician whose children are involved in politics. In such cases the customer would also likely qualify as the family member of a PEP).
- The nature and purpose of the business relationship, and the overall risks of the products and services the customer avails or intends to avail.
- The customer's relationship to the PEP. Family relationships tend to endure through time, but business relationships do not always persist. A customer who was formerly the close associate of a PEP, but who severed the business relationship some time ago, may present reduced corruption risk.

3.2.4. PEP Screening

Classification of a customer as a PEP or a Related Customer should take place during the CDD stage, prior to the commencement of the business relationship. Under Article 15 of the AML-CFT Decision, LFIs are required to have suitable risk management systems in place to determine whether a customer, or the beneficial owner of a customer, is a foreign PEP, or Related Customer and are required to take sufficient measures to identify whether a customer, or the beneficial owner of a customer, is a domestic PEP or an HIO, or Related Customer. In practice, however, it will generally be appropriate to conduct **onboarding screening and ongoing screening on all customers**. Even citizens of the UAE may qualify as foreign PEPs if they have been entrusted with prominent functions by foreign governments, for example, if they are dual citizens, or held office in a country that does not restrict prominent functions to citizens.

Screening may begin by including a question in onboarding forms or interviews that inquires whether the customer or any beneficial owner is a PEP or Related Customer. LFIs should not however rely solely on a customer's assertion, but supplement this basic screening question with additional due diligence such as additional questions regarding the customer's employment and job title, questions regarding the customer's sources of funds and wealth, and conducting searches of public records (e.g. internet searches or searches of UAE databases) or proprietary databases. Should searches of public records or proprietary databases reveal adverse media on the potential PEP customer, the LFI should review the adverse media and determine whether it is within the LFI's risk appetite to onboard the potential PEP customer and/or subject the PEP to enhanced monitoring.

Where customers are public servants, LFIs should be sure to conduct these searches using not only the customer's name but also the customer's title, as some useful information (such as lists of high-level government positions) may be available by title only.

Some PEPs and Related Customers may be determined to conceal their status from financial institutions and the public at large in order to avoid enhanced scrutiny. In these cases, searches of public records or private databases

may not reveal their status or the connection between the customer and a PEP. As always, LFIs should be alert to any aspects of a customer profile that are inconsistent or do not have a clear explanation. These 'red flags' may be connected to a variety of illicit or questionable activity, including concealed PEP status. Some potential indicators include:

- The customer purports to own and operate a business (particularly a business that relies on political connections) without having the experience or expertise that would likely be considered necessary to successfully operate such a business (e.g., a young person, or a person with no work history, owns a company in an industry that is closely connected to the public sector; or a small firm receives a large government contract that appears far beyond its work experience and capabilities);

- The customer engages in financial transactions that are inconsistent with his or her declared income;

- A minor, or a person with few assets, owns a shell company;

- The customer is a legal arrangement (particularly a complex legal arrangement) where the ultimate settlor and the ultimate beneficiary is the same person;

- The customer wishes to engage in complex transactions, or uses complex corporate structures, with no clear economic purpose.

Because a customer transforms from a non-PEP to a PEP immediately on being entrusted with a prominent public function, LFIs should use the ongoing monitoring process to determine whether a customer's status has changed. Where a PEP customer, or a PEP who is connected to a Related Customer, has lost the prominent public function that qualified him or her for PEP status, ongoing monitoring can also determine whether it is appropriate to no longer classify the customer as a PEP or as a Related Customers, and to cease enhanced measures.

3.2.5. PEP Risk Rating

Under article 15.1.First.d) of the AML-CFT Decision, LFIs must conduct enhanced ongoing monitoring over relationship with foreign PEPs and Related Customers. This does not mean however that such customers should all be automatically assigned the same risk rating. In addition, as per article 15.1.Second.b), for domestic PEPs and HIOs, and their Related Customers, the EDD requirements in section 3.2.6 below are mandatory when there is a high-risk business relationship accompanying such persons. Therefore, it is important to appropriately risk-rate all PEP customers, customers whose beneficial owners are PEPs, and customers that are direct family members and close associates of a PEP. PEP-specific factors to consider in risk rating include:

- The nature of the PEP's position. As discussed in section 2 above, where a PEP has greater ability to control or influence consequential government decisions, the corruption risk is greater. LFIs should consider, among other factors:

    - The nature of the issues or decisions over which the PEP has or had control;
    - The extent to which the PEP had control over the disbursement of funds;
    - The degree of autonomy or independence the PEP has or had in decision-making;
    - The PEP's rank or status within the government or international organization.

- The controls in place in the PEP's own country jurisdiction to prevent corruption, including:

    - The country's position on widely adopted global corruption or transparency ratings;
    - The extent to which the country investigates and prosecutes high-level corruption;
    - Whether the country has a free and empowered political opposition and a free press;
    - Whether the agency, body, or organization in which the PEP holds his or her function has an internal audit/inspector/comptroller function;

- Whether asset disclosure requirements or similar requirements apply to PEPs in that country or jurisdiction.

For Related Customers, LFIs should consider the risk of the PEP to which the customer is connected, and also the nature and extent of the connection, in determining the risk rating.

The risk-rating process should also take into consideration not just features specific to PEPs but also all the standard elements of customer risk rating, such as the nature of the customer's business and the products and services the customer intends to use. For example, a PEP who owns a cash-intensive business and seeks to make bulk cash deposits would likely be considered higher risk than a PEP whose only income is his salary, even if the two customers hold similar positions within a similarly high-risk jurisdiction.

In those cases where a natural person customer has PEP status from two sources, or where more than one PEP is involved in a legal person customer, LFIs should always use the higher risk rating. For example, if a single natural person customer has been appointed to prominent public functions by both the government of the UAE and a foreign government, that customer should be treated as a foreign PEP. Similarly, if a legal person customer has two domestic PEP owners, one high risk and the other medium risk, the legal person customer should be subject to EDD requirements.

3.2.6. Enhanced Due Diligence Requirements

Under Article 15 of AML-CFT Decision, when a customer (or the beneficial owner of a customer) is determined to be a foreign PEP or Related Customer, or where a customer (or the beneficial owner of a customer) is determined to be a domestic PEP or HIO or Related Customer, **and** when there is a high-risk business relationship accompanying such persons, LFIs must take the following mandatory steps:

- **Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP or Related Customer.** The specific senior management member within the LFI who are responsible for approving these relationships will vary based on the LFI's own unique governance arrangements. The CBUAE expects that, if the approving member represents the business (e.g. the Chief Executive Officer or Chief Operating Officer) as opposed to the compliance function (e.g. the Compliance Officer), the LFI's policies and procedures will clearly require that the head of the LFI's compliance function give an opinion as to whether the risk associated with the customer is acceptable. When approving an existing relationship with a PEP or Related Customer, senior management should be notified and their approval obtained for the continuance of the relationship.
- **Take reasonable measures to establish the source of funds, including the source of wealth, of PEPs and Related Customers.** This requirement encompasses two distinct concepts:

  - Source of funds: The direct source of the funds that are used to initially fund the account, and of any funds that are transacted through the account during the course of the business relationship.
  - Source of wealth: The source of the customer's overall wealth, whether or not the LFI is exposed to it.

  In the case of foreign PEPs, higher risk domestic PEPs or HIOs, and Related Customers, LFIs should understand, at least at a high level, how the customer acquired his or her wealth. The goal of the process is to provide the LFI with a reasonable degree of confidence that the customer has not generated his or her wealth through illicit activities. Determining source of wealth does not require that the LFI identify and account for every one of the customer's assets. But the LFI should require the customer to provide information on the customer's total net worth, and the customer's principal sources of income (e.g., salary, inheritance, business income, spousal support, etc.). The LFI should supplement information provided by the customer with publicly or privately available information, including, for example media reports, public employee asset declarations (where required by the PEP's national laws), or published salaries for civil service positions.

The LFI should then make two determinations:

- Whether the customer's stated net worth is consistent with his or her declared sources of income. For example, if a customer who has spent his career in public service claims not to have inherited any funds yet has a net worth of several million of a currency, this would require further investigation. Alternatively, if a customer was a successful business person for most of his career and only recently entered public service, a high net worth may not be a "red flag".
- Whether the customer's stated net worth is consistent with the customer's financial behavior. PEPs who have engaged in illicit activities may lie about their net worth to hide discrepancies with their disclosed sources of income. This is likely to be exposed however when the PEP attempts to engage in financial behavior inconsistent with his or her declared income or net worth. For example, if a PEP declares a total net worth of one million of a currency, this may be consistent with his or her declared licit income; but if he or she chooses to invest a sum equivalent to the entire declared net worth in a speculative investment, this is a sign that his or her wealth requires further investigation.

Where risks are higher, LFIs should perform more intense due diligence on the customer's source of wealth. For example, if a PEP declares that a substantial portion of his net worth is derived from ownership of a business, the LFI should collect information to satisfy itself that the business exists, is operational, and can reasonably be expected to generate such funds for the PEP.

- **Conduct enhanced ongoing monitoring of the relationship.** LFIs must perform risk-based ongoing monitoring of the business relationship for all customers. In the above mentioned cases, the required enhanced ongoing monitoring could include a number of actions designed to manage the enhanced risk of these customers:

  - Subjecting the customer file to more frequent review and updating, including a manual review of transactions. All customer files should be reviewed on a risk-based schedule. For the highest-risk PEPs and Related Customers, reviewing the file as frequently as every six or nine months may be appropriate. This review should also include a review of substantial transactions on the account to ensure that they are consistent with information provided by the customer regarding source of funds and source of wealth.
  - Applying specific risk-based transaction monitoring rules. Where automated transaction monitoring systems allow it, LFIs should apply specific monitoring rules to all PEPs and Related Customers. These rules should have more sensitive thresholds for alerts, and should also be able to flag transactions between PEPs and Related Customers where both customers maintain accounts with the LFI.
  - Requiring pre-approval for large transactions. It may be appropriate for LFIs to require pre-approval from the compliance function for any transactions representing a substantial portion of the PEP's declared net worth, taking into consideration the size of the LFI and defined risk appetite.

3.3. Transaction Monitoring and Suspicious Transaction Reporting

3.3.1. Transaction Monitoring

As required by Article 7 of the AML-CFT Decision, LFIs must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. As with all customer types, LFIs that use automated monitoring systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD.

Monitoring systems can include manual monitoring processes and the use of automated and intelligence led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the money laundering and financing of terrorism (ML/FT) risks of the institution's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an LFI's business lines or units, where applicable. TM programs should also be calibrated to the size, nature, and complexity of each institution. The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for PEPs customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high risk rating. Please consult also the *CBUAE's Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*[3] for further information.

[3] Available at: centralbank.ae/en/cbuae-amlcft

3.3.2. Suspicious Transaction Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file an STR, SAR or other report types with the UAE Financial Intelligence Unit (UAE FIU) when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. As per Article 18 of the AML-CFT Decision, In reporting their suspicions, employees must maintain confidentiality with regard to both the information being reported and the act of reporting itself, and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorised person (Please consult also section 7.8 of the CBUAE's *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations for Financial Institutions*). STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. STR filings assist law enforcement in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system. Please consult also the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[4] for further information.

[4] Available at: centralbank.ae/en/cbuae-amlcft

3.4. Governance and Training

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. The core of an effective risk-based program is an appropriately experienced AML/CFT Compliance Officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. Additionally, the LFI's senior management must clearly endorse and support the AML/CFT program. As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of PEPs customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. As such, an LFI that has a significant number of PEPs customers should offer training that includes an in-depth discussion of risk factors and "red flags" related to such customers (see Annex 1 below).

Annex 1. Red flags

The following is a list of red flags and indicators for suspicion associated with PEPs.[5] PEPS ATTEMPTING TO SHIELD THEIR IDENTITY:

- Use of corporate vehicles (legal entities and legal arrangements) to obscure the beneficial owner.
- Use of corporate vehicles without valid business reason.
- Use of intermediaries when this does not match with normal business practices or when this seems to be used to shield identity of PEP.

- Use of family members or close associates as legal owner.

RED FLAGS AND INDICATORS RELATING TO THE PEP AND HIS BEHAVIOUR:

- Use of corporate vehicles (legal entities and legal arrangements) to obscure i) ownership, ii) involved industries or iii) countries.
- The PEP makes inquiries about the institution's AML policy or PEP policy.
- The PEP seems generally uncomfortable to provide information about source of wealth or source of funds.
- The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries.
- The PEP is unable or reluctant to explain the reason for doing business in the country of the financial institution or Designated Nonfinancial Business and Profession (DNFBP).
- The PEP provides inaccurate or incomplete information.
- The PEPs seeks to make use of the services of a financial institution or DNFBP that would normally not cater to foreign or high value clients.
- Funds are repeatedly moved to and from countries to which the PEPs does not seem to have ties with.
- The PEP is or has been denied entry to the country (visa denial).
- The PEP is from a country that prohibits or restricts its/certain citizens to hold accounts or own certain property in a foreign country.

THE PEP'S POSITION OR INVOLVEMENT IN BUSINESSES:

- The PEP has a substantial authority over or access to state assets and funds, policies and operations.
- The PEP has control over regulatory approvals, including awarding licences and concessions.
- The PEP has the formal or informal ability to control mechanisms established to prevent and detected ML/FT.
- The PEP (actively) downplays importance of his/her public function, or the public function s/he is relates to associated with.
- The PEP does not reveal all positions (including those that are ex officio).
- The PEP has access to, control or influence over, government or corporate accounts.
- The PEP (partially) owns or controls financial institutions or DNFBPs, either privately, or ex officio.
- The PEP (partially) owns or controls the financial institution or DNFBP (either privately or ex officio) that is a counter part or a correspondent in a transaction.
- The PEP is a director or beneficial owner of a legal entity that is a client of a financial institution or a DNFBP.

RED FLAGS AND INDICATORS RELATING TO THE INDUSTRY/SECTOR WITH WHICH THE PEP IS INVOLVED:

- Arms trade and defence industry.
- Banking and finance.
- Businesses active in government procurement, i.e., those whose business is selling to government or state agencies.
- Construction and (large) infrastructure.
- Development and other types of assistance.
- Human health activities.
- Mining and extraction.
- Privatisation.
- Provision of public goods, utilities.

BUSINESS RELATIONSHIP / TRANSACTION, PURPOSE OF BUSINESS RELATIONSHIP:

- Multiple STRs or other reports have been submitted on a PEP.
- (Consistent) use of rounded amounts, where this cannot be explained by the expected business.
- Deposit or withdrawal of large amounts of cash from an account, use of bank cheques or other bearer instruments to make large payments. Use of large amounts of cash in the business relationship.

- Other financial institutions and DNFBPs have terminated the business relationship with the PEP.
- Other financial institutions and DNFBPs have been subject to regulatory actions over doing business with the PEP.
- Personal and business related money flows are difficult to distinguish from each other.
- Financial activity is inconsistent with legitimate or expected activity, funds are moved to or from an account or between financial institutions without a business rationale.
- The account shows substantial activity after a dormant period; or over a relatively short time; or shortly after commencing the business relationship.
- The account shows substantial flow of cash or wire transfers into or out of the account.
- Transactions between non-client corporate vehicles and the PEP's accounts.
- A PEP is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting transactions.
- A PEP receives large international funds transfers to a gaming account. The PEP withdraws a small amount for gaming purposes and withdraws the balance by way of cheque.
- A PEP uses third parties to exchange gaming chips for cash and vice versa with little or minimal gaming activity.
- A PEP uses multiple bank accounts for no apparent commercial or other reason.

PRODUCTS, SERVICE, TRANSACTION OR DELIVERY CHANNELS:

- Businesses that cater mainly to (high value) foreign clients.
- Trust and company service providers.
- Wire transfers, to and from a PEP account that cannot be economically explained, or that lack relevant originator or beneficiary information.
- Correspondent and concentration accounts.
- Dealers in precious metals and precious stones, or other luxurious goods.
- Dealers in luxurious transport vehicles (such as cars, sports cars, ships, helicopters and planes).
- High-end real estate dealers.

COUNTRY SPECIFIC RED FLAGS AND INDICATORS

- The foreign or domestic PEP is from a higher risk country.
- Additional risks occur if a foreign or domestic PEP from a higher risk country would in his/her position have control or influence over decisions that would effectively address identified shortcomings in the AML/CFT system.
- Foreign or domestic PEPs from countries identified by credible sources as having a high risk of corruption.
- Foreign or domestic PEPs from countries that have not signed or ratified or have not or insufficiently implemented relevant anti-corruption conventions, such as the UNCAC, and the OECD Anti-Bribery Convention.
- Foreign or domestic PEPs from countries with a mono economies (economic dependency on one or a few export products), especially if export control or licensing measures have been put in place.
- Foreign or domestic PEPs from countries that are dependent on the export of illicit goods, such as drugs.
- Foreign or domestic PEPs from countries (including political subdivisions) with political systems that are based on personal rule, autocratic regimes, or countries where a major objective is to enrich those in power, and countries with high level of patronage appointments.
- Foreign or domestic PEPs from countries with poor and/or opaque governance and accountability.
- Foreign or domestic PEPs from countries identified by credible sources as having high levels of (organised) crime.

---

[5] FATF: fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

Annex 2. Synopsis

<table>
<tr><td rowspan="2">Purpose of this Guidance</td><td>Purpose</td><td>The purpose of this Guidance is to assist the understanding and effective performance by licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE relating to PEPs.</td></tr>
<tr><td>Applicability</td><td>This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, stored value facilities, retail payment service providers, card schemes, registered Hawala providers, and other LFIs; and insurance and re-insurance companies, agencies, and brokers.</td></tr>
<tr><td>Understanding Risks</td><td colspan="2">Article 15 of the AML-CFT Decision and the FATF standards impose specific Customer Due Diligence (CDD) obligations on LFIs with respect to Customers that are Politically Exposed Persons (PEPs) which include the Direct Family Members or Associates Known to be Close to the PEPs. The special requirements related to PEPs are not an indication that LFIs should avoid dealing with such customers. Instead, these requirements are meant to ensure that LFIs have done the due diligence necessary to fully identify, understand their customers and have made fully-informed decisions regarding whether or not to accept the customer or to continue the relationship.

There are three sub-groups of PEPs: (1) Domestic PEPs; (2) Foreign PEPs; and (3) Heads of International Organizations (HIOs). PEPs are at higher risk of involvement in crimes because of the powers that come with their position or status. PEPs may use their power or influence to directly enrich themselves, their family members, and their associates, by stealing or misdirecting government funds. Customers that are the direct family members of a PEP, the known close associates of a PEP, or that are legal persons or legal arrangements with at least one beneficial owner who is a PEP are referred to as "Related Customers."

Although LFIs are required to apply special procedures for all PEPs and Related Customers, not all PEPs and Related Customers are equally high-risk. Some factors that can influence the risks of a particular PEP are:

• The PEP's ability to control highly consequential outcomes.
• The authority and independence inherent in the PEP's role or function.
• The access to funds inherent in the PEP's role.
• The nature of governance in the state or organization that has entrusted the PEP with a prominent function.
• The overall level of corruption in the state or organization that has entrusted the PEP with a prominent function.
The sources of risk for a Related Customer can be divided into two broad categories:

• The risk of the PEP to which the Related Customer is connected
• The relationship between the Related Customer and the PEP.</td></tr>
<tr><td>Mitigating Risks</td><td>Legal requirements</td><td>The AML-CFT Decision requires LFIs to carry out specific mandatory due diligence measures on PEPs and Related Customers, in addition to the standard CDD required for all customers. In line with FATF standards, the AML-CFT Decision imposes different requirements on LFIs for foreign PEPs as opposed to domestic PEPs and HIOs.

• For foreign PEPs and Related Customers, LFIs must: (1) Put in place suitable risk management systems to determine whether a Customer or the Beneficial Owner is considered a PEP: (2) obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP; (3) take reasonable measures to establish the source of funds and the</td></tr>
</table>

		sources of wealth of Customers and Beneficial Owners identified as PEPs; and (4) conduct enhanced ongoing monitoring over such relationship. • For domestic PEPs and HIOs and Related Customers, LFIs must (1) Take sufficient measures to identify if their customer or the Beneficial Owner is considered one of those persons and (2) Take the measures identified in (b), (c), and (d) when there is a high-risk business relationship accompanying such persons. LFIs must take reasonable measures to determine whether the beneficiary, or the beneficial owner of a beneficiary, of a life insurance policy or of family takaful insurance is a PEP or a Related Customer. LFIs must inform senior management before pay-out of those policies, or prior to the exercise of any rights related to them. LFIs must also thoroughly examine the overall business relationship.
	Applying Legal Requirements	**Classifying Customers as PEPs:** • The legal definition of PEP specifically lists the roles of persons who always qualify as PEPs, such as Heads of States or Governments, senior politicians, senior government officials, and judicial officials, among others. • However, as there is **no exhaustive list** of the positions that qualify an individual as a PEP globally and LFIs should use their discretion in identifying PEPs and develop **risk-based policies and procedures** to ensure they appropriately identify customers who are PEPs, or the family members or close associates of PEPs. • The determination of whether a customer is a PEP should therefore consider **a number of factors,** including, most importantly, whether the natural person currently holds, or has recently held, a role that gives him or her power or influence over decisions, policy or the disbursal of funds belonging to a government or an international organization. • PEPs are always **natural persons,** and LFIs should perform a PEP analysis on customers who are the beneficial owners of legal persons or legal arrangements.
		Classifying Customers as Related Customers: • LFIs are required to treat the direct family members (spouses, children, spouses of children, and parents) and close associates of PEPs (Natural persons having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP or having individual ownership rights in a legal person or arrangement established in favour of the PEP) as if they were PEPs themselves. • The above-mentioned relationships should be viewed as a mandatory minimum, not as an exhaustive list of all relationships that may justify to treat a customer as a PEP. LFIs should take a **risk-based approach** and consider whether a relationship exists between their customer and the PEP that could be exploited or abused to obscure the PEP's connection to illicit funds. • Once an LFI has established that a qualifying relationship exists between a customer (or the beneficial owner of a customer) and a PEP, the LFI must treat the customer as a PEP (or as owned by a

PEP). However, between a PEP and the direct family member or close associate of a PEP: the latter cannot transfer their status to their own family members and close associates.

Time Limits of PEP Status:

- A PEP's risk derives from the PEP's power or influence over decisions, funds, or policy. Therefore, it may not be appropriate to continue to treat a customer as a PEP long after they have lost such power or influence. While LFIs may set a schedule to review PEP status, they should make a risk-based decision as to when sufficient time has passed for a customer to no longer be classified as a PEP.
- Factors to consider when making such a determination include: the seniority and power inherent in the customer's previous role; the corruption potential of the customer's previous role; whether the customer still exercises informal influence over government decisionmaking through his or her current formal role; whether the previous and current role of the customer are linked in any way; the customer's relationships to other PEPs and the nature and purpose of the business relationship, and the overall risks of the products and services the customer avails or intends to avail.

PEP Screening:

- Classification of a customer as a PEP or a Related Customer should take place during the CDD stage, prior to the commencement of the business relationship. LFIs are required to have suitable risk management systems in place to determine whether a customer, or the beneficial owner of a customer, is a foreign PEP, or Related Customer and are required to take sufficient measures to identify whether a customer, or the beneficial owner of a customer, is a domestic PEP or an HIO, or Related Customer. In practice, however, it will generally be appropriate to conduct onboarding screening and ongoing screening on all customers.
- Preliminary screening may begin by including a question in onboarding forms or interviews that inquires whether the customer or any beneficial owner is a PEP or Related Customer. LFIs should not however rely solely on a customer's assertion, but supplement this basic screening question with additional due diligence.
- LFIs should be alert to any aspects of a customer profile that are inconsistent or do not have a clear explanation. LFIs should use the ongoing monitoring process to determine whether a customer's status has changed.

PEP Risk Rating: Under the AML-CFT Decision, LFIs must conduct enhanced ongoing monitoring over relationships with foreign PEPs and Related Customers. Therefore, it is important to appropriately risk-rate all PEP customers, customers whose beneficial owners are PEPs, and customers that are direct family members and close associates of a PEP. PEP-specific factors to consider in risk rating include: the nature of the PEP's position, and the controls in place in the PEP's own country jurisdiction to prevent corruption. For Related Customers, LFIs should consider the risk of the PEP to which the

		customer is connected, and also the nature and extent of the connection, in determining the risk rating. In cases where a natural person customer has PEP status from two sources, or where more than one PEP is involved in a legal person customer, LFIs should always use the higher risk rating.
		Enhanced Due Diligence Requirements: Under the AML-CFT Decision, when a customer (or the beneficial owner of a customer) is determined to be a foreign PEP or Related Customer, or where a customer is determined to be a domestic PEP or HIO or Related Customer, and when there is a high-risk business relationship accompanying such persons, LFIs must take the following mandatory steps: (1) Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP or Related Customer; (2) take reasonable measures to establish the source of funds, including the source of wealth, of PEPs and Related Customers; and (3) conduct enhanced ongoing monitoring of the relationship.
	Transaction Monitoring and Suspicious Transaction Reporting	**Transaction Monitoring:** As required by the AML-CFT Decision, LFIs must continuously monitor all their transactions to ensure that transactions are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. Monitoring systems can include manual monitoring processes and the use of automated and intelligence led monitoring systems. The transaction monitoring system used by LFIs should be equipped to identify patterns of activity that appear unusual and potentially suspicious for PEP customers as well as unusual behaviour that may indicate that a customer's business has changed in such a way as to require a high-risk rating.
		Suspicious Transaction Reporting: As required by the AML-CFT Law and the AML-CFT Decision, LFIs must file a suspicious transaction report (STR) or suspicious activity report (SAR) or other report types with the UAE Financial Intelligence Unit (UAE Fill) when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime.
	Governance and Training	The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks of PEPs customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls.

Guidance for the Insurance Sector

Effective from 31/10/2022 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations*, as amended, charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding, and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed insurers, agents, and brokers of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for licensed insurers, agents, and brokers to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators identified by the FATF and leading jurisdictional authorities. These are not exhaustive and do not set limitations on the measures to be taken by licensed insurers, agents, and brokers in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, licensed insurers, agents, and brokers should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with licensed insurers, agents, and brokers expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at: centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all insurance and re-insurance companies, agents, and brokers that are licensed and supervised by the CBUAE.

1.3. Legal Basis

This Guidance builds upon the provisions of the following AML/CFT related laws and regulations:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT") and Financing Illegal Organisations as amended by Federal Decree Law No. (26) of 2021 ('AML-CFT Law");
- Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Federal Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations, as amended by Cabinet Decision No. (24) of 2022 ("AML-CFT Decision");
- Insurance Authority's Board of Directors' Decision No. (19) of 2020 Concerning the Guidance Manual for Insurance Companies and Related Professions to Submitting the Data, Information, & Supervisory Reports.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
DNFBP	Designated non-financial business or profession
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FFR	Fund Freeze Report
FIU	Financial intelligence unit
LFI	Licensed financial institution
ML	Money laundering
PEP	Politically exposed person
PNMR	Partial Name Match Report
SAR	Suspicious activity report
SDD	Simplified due diligence
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations
UNSC	United Nations Security Council
UNSCR	UN Security Council Resolution

2. Understanding and Assessing the ML/FT Risks

2.1. Overview of Insurance Sector Activities and Participants

The insurance sector offers a range of products and services to individuals and companies designed to provide a guarantee of compensation for specified loss, damage, illness, or death and facilitate financial planning and risk management in the face of uncertain future events. At the most general level, insurance products can be divided into two categories:

- **Insurance of persons and funds accumulation (hereafter referred to as "life and other investment-related insurance")**, which provides *long-term* coverage against the risk of a future loss, such as death, and may serve as an alternative long-term savings or investment vehicle (e.g., to be paid out upon retirement); and

- **Property and liability insurance (hereafter referred to as "general insurance")**, which provides *shorter-term* coverage against the risk of specific losses, such as damage to property, illness and associated medical expenses, or personal or corporate liability.

Both types of insurance may be offered in the UAE by conventional and Takaful insurance companies. The classes and types of the above-mentioned insurance categories are defined by Articles 3 and 4 of the Executive Regulation[2] of the Federal Law No. (6) of 2007 on the Establishment of the Insurance Authority & Organization of Its Operations as amended by Federal Law No. 3 of 2018 ("Insurance Law")).

Under Article 2.16 of the AML-CFT Decision as amended, **only life insurance and other investment-related insurance products are subject to the UAE's AML/CFT legal and regulatory framework.** It is therefore critical that each licensed insurer, re-insurer, agent, and broker undertakes a comprehensive assessment of its ML/FT risks, including especially the risks associated with its life insurance and other investment-related insurance product offerings, and that it designs and implements an AML/CFT compliance program that is commensurate with those risks.

Insurance sector participants include **operators** in the insurance sector, which sell or facilitate the sale of insurance products and must be licensed by the CBUAE, and **customers** who own, pay for, and/or are covered by or the beneficiaries of insurance products.

Principal insurance sector operators, as defined by the Insurance Law, include:

- **Insurers**, defined as any insurance company incorporated in the UAE or foreign company licensed to carry out insurance operations in the UAE according to the provisions of the Insurance Law, including Takaful insurance companies.
    - *Note: An insurer can issue insurance policies to consumers, or to other insurers or **re-insurers**, in exchange for payment of a premium.*
- **Re-insurers,** defined as any re-insurance company incorporated in the UAE of foreign re-insurance company licensed to carry out insurance operations inside the UAE or a foreign re-insurance company outside the UAE.
    - *Note: Reinsurers are insurers that issue insurance policies to customers that are themselves insurers or reinsurers. Reinsurance includes both "treaty" agreements, which cover broad groups of policies issued by the primary insurer, as well as "facultative" agreements, which cover specific policies or risks, negotiated on an ad hoc basis.*
- **Insurance agents**, defined as any natural or legal person approved and authorized by the insurance company to carry out insurance operations on its behalf or on behalf of any branch thereof.
    - *Note: All insurance agents are "tied" agents, meaning they have a contractual agreement to underwriting and sell insurance products exclusively on behalf of a single insurer. Persons who are contractually free to sell insurance on behalf of multiple insurers or as a freestanding intermediary between insurers and consumers are referred to as insurance brokers, as defined below.*
- **Insurance brokers**, defined as any legal person who independently intermediates in insurance and re-insurance operations between the insurance or re-insurance seeker on one side and any insurance or re-insurance company on the other side and receives for his efforts commission from the insurance company or the re-insurance company with which the insurance or re-insurance has been accomplished.
    - *Note: Insurance brokers can be authorized by multiple insurers to sell insurance products to consumers (or other insurers or reinsurers) on their behalf or to execute insurance sales as freestanding intermediaries between insurers and consumers, in either case in exchange for payment of a commission from the insurer.*

Under the Insurance Law and supporting Insurance Authority Board Resolutions[3], insurance operators also include:

- Health insurance **third-party administrators**, defined as legal persons licensed by the CBUAE to perform health insurance third party administration in accordance with the provisions of the related instructions (e.g. manage health insurance programs and pay health insurance claims on behalf of an insurer);
- **Insurance producers**, defined as natural or legal persons licensed by the CBUAE to practice the profession of marketing insurance policies through ordinary means or electronic means;
- **Price comparison websites** (also referred to as **"insurance aggregators")**, defined as legal persons registered by the CBUAE to provide insurance premium price comparison services using the Internet;
- **Consultants**, defined as natural or legal persons who study the insurance requirements for his customers, give advice in respect of the suitable insurance coverage, assist in preparing the insurance claims along with conducting the other duties specified in the regulation and receive their fees from his customers;[4]

- **Actuaries**, defined as persons who estimate values of the insurance contracts, documents and the related accounts; and
- **Loss and damage adjusters**, defined as persons who examine the damages occurred to the subject matter of the insurance, and assess them.

However, as these participants are not involved or play a very limited role in selling or facilitating the sale of insurance products, and as per Article 2 of the AML-CFT Decision, they are not included under Section 1.2. Applicability of this Guidance.

Principal insurance sector customers include:

- **Policyholders** or **policy owners**, defined as natural persons, legal persons, or legal arrangements who own and maintain the contractual rights of an insurance policy, including powers to inject funds, establish the beneficiary, and exercise early surrender rights. In the case of a group policy, the policyholder is the owner of the master policy.

- **Policy payers**, defined as natural persons, legal persons, or legal arrangements who pay the necessary premium to keep the policy in force.

- **Insured**, defined by the Insurance Law as natural persons, legal persons, or legal arrangements who concluded an insurance contract with the Insurer.

    - *Note: In many cases, the policyholder, policy payer, and insured will be the same person. The insured will also be the person covered by the insurance policy.*

- **Beneficiaries**, defined by the Insurance Law as natural persons, legal persons, or legal arrangements who acquired the rights of the insurance contract at the start or these rights has been legally transferred thereto.

    - *Note: Beneficiaries and other payees are entitled to receive claim payments, distributions, or other payouts under an insurance policy. The payee of a general insurance policy is typically the insured, although certain property insurance policies may specify a third party, such as a lender or lessor with an interest in the covered property, as entitled to all or part of the claim payments on the policy.*[5]

---

[2] Insurance Authority – The Board of Directors' Resolution No.2 of 2009 on Issuance of the Executive Regulation of the Federal Law No.6 of 2007 on Establishment of the Insurance Authority and Organization of the Insurance Operations (Published in the Official Gazette No.504 on 31/01/2010).
[3] Including Insurance Authority Board Resolution No. 9 of 2011 Concerning the Instructions for Licensing Health Insurance Third Party Administrators and Regulation and Control of their Business, Insurance Authority Board of Directors' Decision No. 12 of 2018 Concerning the Regulation on Licensing and Registration of Insurance Consultants and Organization of their Operations, Insurance Authority Board of Directors' Resolution No. 27 of 2020 Concerning the Instructions for Licensing Insurance Producers, and Insurance Authority Board of Directors' Resolution No. 18 of 2020 Concerning the Electronic Insurance Regulations.
[4] Unlike agents and brokers, consultants are not authorized to complete insurance sales (or to "bind coverage") on behalf of an insurer.
[5] A policyholder's **insurable interest** is an interest in the value of the subject of insurance, including any item, event, action, or legal or financial relationship whose loss would cause a financial or other hardship. An insurable interest may result from property rights, contractual rights, or potential legal liability.

2.2. ML/FT Risks Relevant to Life Insurance and other Investment-Related Insurance Products

Criminal actors may use life insurance and other investment-related insurance products to place illicit proceeds into the financial system, especially (though not exclusively) where the insurer or intermediary accepts premium payments in cash. Such products may be purchased with the intention of either holding the insurance policy over its standard duration or canceling coverage before maturity and, where permitted, withdrawing premiums paid less a penalty (a practice known as "early surrender") so as to free up funds for alternative uses. Illicit actors may also deliberately overpay premiums and request a refund for the amount overpaid to the insurance carrier in order to trigger payout under a policy. Reimbursed premiums, withdrawn contributions, and payout proceeds (whether legitimate or fraudulent) can then be deposited into a bank account or used to purchase other financial instruments without necessarily revealing the ultimate origin of the funds.

As noted above, life and other investment-related products are generally considered to present higher ML/FT risk, particularly where they have high cash values upon surrender. The following methods may be employed to launder funds through life insurance and other investment-related insurance products or relationships:

- Assigning policies and payments to third parties, especially through policies (such as secondhand endowment and bearer insurance policies) that allow the policyholder to change the beneficiary before maturity or surrender without the knowledge or consent of the insurer;
- Borrowing against the cash surrender value of permanent life insurance policies or using a policy as collateral to purchase other financial instruments;
- Selling units in investment-linked products, such as annuities;
- Buying products with insurance termination features without concern for the product's investment performance; and
- Establishing fictitious insurance or reinsurance companies or intermediaries in order to place or move illicit proceeds without revealing the true source of funds.

In addition to these vulnerabilities, the insurance sector is also vulnerable to abuse from other types of economic crime, particularly orchestrated fraud. Moreover, even where insurance products or relationships are not directly abused to launder money or perform other illicit transactions, insurance may be purchased by illicit actors to provide an appearance of legitimacy to the underlying, insured activities. As per Article 11.2 of the AML-CFT Decision, **LFIs must consider the customer and the beneficiary of life insurance and family Takaful policies as risk factors when determining the applicability of enhanced due diligence procedures (EDD).**

The remainder of this section presents additional examples of key ML/FT risk factors relevant to the insurance sector for life insurance and other investment-related insurance products, organized by risks related to insurance products, services and transactions, distribution channels and intermediaries, customers, and geographies. These should be considered by insurance sector operators when performing their financial crimes risk assessments (see section 3.1) and determining the risks presented by specific customers or business activities. Individual risks may be heightened in view of the UAE's national and regional circumstances and the composition of the local insurance sector. Where a risk factor is coupled with one or more of the red flag indicators provided in Annex 1 of this Guidance, insurance sector operators should consider assigning additional resources or controls to the area of heightened risk, such as by applying enhanced due diligence ("EDD") or heightened ongoing monitoring.

Insurance operators are expected to perform and document an enterprise ML/FT risk assessment and keep the risk assessment up to date given material changes to their risk profile or legal, regulatory, or supervisory environment. Additional details on the enterprise risk assessment process and the use of risk assessment findings to support a risk-based approach are provided in section 3.1.

2.2.1. Product Risk Factors

Product risk is assessed by identifying how vulnerable a product is to money laundering and terrorist financing based on the product's design. Product risk should be assessed periodically and when significant changes are made to product offerings, including the development of new products, services, or technologies. Product risk is a significant factor in identifying unusual activity.

The following table describes attributes used to assess the vulnerability of product offerings and provides lower-and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Ability to hold funds or transact large sums	Product design that does not hold a balance or cannot be withdrawn against, such as group benefits	Product design that allows funds to be held on behalf of the customer; high-value or unlimited-value premium payments, overpayments, or large volumes of lower-value payments
Customer anonymity or third-party transactions	Product design that only allows transactions from customers with identification, or where all funds flow back to the customer	Product design that allows deposits and payments by third parties or that provides for non-face-to-face transactions (e.g., mobile apps where payment source is unknown)
Liquidity	Product design that does not permit withdrawals or includes significant fees or other penalties for early withdrawals	Product design that has no (or no significant) fees or other penalties for early withdrawal
Time horizon	Products that are typically held for a long period of time, such as years, until retirement or death	Products that are typically held for a shorter time period
Purpose or intended use of the product	Product design makes it easy to identify if products are not being used as intended	Product design makes it difficult to identify if products are not being used as intended

2.2.2. Service and Transaction Risk Factors

Service and transaction risk can be assessed by identifying how vulnerable a product is to use by a third party or unintended use based on the methods of transaction available. Service and transaction risk is influenced by product design. Understanding potential service and transaction risks in the business is a significant factor in recognizing unusual activity at a customer level.

The following table describes attributes used to assess service and transaction risk and provides lower-and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Difficulty in tracing ownership of funds	Preprinted checks, bill payments, and electronic funds transfer (EFT) payments with verified banking records	Cash, bank drafts in bearer form, travelers checks, counter checks (where ownership information is handwritten or typed in a different font than the rest of the check), and potentially some digital currencies
The customer is not the payer or recipient of the funds	The funds are moved from or to another financial institution	The third-party paying or receiving funds has not previously been disclosed
Payment source or recipient is based outside of the country	The recipient or payer is the policyholder and is in a low-risk	The recipient or payer is the policyholder and is in a higher-risk

	country	country or is a third party outside the country (making it more difficult to trade or confirm the source of funds)
Number of transactions	The low number of transactions or transaction frequency that is typical for the product	A large number of transactions back and forth with the customer or third parties, especially where it exceeds typical usage for the product
Transactional patterns	Regular and expected customer account activity	Significant, unexpected, and unexplained change in the customer's typical activity, such as early surrenders or withdrawals where such service is offered

2.2.3. Distribution Channel and Intermediary Risk Factors

The distribution channel is the method a customer uses to open a new policy or account. The distribution channel risk is identified by assessing how vulnerable the channel is to money laundering or terrorist financing activities based on attributes that may make it easier to obscure customer identity.

The risk of failing to identify a customer correctly may be higher for distribution channels that use an intermediary or do not require face-to-face contact. Depending on the product, distribution channel risk may be mitigated by using distributors who are also subject to AML/CFT obligations or a pension scheme subscribed through the customer's employer.

The following table describes attributes used to assess the vulnerability of distribution channels and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
The distributor has AML/CFT obligations	The distributor is overseen by a regulatory authority and subject to AML/CFT laws equivalent to or stronger than the insurer	Distributor is not subject to AML/CFT requirements
Payment to an insurer	Customer pays the insurer directly from their account at a bank or securities dealer	The customer pays the distributor, who then pays the insurer
The direct relationship of customer to insurer	Tied agents, brokers, and banking consultants; products distributed directly by insurers	Non-face-to-face relationships[6] with insurers or agents (e.g., trusts or insurance sold by telephone or online without adequate safeguards for confirmation of identity)

[6] As discussed in section 3.3.1.5 below, relationships in which personal contact between an insurer or agent and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships.

2.2.4. Customer Risk Factors

Customer-based risk factors are assessed to evaluate the level of vulnerability to ML/FT threats posed by customers based on their characteristics. Understanding the inherent risks enables an insurer, agent, or broker to identify appropriate mitigating controls and manage residual risks. Customer risk factors combined with business risk factors can be used as criteria for risk scoring to identify high-risk customers. Such risk factors include:

- Customer identity;
- Third-party involvement;
- Customer's source of wealth or funds;
- Customers who are politically exposed persons ("PEPs"), including the direct family members and close known associates of a PEP, and legal entities where at least one beneficial owner is a PEP; and
- Known criminals, terrorists, or persons on sanctions lists.[7]

The following table describes attributes used to assess customer risks and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Identification	Customer provides identification or can be identified using third-party sources.	Customer has difficulty producing identification, or the authenticity of the identification provided is questionable
Third-party relationships	No third-party involvement	Customer is controlled by a third party, or there are multiple indicators of third-party deposits or payments; customer is controlled by a gatekeeper (such as an accountant, lawyer, or other professional holding accounts or contracts at the insurer) without any interaction with the beneficial owner
Customer's legal form	Customer is a living person or is a large, publicly-traded legal entity with clear ownership and control	Customer is a legal entity with a complex structure where it is difficult to ascertain those who own or control the entity; policyholder and/or beneficiary are companies with nominee shareholders and/or shares in bearer form
Occupation, business type, or another source of wealth or funds	Customer's business type or occupation is in a lower-risk industry	Customer's business or occupation is in a higher-risk industry (such as a cash-intensive business or an industry that has extensive international exposure or is associated with crime typologies) or is associated with a lower income for a high-value deposit without a confirmed source of funds or wealth (such as inheritance or real estate)
Depth and duration of relationship with customer	Customer has a long history with the insurer or its agents and additional information is on file (such as credit underwriting, insurance underwriting, customer due diligence, etc.)	Customer is new to the insurer or insurer has little or no experience with the customer
Customer only holds accounts with lower risk products and services	Customer holds policies or accounts that are registered with the government, such as a registered retirement savings plan	Customer only holds non-registered policies or accounts (e.g., investment or bank accounts with an affiliate)
Political exposure	Customer does not have any ties to politically exposed persons	Customer is considered a politically exposed person, particularly from a

		foreign jurisdiction
Other screening results	Customer does not have negative news media or media confirms what is known about the customer (such as career confirmation or community engagement)	Customer has ties to or is on a designated sanctions list; has a history of predicate offenses; or is associated with negative news

[7] Please see section 3.5 below and also refer to the Executive Office's "*Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction":* available at uaeiec.gov.ae/en-us/un-page?p=2#

2.2.5. Geographic Risk Factors

A customer's geographic location or connections may indicate a higher risk for ML/FT activities. To mitigate risk, controls are recommended based on domestic and international geographic risk factors. Where available, data from internal insurer historical case experiences or government data based on crimes applicable to ML or predicate offenses can be used to inform the assessment of domestic geographical risk. Customer risk is higher among customers with connections outside the country, especially connections to higher-risk countries. According to the National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates, the regions and jurisdictions most often involved in criminal activity in relation to the UAE were Pakistan, India, Iran, Bangladesh, China, Russia, South Africa, Nigeria, Somalia, Lebanon, Yemen, Syria, Iraq, Afghanistan, and North Africa. The following table describes attributes used to assess geographic risks and provides each's lower- and higher-risk examples.

Attribute	Lower-risk example	Higher-risk example
Higher-crime regions	Customer does not reside in a region with higher frequency and severity of crimes with ML risk, based on the insurer's own risk assessment (utilizing historical case experiences or government data where appropriate)	Customer resides in a region with high frequency and severity of crimes with ML risk, based on the insurer's own risk assessment (utilizing historical case experiences or government data where appropriate)
History high-risk activity or fraud	Customer does not reside in a region that experiences a higher incidence of high-risk activity or fraud	Customer resides in a region that experiences a higher incidence of high-risk activity or fraud
Foreign tax or physical residency of customer	Countries risk rated as low by the insurer	Countries risk rated as high by the insurer
Foreign ties or transactions	Customer does not have any indicators of foreign residency or transactions outside of country	Customer has requested or performed transactions with ties to high-risk countries, including especially those on the NAMLCFTC's and FATF's lists of high-risk jurisdictions subject to a call for action and jurisdictions under increased monitoring.

3. Mitigating Risks

The sections below discuss how insurance operators can apply preventive measures to identify, assess, manage, and mitigate the risks associated with the insurance sector for life insurance and other investment-related insurance products. This is not a comprehensive discussion of all AML/CFT requirements imposed on insurance sector

participants; insurers, agents, and brokers should therefore consult the UAE legal and regulatory framework currently in force.

The controls discussed below should be integrated into each institution's larger AML/CFT compliance program and supported by appropriate governance, training, and independent audit. As discussed in section 3.6 below, insurers are permitted to delegate the performance of specified controls to insurance agents, brokers, banks, or other intermediaries, using either a **third-party reliance** or an **outsourcing** model.

- Under a **third-party reliance** model, insurers may rely on any third-party LFI, such as a bank, insurance agent, or insurance broker, to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, following *the third party's* AML/CFT policies and procedures. In such circumstances, the third party will usually have an existing business relationship with the customer, which is independent of the relationship to be formed by the customer with the relying institution. The third-party reliance model is most commonly employed in the case of insurance brokers, who sell insurance products to consumers on behalf of multiple insurers and therefore typically maintain and apply their own AML/CFT policies and procedures.
- Under an **outsourcing** model, by contrast, insurers may engage a third-party service provider, such as an insurance agent, broker, or other intermediaries, to apply some or all of the AML/CFT preventive measures described in this section on behalf of the delegating institution, following *the insurer's* AML/CFT policies and procedures. In an outsourcing scenario, the third party is subject to the delegating insurer's control regarding the effective implementation of those policies and procedures by the outsourcing entity. The outsourcing model is most commonly employed in the case of tied agents, who sell insurance products to consumers exclusively on behalf of a single insurer and therefore typically follow the insurer's AML/CFT policies and procedures.

Under either model, **the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures** (including maintaining the availability of all relevant data and records), and the arrangement must satisfy the conditions set forth in section 3.6 below.

3.1. Risk-Based Approach and Enterprise Risk Assessment

Under article 4 of the AML-CFT Decision, the insurance operator is required to perform, document, and keep up to date an enterprise risk assessment for the purposes of identifying, assessing, and understanding its ML/FT risks for life insurance and other investment-related insurance products, including those arising in relation to its:

- Products;
- Services and transactions;
- Distribution channels and intermediaries;
- Customers; and
- Geographies, in terms of both the jurisdictions or regions in which has operations and the jurisdictions or regions in which its customers are located or do business.

The insurance operator is expected to document the methodology and findings of the risk assessment, considering all relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied. Insurance operators must keep their risks assessments up to date and ensure that identified risks are within the institution's risk appetite and that identified deficiencies are appropriately tracked and remediated. Risk assessments should provide a consolidated assessment of the insurance operator's ML/FT risks across all business units, product lines, and delivery channels, including those of branches, subsidiaries, parent entities, or other affiliates located outside the UAE.

ML/FT risk factors relevant to the insurance sector for life insurance and other investment-related insurance products can be found in section 2.2 above, and red flag indicators for the UAE insurance sector are provided in Annex 1. Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 4[8] for further information.

[8] Available at: centralbank.ae/en/cbuae-amlcft.

3.2. New Products, Practices, and Technologies

Under Article 23 of the AML-CFT Decision, an insurance operator is required to identify and assess the ML/FT risks for life insurance and other investment-related insurance products that may arise in relation to:

- The development of new products and new business practices, including new delivery mechanisms (such as mobile insurance applications, insurance portals, transaction terminals, and insurance booths); and
- The use of new or developing technologies for both new and preexisting products.

An operator must undertake such risk assessments prior to the launch or use of new products, practices, and technologies and must take appropriate measures to manage and mitigate the identified risks. Operators should pay special attention to new products, practices, or technologies that favor anonymity.

3.3. Customer Due Diligence

3.3.1. General CDD Measures

For life insurance and other investment-related insurance products, insurance operators must perform customer due diligence ("CDD") on their customers, defined as natural persons, legal persons, or legal arrangements with whom an insurer, agent, or broker establishes or intends to establish a business relationship to carry out insurance operations, as defined in Articles 4 and 5 of the Insurance Law.

Unless otherwise specified below, the customer of an insurance operator is the existing or prospective **policyholder**, defined as the *natural person, legal person, or legal arrangement* who owns and maintains the contractual rights of the insurance policy. Where the insurer is acting as a reinsurer, the customer will be the insurer (or reinsurer) in whose name the reinsurance policy is issued. Additionally, in the case of group life insurance or other policies, when the insured persons have active powers on the contract (e.g., to inject sums into the contract, establish the beneficiary, or exercise early surrender of the amounts), those persons should be considered equal to customers, and life insurers and relevant intermediaries should therefore conduct CDD on these persons, as well as on their related third parties. In cases where the insured persons have no active powers, their names should be screened against sanctions lists, but they are not considered customers for AML/CFT purposes, and insurers and intermediaries are not required to conduct full CDD checks on them.

Finally, although in most cases the policyholder will also be the party who pays the necessary premium to keep the policy in force, there may be exceptional cases in which the policy payer is an unrelated third party (referred to as a **third-party payer**). In such cases, the insurer—or its agent, under a third-party reliance or outsourcing arrangement, if applicable—should perform the following general CDD measures on *both* the policyholder and the third-party payer.

3.3.1.1. Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, insurance operators are required to identify and verify the identities of all customers. Customers should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, as per Article 4.3 of the AML-CFT Decision, where there is no ML/FT suspicion and ML/FT risks are assessed to be low, an operator may complete the verification of the customer's identity after establishing a business relationship, as set forth in section 3.3.3 below.

When verifying the Emirates ID card either physically, by way of digital or electronic Know Your Customer (e-KYC) solutions, the insurance operator must use the online validation gateway of the Federal Authority for Identity & Citizenship, Customs & Port Security, the UAE-Pass Application or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than the Emirates ID are

used in the KYC process, a copy must be physically obtained from the original passport which must be certified (i.e. certified copy) as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.

Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.1, for further information.

3.3.1.2. Beneficial Owner Identification and Verification

Under Article 9.1 of the AML-CFT Decision, insurance operators are required to identify and verify the identities of all beneficial owners of any legal person customer, defined as all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25 percent or more. Where no individual meets this description, the operator is required to identify and verify the identity of the individual(s) holding the senior management position in the entity. This option should be used only as a last resort, however, and when the operator is confident that no one individual, or small group of individuals, exercises control over the customer.

Under Article 9.2 of the AML-CFT Decision, for legal arrangements, insurance operators must verify the identity of the settlor, the trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement and obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment, or at the time he/she intends to exercise his/her legally acquired rights. The beneficial owner of a legal person or arrangement must be an individual. Another legal person cannot be classified as the beneficial owner of a customer, no matter what percentage it owns. Insurance operators should continue tracing ownership all the way up the ownership chain until it identifies all individuals who own or control at least 25 percent of the operator's customer. If the insurance operator has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the operator should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so for legal person is to identify additional beneficial owners below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10 percent or even the 5 percent level, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD— in order to conduct sanctions screening or negative news checks.

Beneficial owners should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, pursuant to Article 4.3 of the AML-CFT Decision, where there is no ML/FT suspicion and ML/FT risks are assessed to be low, an operator may complete verification after establishing a business relationship, as set forth in section 3.3.3 below.

Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.3.1 and 6.3.3, respectively, as well as the *CBUAE's Guidance for LFIs providing services to Legal Persons and Arrangements*[9] for further information.

[9] Available at: centralbank.ae/en/cbuae-amlcft.

3.3.1.3. Understanding the Nature of the Customer's Business and the Nature and Purpose of the Business Relationship

Under Article 8 of the AML-CFT Decision, insurance operators are required to understand the nature of the customer's business and the nature and purpose of the operator's relationship with the customer, including the expected uses to which the customer will put the operator's products or services. This step requires the operator to collect information that allows it to create a profile of the customer, including the types and volumes of transactions the customer is expected to engage in, and to assess the risks associated with the relationship. In certain instances,

the expected type and volume of transactions are implicit in the specific insurance product being provided, in which case this aspect of the customer's profile can be derived directly from the product choice.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship—together with the ongoing analysis of actual customer behavior and the behavior of relevant peer groups—allows the insurance operator to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. This element of CDD can also serve to inform the operator's risk rating or other risk assessment of the customer for the purposes of performing risk-based ongoing monitoring (see section 3.3.1.4) and determining whether simplified or enhanced due diligence measures may be warranted (see sections 3.3.3 and 3.3.4, respectively).

3.3.1.4. Ongoing Monitoring

Under Article 12 of the AML-CFT Decision, insurance operators are required to subject all customers to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the operator's products and services are being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

Insurance operators are required to ensure that the CDD information they hold on all customers is accurate, complete, and up to date. This is particularly crucial in the context of customers that are companies or that engage in business. Operators should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular should ascertain that:

- The customer's beneficial owners remain the same;
- The customer continues to have active status with a company registrar;
- The customer has the same legal form and is domiciled in the same jurisdiction; and
- The customer is engaged in the same type of business and in the same geographies.

In addition to a review of the customer's CDD file, under Article 7 of the AML-CFT Decision, the operator must also review the customer's transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. It must determine whether they continue to fit the customer's profile and business and are consistent with the business the customer is expected to engage in when the business relationship was established. This type of transaction review is distinct from the transaction monitoring discussed in section 3.4 below and its purpose is to complement it by identifying behaviors, trends, or patterns that are not necessarily subject to transaction monitoring rules. The techniques used for transaction review will vary depending on the customer. For lower-risk customers, a review of alerts, if any, is likely to be sufficient. For higher-risk customers, a more intensive review may be necessary. For customers with a large volume of transactions, operators may use data analysis techniques.

If the review finds that the customer's behavior or information has materially changed, the operator should risk-rate the customer again. New information gained during this process may cause the operator to determine that EDD is necessary or may bring the customer into the category of customers for which EDD is mandatory (i.e., customers that are PEPs, or owned or controlled by PEPs, the direct family members or associates known to be close to the PEPs; customers that are based in high-risk jurisdictions; etc.).

Operators may consider requiring that the customer update them on any changes in its beneficial ownership or business activities. Even if this requirement is in place, however, operators should not rely on the customer to notify it of a change but should still update CDD on a schedule appropriate to the customer's risk rating.

3.3.1.5. Non-Face-to-Face Relationships

Insurance operators should develop policies and procedures to address any specific risks associated with non-face-to-face customer relationships and transactions undertaken in the course of such relationships. Such policies and procedures should be applied when establishing a new customer relationship and when conducting ongoing monitoring, and should be at least as stringent as those that would be required to be performed if there was face-to-face contact.

- *Note: Relationships in which personal contact between an insurer or agent and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships for the purpose of this Guidance.*

Heightened ML/FT risks may arise from establishing business relationships or undertaking transactions according to instructions conveyed by customers over the internet (absent personal contact via video teleconference), post, fax, or telephone. An operator should note that online applications and transactions may pose greater risks than other non-face-to-face business due to the following factors, which taken together may compound the associated ML/FT risks:

- The ease of unauthorized access to the facility, across time zones and locations;
- The ease of making multiple fictitious applications without incurring additional cost or the risk of detection;
- The absence of physical documents; and
- The speed of electronic transactions.

The measures taken by an insurance operator for verifying the identity of customers and beneficial owners in the context of non-face-to-face relationships will depend on the nature and characteristics of the product or service provided and the customer's risk profile. Where verification of identity is performed without face-to-face contact (e.g., electronically), an operator should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the operator routinely undertakes as part of its existing procedures, which may include as appropriate and feasible:

- Telephone contact with the customer at a residential or business number that can be verified independently;
- Confirmation of the customer's address through an exchange of correspondence or other appropriate method;
- Subject to the customer's consent, telephone confirmation of the customer's employment status with his or her employer's human resource department at a listed business number of the employer;
- Confirmation of the customer's salary details by requiring the presentation of recent bank statements where applicable;
- Provision of certified identification documents by lawyers or notaries public;
- Requiring the customer to make an initial premium payment using a check drawn on the customer's personal account with a bank in the UAE; and
- Video call with the customer.

3.3.1.6. Name Screening

An insurance operator should screen the following parties against relevant ML/FT information sources (such as negative media databases) and internal watchlists (such as lists of customers previously exited for financial crime

reasons) prior to a customer's onboarding:

- All customers, regardless of risk rating or risk profile;
- Beneficial owners of legal entity customers;
- Natural persons appointed to act on behalf of the customer (see section 3.3.2.1);
- Directors, partners, and managers of customers that are legal persons;
- Natural persons having executive authority over customers that are legal arrangements; and
- Insured with no active powers on the contract (if any).

With respect to sanctions lists, the parties listed above must be screened prior to a customer's onboarding and on an ongoing basis thereafter (please see section 3.5 below). In addition, *at the time of payout*, an insurer must screen against sanctions lists and should screen against the same other lists and information sources all beneficiaries or other payees and their beneficial owners (where applicable).

The results of screening and assessment by the insurance operator should be documented. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*[10] for further information.

---

[10] Available at: centralbank.ae/en/cbuae-amlcft.

3.3.1.7. Customer Rejection and Exit

Insurance operators should not deal with any person on an anonymous basis or any person using a fictitious name. Prior to establishing an insurance relationship, if an insurance operator has any reasonable grounds to suspect that the assets or funds of a customer are the proceeds of crime or related to the financing of terrorism, the operator should reject the business relationship and, per Article 17 of the AML-CFT Decision, file a suspicious transaction report ("STR") with the UAE Financial Intelligence Unit ("FIU").

As per article 13 of the AML-CFT Decision, where an insurance operator is unable to undertake the CDD measures described above, or is a confirmed match to a party included on applicable sanctions lists, the insurance operator must:

- Not onboard the customer;
- Exit the relationship if one has been established;
- Not make any payment to a payee or beneficiary under the customer's policy or other insurance relationship; and
- Maintain the related records (Please see Section 3.10 below).

In addition, it should add the customer, its beneficial owners, directors, and managers to internal watchlists. The operator should also determine whether the circumstances warrant the filing of a suspicious transaction report ("STR") or SAR.

3.3.2. Specific CDD Measures for Insurers

In addition to performing general CDD on their customers, insurers are also expected to collect and verify the identities of any natural persons appointed to act on the customer's behalf and are required, under Article 11 of the

AML-CFT Decision, to collect and verify the identities of the beneficiaries or other payees of an insurance policy and their beneficial owners (where applicable), as set forth below.

3.3.2.1. Identification and Verification of Natural Persons Appointed to Act on a Customer's Behalf

As per Article 8.2 of the AML-CFT Decision, where a customer appoints one or more natural or legal persons (such as an insurance broker) to act on his, her, or its behalf in establishing a business relationship with an insurer, the insurer must identify and verify the identity of each such natural person in accordance with the same procedures used to identify and verify the identity of a natural person customer. The insurer should also verify the due authority of each natural person appointed to act on behalf of the customer by obtaining, at a minimum:

- The appropriate documentary evidence authorizing the appointment of such natural or legal person by the customer to act on his, her, or its behalf; and

- The signature of such a natural or legal person appointed.

As with customers, natural persons appointed to act on a customer's behalf should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, where there is no ML/FT suspicion, and ML/FT risks are assessed to be low, and where the deferral of verification is essential in order not to interrupt the normal course of business operations, an operator may complete the verification of the appointed person's identity after establishing a business relationship, as set forth in section 3.3.3 below.

3.3.2.2. Identification and Verification of Beneficiaries or Other Payees and Their Beneficial Owners

Under Article 11.1 of the AML-CFT Decision, insurers are required to conduct CDD measures, including ongoing monitoring, with respect to any beneficiary of life insurance and other investment insurance insurance products, including life insurance products relating to investments and family Takaful insurance, as soon as the beneficiary is identified or designated. In addition, *as soon as a beneficiary or other payee is designated*, an insurer must perform the following:

- For a beneficiary or payee who is identified as a specifically named natural person, legal person, or legal arrangement, obtain the full name, including any aliases, of such beneficiary or payee; or
- For a beneficiary or payee who is designated by characteristics, class, or other means, obtain sufficient information concerning the beneficiary or payee to satisfy itself that it will be able to establish the identity of such beneficiary or payee at the time of payout.
- *At the time of payout*, insurers must also verify the identities of all beneficiaries or payees and their beneficial owners in accordance with the same procedures used to identify and verify the identity of a natural person customer.

3.3.3. Simplified Due Diligence for Lower-Risk Scenarios

As per Article 4.3 of the AML-CFT Decision, an insurance operator may perform simplified due diligence ("SDD") measures in relation to a customer, a beneficial owner of a customer, a natural person appointed to act on behalf of a customer, or a beneficiary or other payee if it is satisfied that the risks of ML/FT are low. The assessment of low risks should be supported by an adequate analysis of risks by the insurance operator, and the selection of simplified measures should be commensurate with the type and level of risk identified through such risk analysis. In all cases, the operator should document the details of its risk analysis and the nature of the SDD measures employed.

Examples of potentially lower-risk scenarios include, but are not limited to, those in which:

- The customer is a UAE government entity, including UAE state-owned enterprises;
- The customer is an entity listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency with respect to beneficial owners;
- The insurance product does not offer cash payouts except upon the occurrence of specified trigger events;
- The insurance product does not have an early surrender option and cannot be used as collateral; or
- The insurance product is a pension or other scheme where contributions are made via deduction from wages and scheme rules and do not permit the assignment of a member's interest under the scheme.

Additional examples of lower-risk attributes for the insurance sector are provided in section 2.2 above.

Where an insurance operator is satisfied that the ML/FT risks are low, the operator may perform one or more of the following SDD measures, as warranted by the risk analysis:

- Verifying the identity of the customer and any beneficial owner(s) after establishing the business relationship, provided verification is nonetheless completed in a timely fashion (to be documented in the operator's internal procedures) and appropriate controls are in place to manage the ML/FT risks associated with the customer and the relationship prior to verification;[11]
- Reducing the frequency of updates to CDD information;
- Reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
- Developing an understanding of the intended nature and purpose of the customer relationship on the basis of the relationship type and the customer's historical transaction activity, rather than by collecting information regarding the intended nature and purpose of the relationship during onboarding or CDD updating.

An insurance operator should not perform SDD measures where:

- A customer or any beneficial owner of the customer is from or in a country or jurisdiction against which the FATF has called for countermeasures;
- A customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the operator for itself or notified to operators generally by local regulatory or supervisory authorities; or
- The operator suspects that ML or FT is involved.

---

[11] Such measures may include holding funds in suspense or escrow until verification of identity has been completed or making completion of identity verification a precondition of closing any transaction with or on behalf of the customer.

3.3.4. Enhanced Due Diligence for Higher-Risk Scenarios

The AML-CFT Law and the AML-CFT Decision impose specific and enhanced due diligence obligations on insurance operators with respect to two classes of customers or transactions:

- Customers that are politically exposed persons ("PEPs"), which include the direct family members or associates known to be close to the PEPs; and

- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries.

The AML-CFT Law and Decision give special attention to customers in these groups because they are likely to expose operators to a heightened risk of money laundering, terrorism financing, and other illicit finance.

In addition to these classes of customers and transactions, for which EDD is mandatory, operators are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken

for or on behalf of a customer present a higher risk for ML or FT. Examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The customer belongs to a higher-risk industry or sector identified in topical risk assessments, or to an industry or sector identified by the operator as higher-risk for ML or FT;
- The ownership structure of a legal entity customer appears unusual or excessively complex given the nature of the legal entity's business;
- The legal entity customer is a personal asset-holding vehicle;
- The business relationship is conducted under unusual circumstances, such as significant unexplained geographic distance between the operator and the customer;
- The legal entity customer has nominee shareholders or shares in bearer form;
- The customer is a cash-intensive business;
- The customer operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, or inadequate AML/CFT measures, as identified by the FATF;
- The customer operates in or does business with a jurisdiction identified by credible bodies (e.g., reputable international bodies such as Transparency International) as having significant levels of corruption, terrorism financing, or other criminal activity;
- The relationship involves or could involve cash or anonymous transactions;
- The relationship involves or could involve frequent payments received from unknown or unassociated third parties.

Additional examples of higher-risk attributes and red flag indicators for the insurance sector are provided in section 2.2 and Annex 1 of this Guidance respectively.

As per Article 4.2 b) of the AML-CF Decision, where the operator identifies a customer or relationship as presenting higher ML/FT risks, it must apply EDD measures commensurate with those risks. Examples of EDD measures include but are not limited to:

- Obtaining approval from the operator's senior management to establish or continue a business relationship with the customer, including making any payment to a beneficiary or payee;
- Establishing the source of wealth and source of funds of the customer and any beneficial owner of the customer;
- Conducting enhanced monitoring during the course of the business relationship with the customer, including by increasing the degree and nature of transaction monitoring and CDD updating;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar or equivalent CDD standards;
- Using public sources of information (e.g., websites) to gain a better understanding of the reputation of the customer or any beneficial owner of the customer;

- Commissioning external intelligence reports where it is not possible for the operator to easily obtain information through public sources or where there are doubts about the reliability of public information; and

- For high-net-worth individuals, particularly those utilizing higher-risk products or services or characterized by other markers of heightened ML/FT risk:

    - Independently corroborating information obtained on the source of wealth of customers and beneficial owners against documentary evidence or public information sources;

    - Screening operating companies and individual benefactors contributing to the customer's and beneficial owner's wealth or funds; and

    - Scrutinizing transactions relating to customers that have multiple policies with the operator or to customers having a common beneficial owner.

In addition, as noted in section 3.3.1.2 above, if the insurance operator has followed its standard beneficial ownership identification and verification procedures and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the operator should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so is to identify additional beneficial owners below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10 percent or even the 5 percent level, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

Additional examples of EDD measures are provided in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.4.

3.4. Transaction Monitoring and Suspicious Transaction Reporting

3.4.1. Transaction Monitoring

Under Article 16 of the AML-CFT Decision, insurance operators must monitor activity by all customers to identify behavior that is potentially suspicious and that may need to be the subject of an STR or SAR when conducting operations related to life insurance and other investment-related insurance products. Transactions may be suspicious simply in virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries) or because, together with other transactions, they form a pattern that diverges from expected or historical transactional activity or may otherwise be indicative of illicit activity, including the evasion of reporting or recordkeeping requirements. When monitoring and evaluating transactions, the operator should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. In addition, higher-risk customers should be subject to more stringent transaction monitoring, with lower thresholds for alerts and more intensive investigation.

Transaction monitoring can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/FT risks of the operator's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an operator's business lines or units, where applicable.

Transaction monitoring programs should also be calibrated to the size, nature, and complexity of each institution. Operators with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. Operators utilizing automated systems should perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and

processes. While smaller operators may rely on transaction monitoring systems that are less automated, they should still ensure that these are appropriately executed to address the risks from their day-to-day transactional activity.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information.

3.4.2. STR Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, insurance operators must file without any delay an STR or SAR with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. STR/SAR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. STR/SAR filings are essential to assisting law enforcement authorities in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an operator suspects that a transaction or funds are linked to a crime, operators should consider filing an STR or SAR in the following situations involving higher-risk customers:

- A potential customer decides against purchasing financial services after learning about the operator's CDD requirements;
- A current customer cannot provide required information (including documentation) about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- The operator is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the operator should not establish the business relationship, or continue an existing business relationship; or
- Other situations that are suspicious or involve activity with no legitimate business or other lawful purpose.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[12] for further information.

[12] Available at: uaeiec.gov.ae/en-us/un-page.

3.5. Sanctions Obligations and Freezing Without Delay

The AML-CFT Law and AML-CFT Decision require insurance operators to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision No. (74) of 2020 sets out the legislative and regulatory framework regarding the Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List. As per Cabinet Decision 74 and in particular its Article 15, **all insurance operators without any exception,** are obliged to apply policies, procedures and controls to implement TFS to those sanctioned and designated in the Local Terrorist List and the UN Consolidated List.

For more information and details on their obligations in relation to their sanctions obligations, insurance operators should consult the Executive Office for Control and Non-Proliferation (former Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's – referred to as the Executive Office) "*Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions*"[13]; the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions* as well as the CBUAE*'s Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions*

screening and any of their amendments or updates thereof. Insurance operators should also consult the CBUAE's and the Executive Office's websites as updated from time to time, and refer to the Executive Office's list of Frequently Asked Questions (FAQ) for the insurance sector.

[13] Available at: uaeiec.gov.ae/en-us/un-page.

3.6. Third-Party Reliance and Outsourcing

As noted above, insurers are permitted to delegate the performance of specified controls to insurance agents or other intermediaries, using either a **third-party reliance** or an **outsourcing** model.

- Under a **third-party reliance** model, insurers may rely on any third-party LFI, such as a bank or insurance agent or broker, to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, following *the third party's* AML/CFT policies and procedures. In such circumstances, the third party will usually have an existing business relationship with the customer, which is independent of the relationship to be formed by the customer with the relying institution. The third-party reliance model is most commonly employed in the case of insurance brokers, who sell insurance products to consumers on behalf of multiple insurers and therefore typically maintain and apply their own AML/CFT policies and procedures.
- Under an **outsourcing** model, by contrast, insurers may engage a third-party service provider, such as an insurance agent or other intermediary, to apply some or all of the AML/CFT preventive measures described in this section on behalf of the delegating institution, following *the insurer's* AML/CFT policies and procedures. In an outsourcing scenario, the third party is subject to the delegating insurer's control regarding the effective implementation of those policies and procedures by the outsourcing entity. The outsourcing model is most commonly employed in the case of tied agents, who sell insurance products to consumers exclusively on behalf of a single insurer and therefore typically follow the insurer's AML/CFT policies and procedures.

Under either model, the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures.

3.6.1. Third-Party Reliance

Insurers are permitted to rely on third-party LFIs to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, provided the insurer relying on a third party:

- Immediately obtains the necessary CDD information concerning the elements described in sections 3.3.1.1 through 3.3.1.3;
- Takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay;
- Satisfies itself that the third party is regulated, supervised, or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements in line with FATF standards and local law and regulation; and
- Takes appropriate steps to identify, assess, and understand the ML/FT risks specific to the countries or jurisdictions in which the third party operates.

With respect to the second of these conditions, a best practice is for insurers to obtain a copy of the relevant CDD records or have direct access to the database where such information is held, in order to facilitate ongoing monitoring of the business relationship and, if applicable, the filing of STRs and for a complete assessment record in case of a change of intermediary servicing the policy.

Insurers are not permitted to rely on third parties to conduct ongoing monitoring of business relationships (described in section 3.3.1.4), although they may *outsource* such functions following the guidelines described

immediately below.

3.6.2. Outsourcing

In an outsourcing or agency scenario, the outsourced entity applies CDD or other AML/CFT measures on behalf of the delegating insurer, in accordance with the insurer's internal policies and procedures, and is subject to the insurer's control of the effective implementation of those policies and procedure by the outsourced entity. When outsourcing a part of their AML/CFT function, including the distribution of products, an insurer should therefore include any outsourced entity in its own AML/CFT program and internal control processes, and should monitor such an entity for compliance with its internal AML/CFT policies and procedures. Outsourced entities should also be subject to the employee and agent screening and monitoring checks described immediately below.

3.7. Employee, Officer, Agent, and Broker Risk Management

Insurance operators should have in place screening procedures to ensure high standards when hiring employees, appointing officers, or engaging agents or brokers (including but not limited to outsourced entities, as described in section 3.6.2 above). Employee, officer, and agent or broker screening procedures should include:

- Background checks of employment history; and
- Screening against sanctions lists, ML/FT information sources, and internal watchlists.

In addition, insurance operators should conduct credit history checks on a risk basis. The operator should be aware of potential conflicts of interest for staff with AML/CFT responsibilities and should act to reduce or manage such conflicts of interest, for example by reallocating responsibilities or by instituting quality controls and "four-eye" reviews of the conflicted employee's work.

Operators should also monitor on an ongoing basis for possible indicators of suspicious or illicit behavior by employees, such as:

- An employee whose lifestyle cannot be supported by his/her salary, which may indicate receipt of tips or bribes.
- An employee who is reluctant to take a vacation, which may indicate they have agreed or are being forced to provide services to customers in violation of the law or company policy.
- An employee who is associated with an unusually large number of transactions or a transaction in an unusually large amount, which may indicate they have agreed or are being forced to provide services to customers in violation of the law or company policy.

3.8. Training

As with all risks to which the operator is exposed, the AML/CFT training program should ensure that employees are aware of the risks facing the insurance sector for life insurance and other investment-related insurance products, familiar with the obligations of the operator, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the operator's risk and the nature of its operations, and should be clearly documented in the operator's AML/CFT compliance program and associated training policies, procedures, plans, materials, and attendance records.

3.9. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the operator faces and organized in accordance with the "three lines of defense" model. All three lines of defense must report up to and have the active support and oversight of the operator's senior management, defined broadly to include executives, senior leadership, and the Board of Directors.

Under the model, an operator's business units, sales or relationship managers, and other frontline personnel represent the units or functions that create risk and should therefore serve as the **first line of defense** against ML/TF, and other forms of illicit activity. They should scrutinize customers and their related parties at onboarding and performing periodic and risk-based reviews to update customer information and the operator's understanding of the customer's risks.

The operator's AML/CFT compliance function, in turn, constitutes the **second line of defense**, supporting the frontline units' risk management activities through its system of internal controls and related monitoring, reporting, and risk assessment responsibilities. The core of an effective risk-based program is an appropriately experienced AML/CFT compliance officer, located within the second line of defense, who understands the operator's risks and obligations and who has the resources and autonomy necessary to ensure that the operator's program is effective.

Finally, under article 20.6 of the AML-CFT decision, operators must be subject to independent testing by internal or external auditors, who represent the **third line of defense** by providing independent assurance to the Board and executive management on the effectiveness and adequacy of the operator's governance, risk management, and internal controls. Auditors should have sufficient expertise and understanding of ML/FT risks and requirements and should be fully independent of the activities and reporting structure of the functions subject to independent testing.

Additionally, as per article 32 of the AML-CFT decision, operators with overseas branches, subsidiaries, or other affiliates or legal entities must ensure that all entities within the affiliate network are subject to the AML/CFT policies, procedures, and controls that are at least as stringent as those in place at the entity located in the UAE. Likewise, all entities within the affiliate network should be included in the operator's enterprise risk assessment and subject to AML/CFT independent testing and consolidated governance and oversight.

3.10. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, insurance operators must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, copies of personal identification documents, including STRs/SARs and results of any analysis performed. Operators should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. Operators must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

Annex 1. Red Flag Indicators for the UAE Life Insurance Sector

The UAE Insurance Authority (now merged with the CBUAE) has issued the following list of red flag indicators when handling life insurance and other investment-related insurance products. [14] These indicators should be incorporated into an insurance operator's AML/CFT policies, procedures, detection scenarios, and other processes for identifying potentially suspicious activity related to life and general insurance products.

1. The purchase of an insurance product does not reflect a customer's known needs (e.g., purpose of the account).
2. The early surrender of an insurance product is taken at a cost to the customer.
3. The surrender of an insurance product is initiated with the refund directed to a third party.
4. The customer exhibits no concern for the investment performance of a purchased insurance product and instead exhibits significant concern for its early surrender terms.

5. The customer purchases insurance products using unusual payment methods, such as cash or cash equivalents, or with monetary instruments in structured amounts.
6. The customer demonstrates reluctance to provide identifying information when purchasing an insurance product.
7. The customer borrows the maximum amount available from their insurance product shortly after purchase.
8. The customer used to purchase low-premium insurance and pay premiums by making regular payments but suddenly purchases insurance that requires a large lump-sum premium payment, for which no reasonable explanations are provided.
9. The customer purchases an insurance product without concern for the coverage or benefits, or the customer only cares about the procedures for the policy loan, cancellation of insurance policy, or changing beneficiary when purchasing an insurance policy that has a high cash value or requires a high lump-sum premium payment.
10. The customer usually pays a premium by making regular payments but suddenly requests to purchase a large-sum policy by paying off premium all at once.
11. The customer purchases insurance products with high cash value successively over a short period of time, and the insurance products purchased do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
12. The customer pays premiums in cash and in several payments marginally below the threshold for declaration but cannot reasonably explain the source of funds. In addition, the transactions do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
13. The customer, after making a large premium payment for a policy purchased, applies for a large policy loan or cancels the policy in a short period of time, for which no reasonable explanations are provided.

[14] Sources: FATF, *Life Insurance Sector: Guidance for a Risk-Based Approach* (October 2018), available at: fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf; and U.S. Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, "Insurance," available at: bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/16.

Annex 2. Synopsis

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding of risks and effective performance by CBUAE licensed insurers, agents, and brokers of their AML/CFT obligations.
	Applicability	This Guidance applies to all insurance and re-insurance companies, agents, and brokers that are licensed and supervised by the CBUAE.
Understanding and Assessing ML/FTRisks	Overview of Insurance Sector Activities and Participants	Under Article 2.16 of the AML-CFT Decision, as amended, only direct insurance and re-insurance operations with respect to insuranee of persons and funds accumulation (referred to as life insurance and other investment-related insurance products' hereafter) are subject to the UAE's AML/CFT legal and regulatory framework, with the exception of the targeted financial sanctions' requirements applicable for all insurance operators. Insurance sector participants include operators in the insurance sector, which sell or facilitate the sale of insurance products and must be licensed by the CBUAE, and customers, who own, pay for, and/or are covered by or the beneficiaries of insurance products. • Operators principally include insurers, re-insurers, insurance agents, and insurance brokers. Operators also include consultants, actuaries, loss and damage adjusters, third-party administrators, insurance producers, and price comparison websites (or "insurance aggregators"), although due to their reduced risk exposure these operators are not subject to the Guidance with the exception of the requirements relating to targeted financial sanctions.

		• Customers principally include policy holders (or "policy owners), policy payers, insureds, and beneficiaries.
	ML/FT Risks relevant to life insurance and other investment-related insurance products	• Criminal actors may use life insurance and other investment-related insurance products to place illicit proceeds into the financial system, especially (though not exclusively) where the insurer or intermediary accepts premium payments in cash. • Reimbursed premiums, withdrawn contributions, and payout proceeds (whether legitimate or fraudulent) can be deposited into a bank account or used to purchase other financial instruments without necessarily revealing the ultimate origin of the funds. • Life and other investment-related products are generally considered to present higher ML/FT risk, particularly where they have high cash values upon surrender (e.g. assigning policies and payments to third parties, borrowing against the cash surrender value of permanent life insurance policies, selling units in investment-linked products or buying products with insurance termination features without concern for the product's investment performance).
	Product Risk Factors	Higher-risk productscan include those: whose design allows the insurance operator to hold funds or transact large sums on behalf of the customer; provides for customer anonymity or third-party transactions; has no (or very small) fees or penalties for early withdrawal; allows the product to be held for a shorter period of time; and makes it difficult to identify if products are not being used as intended.
	Service and Transaction Risk Factors	Higher-risk services and transactions can include those: for which it is difficult to trace the ownership of funds; where the customer is not the payer or recipient of the funds; where the payment source or recipient is based outside the country; or involving a large number or transactions back and forth or significant, unexpected, and unexplained changes in the customer's typical activity.
	Distribution Channel and Intermediary Risk Factors	Higher-risk distribution channels can include those: involving a distributor or other intermediary that is not subject to AML/CFT requirements; where the customer pays a distributor, who then pays the insurer; or where the customer has a purely non-face-to-face relationship with insurers or agents (e.g., insurance sold online without adequate safeguards to confirm identity).
	Customer Risk Factors	Higher-risk customers can include those: with incomplete or questionable identification; who are controlled by third parties; that are legal entities with a complex structure: in high-risk industries; making high-value transactions without a confirmed source of funds or wealth; who are new to the insurer; who only hold non-registered policies or accounts; who are politically exposed persons; or who are sanctioned, have ties to sanctioned persons, or are associated with negative news.
	Geographic Risk Factors	Higher-risk geographies can include: regions with high frequency and severity of crimes with ML risk; regions that experience a higher incidence of high-risk activity or fraud; countries risk-rated as high by the insurer; or countries on the NAMLCFTC's or FATF's lists of high-risk jurisdictions or FATF's list of jurisdictions under increased monitoring.
Mitigating Risks	Risk-Based Approach and Enterprise Risk Assessment	Any insurance operator is required to perform, document, and keep up to date an enterprise risk assessment for the purposes of identifying, assessing, and understanding its ML/TF risks for life insurance and other investment-related insurance products and to ensure that identified risks are within the institution's risk appetite and that identified deficiencies are appropriately tracked and remediated.

	New Products, Practices, and Technologies	An insurance operator is required to identify, assess, and take steps to mitigate the ML/TF risks for life insurance and other investment-related insurance products that may arise in relation to: (i) the development of new products and new business practices, including new delivery mechanisms; and (ii) the use of new or developing technologies for both new and preexisting products. The operator must undertake such risk assessments prior to the launch or use of the new products, practices, and technologies and must take appropriate measures to manage and mitigate the identified risks
	Customer Due Diligence ("CDD")	For life insurance and other investment-related insurance products, all insurance operators must perform general CDD on their customers, including customer identification and verification, beneficial ownership identification and verification, understanding the nature of the customer's business and the nature and purpose of the relationship, ongoing monitoring, and name screening. • Additionally, insurance operators are expected to collect and verify the identities of: (i) any natural persons appointed to act on the customer's behalf and (ii) the beneficiaries or other payees of an insurance policy and their beneficial owners. • In low-risk scenarios, insurance operators may perform certain simplified due diligence ("SDD") measures, such as verifying the customer's or beneficial owner's identity after establishing the business relationship, unless there is a suspicious of ML/TF. • In higher-risk scenarios, insurance operators must perform enhanced due diligence ("EDD")measures, such as establishing the source of wealth or funds or conducting enhanced monitoring during the course of the business relationship.
	Transaction Monitoring and STR Reporting	When conducting operations related to life insurance and other investment-related insurance products, Insurance operators must monitor activity by all customers to identify behavior that is potentially suspicious. Insurance operators must file without any delay an STR or SAR with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult CBUAE's *Guidance for Licensed Financial Institutions (LFI) on Transaction Monitoring and Sanctions Screening* as well as CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting*.
	Sanctions Obligations and Freezing without delay	All insurance operators without any exception, are obliged to apply policies, procedures and controls to implement TFS to those sanctioned and designated in the Local Terrorist List and the UN Consolidated List. Please consult the Executive Office for Control and Non-Proliferation (previously known as the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's - referred to as the Executive Office) "*Guidance on TFS for Financial Institutions and designated non-financial business and professions*", the CBUAE's *Guidance for LFIs on the Implementation of Targeted Financial Sanctions* as well as the CBUAE's *Guidance for LFIs on Transaction Monitoring Screening and Sanctions screening*. Insurance operators should also consult the CBUAE's and the Executive Office's websites as updated from time to time (in particular the Executive Office's list of FAQ for the insurance sector).
	Third-Party Reliance and Outsourcing	Insurers are permitted to delegate the performance of specified controls to insurance agents or other intermediaries, using either a third-party reliance model (whereby a third-party licensed financial institution carries out CDD measures following its own AML/CFT policies and procedures) or an outsourcing model (whereby insurers engage a third-party service provider to apply all or

		some of the insurer's own AML/CFT policies and procedures). Under either model, the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures.
	Employee, Officer, Agent, and Broker Risk Management	Insurance operators should have in place screening procedures to ensure high standards when hiring employees, appointing officers, or engaging agents or brokers. Operators should also monitor on an ongoing basis for possible indicators of suspicious or illicit behavior.
	Training	An operator's AM L/CFT training program should ensure that employees are aware of the risks facing the insurance sector for life insurance and other investment-related insurance products, are familiar with the obligations of the operator, and are equipped to apply appropriate riskbased controls.
	Governance and Independent Audit	The preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the operator faces and organized in accordance with the "three lines of defense" model, comprising business unites, a compliance function, and an independent audit function.

Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence

Effective from 31/10/2022 **Status:** In-Force

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019), *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021), and the *Guidelines for Financial Institutions adopting Enabling Technologies* (dated 11/07/2021), and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at centralbank.ae/en/cbuae-amlcft and centralbank.ae/en/fintech-office.

1.2. Applicability

Unless otherwise noted, this guidance applies to all natural and legal persons, which are licensed and/or supervised by CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, issuers and providers of stored value facilities, licensed retail payment service providers, card schemes, registered hawala providers, and other LFIs; and
- Insurance companies, agencies and brokers.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and Financing Illegal Organisations (as amended by Federal Decree Law No. (26) of 2021) ("AML-CFT Law"); and

(ii) Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision").

This Guidance also builds on global standards and best practices issued by the Financial Action Task Force ("FATF")[2] and the Wolfsberg Group, as well as on industry standards and best practices.

[2] Including FATF Guidance on Digital ID, available at: fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
API	Application program interface
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CSP	Credential service provider
DNFBP	Designated non-financial business or profession
DPP	Data protection and privacy
FATF	Financial Action Task Force
FIDO	Fast Identity Online
ID	Identity
IDSP	Identity service provider
IP	Internet Protocol
LFI	Licensed financial institution
MAC	Media Access Control
MFA	Multifactor authentication
ML	Money laundering
NIST	National Institute of Standards and Technology

OTP	One-time password
PKI	Public key infrastructure
PII	Personally identifiable information
PIN	Personal identification number
SIM	Subscriber identity module
TF	Terrorist financing

2. Overview of Digital ID Systems and Participants

2.1. Terminology and Definitions

For the purposes of this Guidance, in relation to identifying and verifying the identity of a customer as part of the customer due diligence ("CDD") process, **identity** ("ID") refers to the specification of a unique natural person that is:

- Based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population or particular context(s); and
- Recognized by the state for regulatory and other official purposes.

Proof of identity generally depends on some form of government-provided or issued registration, documentation, or certification (such as a birth certificate, identity card, or digital ID credential) that constitutes evidence of core attributes (such as name and date and place of birth) for establishing and verifying identity. Proof of identity may be provided through general-purpose ID systems (such as national ID and civil registration systems) or various limited-purpose ID systems (such as taxpayer identification numbers, driver's licenses, passports, voter registration cards, social security numbers, and refugee identity documents).

Digital ID systems use electronic means to assert and prove a person's identity online and/or in in-person environments, including through the use of:

- Electronic databases, including distributed databases and/or ledgers, to obtain, confirm, store, and/or manage identity evidence;
- Digital credentials to authenticate identity for accessing mobile, online, and offline applications;
- Biometrics to help identify and/or authenticate individuals; and
- Digital application program interfaces ("APIs"), platforms, and protocols that facilitate online identification and the verification and authentication of identity.

Identification Systems in the UAE

LFIs should understand and utilize national-level identification systems and processes currently in place or under development in the UAE, including but not limited to:

- **UAE Pass**, the UAE's first national digital identity and signature solution that enables users to identify themselves to government service providers in all emirates through a smartphone-based authentication protocol and to sign documents digitally with a high level of security. The UAE Pass app uses biometric facial recognition software to verify and register users without requiring an in-person visit to a government services center. The UAE Pass also includes a "digital vault" for storing users' digital documents and sharing them with government departments, as well as a "digital signature" function to complete official transactions without the need for paper documents or physical signatures.

- **Emirates ID**, the mandatory, government-issued identity card for all UAE citizens and residents. While issued as a physical card, the Emirates ID card uses public key infrastructure to attach individual identities to digital certificates that can be used to sign and encrypt data, as well as fingerprint biometrics. When verifying an Emirates ID card, LFIs should use the online validation gateway of the Federal Authority for Identity and

Citizenship and should keep a copy of the Emirates ID and its digital verification in their records.

- **Emirates Facial Recognition**, an initiative launched by the UAE Ministry of Interior and Federal Authority for Identity, Citizenship, Customs & Port Security, together with private sector partners. The facial recognition initiative includes a "face fingerprint" system for digital verification of digital transactions and remote identities.

Digital ID systems involve two basic components and an optional third component:

- **Identity proofing and enrollment** answers the question: *Who are you?* It involves collecting, validating, and verifying identity evidence and information about a person, establishing an identity account, and binding the individual's unique identity to authenticators possessed and controlled by this person.

- **Authentication and identity lifecycle management** answers the question: *Are you the person who has been identified and verified?* It establishes, based on possession and control of authenticators, that the person asserting the identity is the same person who was identity proofed and enrolled, and ensures that adequate controls are in place to manage events that can occur over the identity lifecycle that affect the use, security, and trustworthiness of authenticators.

- **Portability and interoperability mechanisms**, where used, enable proof of identity to be portable, so that an individual's digital ID credentials can be used to prove identity for new customer relationships at unrelated private-sector or governmental entities, without their having to obtain and verify personal data and conduct customer identification and verification each time. Portability and interoperability are optional components of any digital ID system.

Not all elements of a digital ID system are necessarily digital. Some elements of identity proofing and enrollment can be either digital or physical, or a combination; however, binding, credentialing, authentication, and portability/federation (where applicable) are always and necessarily digital. These concepts are explained further in the following sections.

Digital ID systems can enable remote customer identification and verification, support remote financial transactions, and otherwise facilitate **non-face-to-face business relationships and transactions**, defined as interactions in which the parties are not in the same physical location and conduct activities by digital or other non-physically present means, such as mail or telephone. Under international standards, non-face-to-face business relationships and transactions are included as an example of a potentially higher-risk situation in undertaking CDD.[3] However, given the evolution of digital ID technology, architecture, and processes, and the emergence of consensus-based open-source digital ID technical standards, non-face-to-face interactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place may present a standard level of risk, and may even present a lower level of risk where higher assurance levels are implemented and/or appropriate control measures are present.[4] See section 4 below for specific risk mitigation measures and strategies that can help ensure that a digital ID system is suitably "reliable" and "independent" in this sense.

---

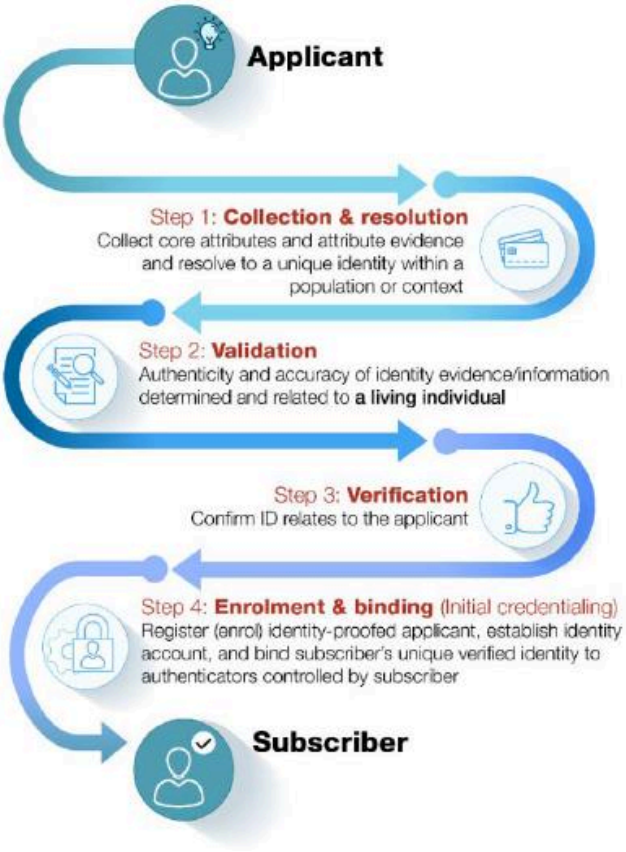
[3] See *The FATF Recommendations*, Interpretive Note to Recommendation 10, at 68, available at: fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[4] FATF, *Guidance on Digital Identity*, at 30, available at: fatf-gafi.org/media/fatf/documents/recommendations/Guidance- on-Digital-Identity.pdf.

2.2. Identity Proofing and Enrollment

Identity proofing and enrollment (with initial binding/credentialing) constitute the first stage of a digital ID system. This component is directly and most immediately relevant to LFIs' customer identification and verification obligations under Article 8 of the AML-CFT Decision. For illustrative purposes only, Figure 1 below presents a sample process flow for identity proofing and enrollment; the discussion that follows explains each step in greater detail.

Figure 1. Identity Proofing and Enrollment



Source: The Financial Action Task Force[5]

Identity proofing comprises three actions: (1) collection and resolution, (2) validation, and (3) verification. Examples of each of these actions are included in the discussion below for illustrative purposes only; there is no expectation that LFIs employing a digital ID system for CDD use any particular method of identity proofing unless otherwise required.

1. **Collection and resolution** involves obtaining attributes, collecting attribute evidence, and resolving identity evidence and attributes to a single unique identity within a given population or context (a process known as "de-duplication").[6]

    - Attribute evidence may be either physical (documentary) or purely digital, or a digital representation of physical attribute evidence (such as a digital representation of a paper or plastic driver's license). Identity evidence has traditionally taken a physical form and been physically presented by the person seeking to prove his or her identity (known as a "claimant") to an identity service provider ("IDSP"). However, with the development of digital technology, identity evidence may now be generated digitally (or converted from physical to digital form) and stored in electronic databases, allowing the identity evidence to be *obtained remotely* and/or identity evidence to be *remotely verified and validated* against a digital database.
    - Attributes may also be inherent, that is, based on an individual's personal biometric characteristics, including:

        - Biophysical biometrics, such as fingerprints, iris patterns, voiceprints, and facial recognition—all of which are static;

        - Biomechanical biometrics, such as keystroke mechanics, which are the product of unique interactions of an individual's muscles, skeletal system, and nervous system—all of which

are dynamic; and

- Behavioral biometrics, such as email or text message patterns, mobile phone usage, geolocation patterns, and file access log, which are based on an individual's patterns of movement and usage in what are known as "geospatial temporal data streams."

- Under Article 8.1 of the AML-CFT Decision and section 6.3.1 of the *AML/CFT Guidelines for Financial Institutions*, required identity attributes for CDD under UAE regulations and guidance include, for a natural person, the name (as in the passport or identity card, number, country of issuance, date of issuance and expiration date of the identity card or passport), the nationality, the address (i.e., the permanent residential address), the date and place of birth, and the name and address of employer (if applicable).

  When verifying the Emirates ID card, either physically or by way of digital or electronic Know Your Customer ("e-KYC") solutions, LFIs should use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE Pass Application, or other UAE Government-supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than Emirates IDs, are used in the KYC process, a copy should be physically obtained from the original passport, which should be certified as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.

2. Validation involves determining that the evidence is *genuine* (i.e., not counterfeit, forged, or misappropriated) and that the information the evidence contains is *accurate*. Validation is performed by checking the identity information and evidence against an authoritative and reliable source to establish that the information matched reliable, independent source data or records.

   - For instance, in order to assess whether an individual's physical identity evidence (such as a driver's license or passport), or the digital images thereof, is *genuine*, an IDSP may review the evidence to determine that there have been no alterations, that the identification numbers follow standard formats, and that the physical and digital security features are valid and intact.

     - When utilizing a physical or digital copy of identity evidence such as an Emirates ID card for purposes of validation, LFIs are expected to review the evidence for physical or digital abnormalities or possible alterations and to make a determination as to whether the evidence has been altered or forged.

   - In order to assess whether such evidence is *accurate*, the IDSP may query the government issuing sources for the license or passport and confirm that the information matches.

     - As noted above, LFIs should use the online validation gateway of the Federal Authority for Identity, Citizenship, Customs & Port Security, the UAE Pass Application, or other UAE Government-supported solutions, to ensure that the information presented for validation purposes matches the information included in reliable databases or other sources.

3. Verification involves confirming that the validated identity relates to the specific individual being identity-proofed, including (but not limited to) through the use of biometric solutions like facial recognition or liveliness detection.

   - For example, if performing verification remotely, an LFI or other IDSP could ask the applicant to take and send a mobile phone video or photo with other liveliness checks, compare the submitted photos to the photos on the applicant's Emirates ID, passport, or other valid documents, and

determine that they match to a given level of certainty.

- To tie this identity evidence to the actual (real-person) applicant, the IDSP could then send an enrollment code to the applicant's validated phone number, email address, or another address that is tied to the identity, require the applicant to provide the enrollment code to the IDSP, and confirm that the submitted code matches the code sent. Such measures would verify that the applicant is a real person, in possession and control of the validated phone number. At this point, the applicant will have been identity proofed.

The fourth and final action in the first stage of a digital ID system is **enrollment and binding**.

4. **Enrollment** is the process by which an IDSP registers (or "enrolls") an identity-proofed applicant as a "subscriber" and establishes their identity account. This process authoritatively **binds** the subscriber's unique verified identity (i.e., the subscriber's attributes/identifiers) to one or more authenticators possessed and controlled by the subscriber, using an appropriate binding protocol. The process of binding the subscriber's identity to authenticator(s) is also referred to as "credentialing."

    - An **authenticator** is something the claimant possesses and controls—typically, a cryptographic module, one-time code generator, or password—that is used to confirm or "authenticate" that the claimant is the individual to whom a credential was issued and therefore is (to a given degree of likelihood) the actual subscriber and accountholder. The likelihood that the claimant to whom a credential was issued is in fact the actual subscriber is a function, in part, of the strength of the authentication component; stronger authenticators, such as longer and more complex passwords, can increase an IDSP's confidence that the claimant is in fact the actual subscriber.

    - A **credential** is a physical object or digital structure, such as a physical or electronic ID card, that authoritatively binds a subscriber's proofed identity (via one or more identifiers) to at least one authenticator possessed and controlled by the subscriber. When a digital IDSP issues an authenticator (such as a password or PIN) and authoritatively binds the authenticator to the subscriber's identity, the physical object or digital structure that results (such as an ID card) is a credential.

    Typically, an IDSP issues one or more authenticators (such as a password or auto-generated code) *to the subscriber* and registers the authenticators in a way that ties them to the subscriber's proofed identity at enrollment. However, the IDSP can also bind the subscriber's account to authenticators provided *by the subscriber* that are acceptable to the IDSP. For example, users of the UAE Pass app are prompted to create a signing password while completing the verification step at a UAE Pass kiosk or through the mobile app. The IDSP can also bind a subscriber's credentials to additional or alternative authenticators at a later point in time, as part of identity lifecycle management (discussed immediately below).

---

[5] Available at: fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

[6] Some government-provided ID solutions include a de-duplication process as part of identity proofing, which may involve checking the applicant's specific biographical attributes (such as name, age, or gender), biometrics (such as fingerprints, iris scans, or facial recognition images), and/or government-assigned attributes (such as driver's license, passport, or taxpayer identification numbers) against the identity system's database of enrolled individuals and their associated attributes and identity evidence to prevent duplicate enrollment.

2.3. Authentication and Identity Lifecycle Management

Authentication and identity lifecycle management constitute the second stage of a digital ID system. **Authentication** answers the question: *Are you the person who has been identified and verified?* It establishes the individual seeking to access an account (or other services or resources) is the same person who has been identity proofed, enrolled, and credentialed and has possession and control of the binding credentials and other authenticators, if applicable. In

other words, it establishes that the *claimant* is the *onboarded customer*. Authentication can rely on various types of authentication factors and processes, with the trustworthiness of the authentication depending on the type of authentication factors used and the security of the authentication processes:

- **Authentication factors** fall into three basic categories:
    - **Knowledge factors**, that is, something you *know*, such as a shared secret (e.g., username, password, or passphrase), a personal identification number ("PIN"), or a response to a pre-selected security question;
    - **Ownership factors**, that is, something you *have*, such as a cryptographic key stored in hardware (e.g., in a mobile phone, tablet, computer, or USB-dongle) or software that the subscriber controls; a one-time password ("OTP") generated by a hardware device; or a software OTP generator installed on a digital device, such as a mobile phone; and
    - **Inherence factors**, i.e., something you *are*, including biophysical biometrics, biomechanical biometrics, and behavioral biometrics (as discussed in section 2.2 above).
- **Authentication processes** have historically been assessed by the number and type of authentication factors the process requires, on the assumption that the more factors an authentication process employs, the more robust and trustworthy the authentication system is likely to be. As authentication technology and processes have evolved, however, this assumption has been revised, and the strength of the authentication component is no longer assumed to depend on *how many* factors (or types of factors) it uses but rather on whether its authentication processes are *secure*: that is, resistant to compromise by commonly executed and evolving attacks, such as phishing and man-in-the-middle attack vectors. In this revised paradigm, multifactor authentication ("MFA")—where an IDSP uses two or more independent authenticators from at least two different authentication factor categories (knowledge/possession/inherence) to authenticate the claimant's identity—is typically assumed.
    - As detailed in the *Guidance for Financial Institutions adopting Enabling Technologies*, LFIs should implement MFA using a biometric factor where possible to authorize high-risk activities and protect the integrity of customer account data and transaction details. High-risk activities include changes to personal data (e.g., customer office or home address, email address, or telephone contact details), registration of third-party payee details, high-value funds transfers, and revisions to funds transfer limits.
        - LFIs deploying MFA at login that includes a biometric factor should consider employing phishing-resistant authenticators where at least one factor relies on public key encryption to secure the customer authentication process.
    - Digital ID authentication has traditionally been conducted at a particular point in time: namely, when the claimant asserts the customer's/subscriber's identity and seeks authorization to begin a digital or in-person interaction to access his or her account or other financial services or resources. Today, however, many regulated entities augment traditional authentication at the beginning of an online interaction with **continuous authentication** solutions that leverage biomechanical biometrics, behavioral biometrics, and/or dynamic transaction risk analysis.
        - Instead of relying on something the claimant has/knows/is to establish at the beginning of the interaction that the claimant is the onboarded customer and is in control of the authenticators issued to that customer, continuous authentication focuses on ensuring that certain data points collected throughout the course of an online interaction—such as geolocation, Media Access Control ("MAC") and Internet Protocol ("IP") addresses, typing cadence, and mobile device angle— match what should be expected during the entire

session.

- However, ways of measuring the effectiveness of continuous authentication technology in mitigating authentication risks have not reached maturity, and the digital ID technical standards, such as the U.S. National Institute of Standards and Technology ("NIST") Digital Identity Guidelines, do not currently address them.

- Finally, **identity lifecycle management** refers to the actions IDSPs should take in response to events that can occur over the lifecycle of a subscriber's authenticator that affect the use, security, and trustworthiness of the authenticator. The attributes associated with an identity may change from year to year, and analytics systems may uncover risk signals suggesting an identity is being used in a manner consistent with fraud or account compromise. Key identity lifecycle events may include:

  - **Issuing and recording credentials:** At customer onboarding, the IDSP issues the credential and records and maintains the credential and associated enrollment data in the subscriber's identity account throughout the credential's lifecycle.

  - **Binding:** Throughout the digital ID lifecycle, the IDSP should also maintain a record of all authenticators that are, or have been, associated with the identity account of each of its subscribers, as well as the information required to control authentication attempts. When an IDSP binds a new authenticator to the subscriber's account post-enrollment, it should require the subscriber to first authenticate at the assurance level (or higher) at which the new authenticator will be used.

  - **Compromised authenticators:** If a subscriber loses or otherwise experiences compromise of all authenticators of a factor required for MFA, the subscriber should repeat the identity proofing process, confirming the binding of the authentication claimant to previously proofed evidence, before the IDSP binds a replacement for the lost authenticator to the subscriber's identity account. If the subscriber has MFA and loses one authenticator, the IDSP should require the claimant to authenticate, using the remaining authentication factors.

  - **Expiration and renewal:** Where an IDSP has issued an authenticator that expires, the IDSP should bind an updated authenticator prior to expiration, using a process that conforms to the initial authenticator binding process and protocol, and then revoke the expiring authenticator.

  - **Revocation or termination:** IDSPs should promptly revoke the binding of authenticators when an identity ceases to exist (e.g.., because the subscriber has died or is discovered to be fraudulent); when requested by the subscriber; or when the IDSP determines that the subscriber no longer meets its eligibility requirements.

2.4. Portability and Interoperability Mechanisms

Digital ID systems can—but need not—include a component that allows proof of identity to be portable. An individual's identity is **portable** when his or her digital ID credentials can be used to prove identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personally identifiable information ("PII") and conduct customer identification and verification each time. Portability requires developing **interoperable** digital identification products, systems, and processes, including through the use of federated digital architecture and assertion protocols to convey identity and authentication information across a set of networked systems or through APIs that do not use federated architecture and protocols.

Portability and interoperability can potentially save relying parties (e.g., financial institutions and government entities) time and resources in identifying, verifying, and managing customer identities, including for account opening and authorizing customer account access, and may reduce the risk of identity theft stemming from the repeated

exposure of PII. However, as discussed below, portability and interoperability are optional components of a digital ID system and will not be a focus of this Guidance.

2.5. Focus of this Guidance

This Guidance focuses on the **use of digital ID systems for CDD**, specifically for customer identification and verification at onboarding or account opening and for ongoing CDD monitoring, thus enabling LFIs to fulfill their obligations under Articles 8 and 7, respectively, of the AML-CFT Decision. The Guidance emphasizes, however, that **customer identification and verification and ongoing monitoring of the business relationship are only two components of LFIs' wider CDD obligations**, which include identifying and verifying the identities of a legal entity customer's beneficial owners and understanding the nature of the customer's business and the nature and purpose of the customer's business relationship with the LFI. LFIs are also separately required under Article 24 of the AML-CFT Decision to maintain all records and documents obtained through CDD measures for a period of no less than five years from the date of termination of the business relationship with the customer; under FATF standards and UAE regulation, such recordkeeping requirements are technology neutral, meaning they apply equally to records kept in digital and physical (documentary) form.

The Guidance focuses primarily on **identity proofing and enrollment** and secondarily on **authentication**; it does not address portability and interoperability, as these components are regarded as optional under international AML/CFT standards and are less directly relevant to the application of CDD measures by LFIs. Particular emphasis will be placed on the use of third-party sources or providers to verify and authenticate customer identity through digital means.

Finally, the Guidance focuses on the use of digital ID systems to identify and verify the identity of customers that are **individuals (natural persons)**. It does not examine the use of digital ID systems to help identify and verify the identity of a legal person's representative(s) or beneficial owner(s) or to understand and obtain information on the nature and intended purpose of the business relationship—although reliable, independent digital ID systems are important for all of these CDD functions.

3. Use of Digital ID Systems for CDD

3.1. Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify each customer and verify the customer's identity using documents, data, or any other identification information from a reliable and independent source. This requirement is technology neutral and expressly permits LFIs to use documentary as well as non-documentary sources (i.e., information or data) when performing identification and verification; it does not impose any restrictions on the form—physical or digital—that identity evidence must take, nor does it impose limitations as to the use of digital ID systems for the purpose of linking a customer's verified identity to a unique, real-life individual, provided this is done using a "reliable" and "independent" source. As such, LFIs are permitted to utilize digital ID systems as well as physical forms to perform customer identification and verification, consistent with the expectations set forth in this Guidance.

In the digital ID context, the requirement that digital source documents, data, or information must be "reliable" and "independent" means that the digital ID system used to conduct CDD relies upon technology, adequate governance, processes, and procedures that provide an appropriate level of confidence that the system produces accurate results. Reliability and independence in this sense depends specifically on the effective application of mitigation measures to prevent and manage risks related to **identity proofing and enrollment**, such as the risks of an applicant using falsified identity evidence or another individual's identity, as well as risks related to **authentication and identity lifecycle management**, including various risks that bad actors will illicitly obtain an individual's legitimate identity credentials and assert them to open an account or obtain unauthorized access to products, services, and data. These risks and the corresponding mitigating measures that LFIs should consider implementing are discussed in greater detail in section 4 below.

3.2. Ongoing Due Diligence on the Business Relationship

Under Article 7 of the AML-CFT Decision, all customers must be subject to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

As discussed in section 2 above, authentication using a digital ID system establishes confidence that the person asserting identity today is the same person who previously opened the account or other financial service and is in fact the same individual who underwent reliable, independent identification and verification at onboarding. In other words, ongoing digital authentication of the customer's identity links that individual with their financial activity. LFIs that use digital ID systems to authenticate the identity of their existing customers as part of account authorization should leverage the data generated by authentication and related information (such as geolocation or IP addresses) to support ongoing due diligence and transaction monitoring, such as to assess whether a customer's actual activity conforms to the LFI's expectations of normal or typical activity and to identify cases in which a customer may be transacting from a sanctioned, otherwise prohibited, or high-risk jurisdiction.

3.3. Third-Party Reliance and Provision of Digital ID Services

Per Article 19 of the AML-CFT Decision, LFIs are permitted to rely on customer identification and verification undertaken by a third party at onboarding, provided the relying LFI:

1. Immediately obtains the necessary information concerning customer identification and verification from the third party, including the assurance levels, where applicable;
    - For example, the digital ID system could enable the prospective customer to assert identity to the relying LFI and the third party to authenticate the person's identity and provide additional needed information, such as the person's name, date of birth, government-provided unique identity number, or other attributes required to prove official identity.
2. Takes adequate steps to satisfy itself that the third party will make available copies of or other appropriate forms of access to identification data and other relevant CDD information and documentation without delay;
    - For example, the relying LFI could take appropriate steps to satisfy itself: (a) that, as part of identity proofing and enrollment, the third party established a digital ID account for the identified person that contains adequate attribute evidence and other identity data and information; and (b) that the third party's authentication processes enable it to provide that information to the relying party upon request without delay.
3. Satisfies itself that the third party adheres to the CDD and recordkeeping requirements set forth in the AML-CFT Decision and is regulated and supervised for compliance with these requirements. **In practice, this means that the third party should either be another LFI, a designated non-financial business and profession ("DNFBP"), or another regulated entity**, as defined in UAE regulation and guidance; and
4. Considers country risk information when determining in which countries a third party meeting the above conditions can be based.

Unlike **outsourcing** relationships, in which an LFI engages a third-party provider to perform certain control functions on the LFI's behalf and in conformity with the LFI's AML/CFT policies and procedures,[7] **third-party reliance** relationships typically involve an LFI relying the customer identification and verification measures already undertaken by another regulated entity on an existing customer of that entity in accordance with the entity's own AML/CFT policies and procedures. In reliance relationships, that is, the third party will usually already have a business

relationship with the customer that is independent of the relationship to be formed by the customer with the relying institution. The third party will therefore have onboarded the customer in accordance with its own AML/CFT policies and procedures. In a typical reliance scenario, a prospective customer will assert identity to the relying LFI using a digital ID system, at which point the third party will be prompted by the system to authenticate the person's identity and (per condition 1 above) immediately provide relevant identification and verification information to the relying LFI. In all reliance relationships, the ultimate responsibility for CDD measures remains with the LFI that relies on the third party.

---

[7] See also *Guidance for Financial Institutions adopting Enabling Technologies*, section 3.90 for additional detail related specifically to the outsourcing of biometric activities.

4. Risks and Challenges Presented by Digital ID Systems

Like any ID system, the reliability of digital ID systems depends on the strength of the documents, processes, technologies, and security measures used for identity proofing, credentialing, and authentication, as well as ongoing identity management. In both documentary and digital ID systems, reliability can be undermined by identity theft and source documents that can be easily forged or tampered with. Some types of fraud, such as "massive attack" frauds, may be less likely to occur in-person or in processes requiring human intervention. While digital ID systems provide security features that mitigate some issues with paper-based systems, they also increase some risks, such as data loss, data corruption, or misuse of data due to unauthorized access.

Digital ID systems also present a variety of technical challenges and risks due to their reliance on open communications networks (i.e., the Internet) for identity proofing and authentication, and the involvement of multiple parties (such as the IDSP, the customer, and the relying LFI), which together can present multiple opportunities for cyberattacks. Without careful consideration of relevant risk factors and the implementation of appropriate, technology-based safeguards and effective governance and accountability measures to address these risks, criminals, money launderers, terrorists, and other illicit actors may be able to abuse digital ID systems to create false identities or exploit (e.g., hack or spoof) authenticators linked to a legitimate identity.

The discussion below covers both identity proofing and enrollment risks and authentication risks. Risks at the identity proofing stage include the risk that proofing and enrollment processes result in digital IDs that are fake—that is, obtained under false pretenses through an intentionally malicious act—and can be used to facilitate illicit activities. These risks are mitigated by having an appropriate identity assurance level. Risks at the authentication stage include the risk that a legitimately issued digital ID has been compromised and that its credentials or authenticators are under the control of an unauthorized person. These risks are mitigated by having an appropriate authentication assurance level. This section concludes with a discussion of broader connectivity, cybersecurity, and privacy challenges in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD.

4.1. Identity Proofing and Enrollment Risks

This section focuses on threats to the identity proofing and enrollment process presented by cyberattacks, security breaches, and the production and presentation of false identity evidence, either by stealing a real person's identity or by combining real and fake information to create a new identity. The enrollment process may also be threatened through the compromise of, or misconduct by, an IDSP or through the compromise of the broader digital ID infrastructure. The latter type of threat is outside the scope of this Guidance and should be directly addressed by traditional computer security controls (such as intrusion protection, recordkeeping, and independent audits) and by broader governance and organizational requirements and digital ID assurance frameworks and standards.

In certain respects, the risks arising from the presentation of stolen or counterfeit identity evidence can be even greater in digital ID systems, as online counterfeiters and cybercriminals may be able to obtain or produce false identity evidence at far greater scale than illicit actors trading solely in physical documents. Impersonation involves a person pretending to have the identity of another genuine person, including by using a stolen document of someone

with a similar appearance or by combining stolen identity evidence with counterfeit or forged evidence (as when an imposter places his or her photo onto a stolen passport or ID card). By contrast, a **synthetic ID** is created by criminals by combining real (usually stolen) and fake information to create a new, synthetic identity, which can be used to open fraudulent accounts and make fraudulent purchases. Unlike impersonation, the criminal using a synthetic ID is pretending to be someone who does not exist in the real world, rather than impersonating an existing identity.

For example, criminal groups have been known to produce synthetic digital IDs at large scale by stealing real individuals' identity attributes and other data from online transactions or by hacking Internet databases, and combining these attributes with entirely fake information. The resulting synthetic IDs have been used to obtain credit cards or online loans and to withdraw funds, with the account abandoned shortly thereafter.

The table below sets out these risks and presents some strategies for mitigating threats to the identity proofing and enrollment process, based on the U.S. National Institute of Standards and Technology ("NIST") Digital Identity Guidelines (also incorporated into the FATF's *Guidance on Digital Identity*). FATF further advises regulated entities to utilize safeguards built into digital ID systems to prevent fraud, such as monitoring authentication events to detect systemic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators, to feed into suspicious activity monitoring and reporting systems.

Type of Risk	Description	Potential Risk Mitigation Strategy
Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license	• IDSP validates physical security features of presented evidence • IDSP validates personal details in the evidence with the issuer or other authoritative source
Fraudulent use of another's identity	An applicant uses a passport associated with a different individual	• IDSP verified identity evidence and biometric of applicant against information obtained from issuer or other authoritative source

4.2. Authentication and Identity Lifecycle Management Risks

Risks at the authentication stage involve the possibility of bad actors asserting an individual's legitimate identity to a relying party to open an account or obtain unauthorized access to products, services, and data. Key authentication vulnerabilities include:

- **Credential stuffing** (also referred to as breach replay or list cleaning): a type of cyberattack where stolen account credentials, often from a data breach, are tested for matches on other systems. This type of attack can be successful if the victim has used the same password that was stolen in the data breach for another account.

- **Phishing**: a fraudulent attempt to gather credentials from unknowing victims using social engineering attacks such as deceptive emails, phone calls, text messages, or websites. For example, a criminal may attempt to trick his or her victim into supplying names, passwords, government ID numbers, or credentials to a seemingly trustworthy source that is in fact controlled by the criminal.

- **Man-in-the-middle** (also known as credential interception): an attack that attempts to achieve the same goal as phishing and can be a tool to commit phishing, but does so by intercepting communications between the victim and the service provider.

- **PIN code capture and replay**: an attack in which a criminal uses a key logger to capture a PIN code entered on a computer keyboard or other device and, without the user noticing, uses the captured PIN to access services (e.g., when a smartcard is present in the reader).

Most authentication vulnerabilities are exploited without the identity owner's knowledge, but abuse can also involve the witting participation of subscribers or IDSPs. For example, shared-secret authenticators, such as passwords, may be stolen and exploited by bad actors, but they can also be deliberately shared by the owner of the identity credentials for illicit purposes, as in the case study below.

Misuse of Digital ID by Straw Men

Criminal organizations can purchase digital ID credentials from individuals that enable them to access the individuals' accounts at LFIs or other regulated entities, in effect turning them into digital mules for the organization. The individuals may either already have an account or agree to open one in connection with selling the identity credentials.

In one case highlighted by the FATF, criminal groups opened bank accounts using straw men, who established the account, obtained a digital ID and a security code, and provided their credentials to the criminal group, in exchange for money. In many cases, multiple digital IDs were used on a single mobile phone or tablet. Access to these accounts afforded the criminal groups access to real-time transactions, making it possible for them to quickly transfer money between various accounts. As the FATF notes, the overwhelming majority of digital IDs that are misused by criminal groups are issued on the basis of legitimate identity evidence.

Some of the primary known risks at the authentication stage are associated with specific types of authenticators or authentication processes, including:

- **Multifactor authentication vulnerabilities:** Passwords or passcodes, which are supposed to be shared-secret knowledge authenticators, are vulnerable to brute-force login attacks, phishing attacks, and massive online data breaches, and are very easily defeated. Stolen, weak, or default passwords are believed to be behind the vast majority of data breaches. MFA solutions, such as SMS one-time codes texted to the subscriber's phone, add another layer of security to passwords and passcodes, but they can also be vulnerable to phishing, subscriber identity module ("SIM") card swapping, mobile device compromise, and other attacks.
    - **Phishing-resistant authenticators**, where at least one factor relies on **public key encryption**, can help combat these vulnerabilities. In public-key encryption, a pair of keys are generated for an entity (person, system, or device), and that entity holds the private key securely, while freely distributing the public key to other entities. Anyone with the public key can then use it to encrypt a message to send to the private-key holder, knowing that only they will be able to open it. Examples of phishing-resistant authenticators include authenticators built off public key infrastructure ("PKI") certificates or the Fast Identity Online ("FIDO") Alliance standards.
    - Per the *Guidance for Financial Institutions adopting Enabling Technologies*, LFIs should implement MFA using a biometric factor (discussed immediately below) where possible to authorize high-risk activities (including changes to personal, registration of third-party payee details, high-value funds transfers, and revisions to funds transfer limits) and to protect the integrity of customer account data and transaction details. Moreover, LFIs deploying MFA at login that includes a biometric factor should consider employing phishing-resistant authenticators where at least one factor relies on public key encryption to secure the customer authentication process.
- **Biometric authenticators:** Biophysical authenticators, such as fingerprints and iris scans, are more difficult to defeat than traditional authenticators and are increasingly ubiquitous. Most smart phones have built-in fingerprint scanners, some have built-in iris scanners, and facial recognition capabilities are built into many personal computer systems and advanced smart phones. Biometric characteristics can be stolen in bulk from central databases, obtained by taking high-resolution photos, lifted from objects the individual

touches, or captured with high-resolution images and then spoofed. Currently, however, these types of attacks are difficult and/or highly resource intensive and therefore not scalable. For example, biometric authenticators that require on-device matching cannot be fraudulently used at scale because they require physical access to the device of the customer.

    - Biometrics have a variety of other weaknesses that give rise to *reliability concerns* when used for authentication purposes and have led some technical standards to restrict their use for authentication (although not for identity proofing). Fingerprints may not be read or may be read incorrectly; and facial recognition factors can be rendered unreliable by changes in facial expressions, facial hair, makeup, or lighting conditions. Due to incomplete data sets, facial recognition has been less reliable for persons with darker skin pigmentation and certain ethnic features, although this is improving. In contrast to knowledge- or possession-based authenticators, stolen biometric authenticators are difficult to revoke or replace.

- **Identity life cycle risks:** Poor identity life cycle and access management can, wittingly or unwittingly, compromise the integrity of authenticators and enable unauthorized persons to access and misuse customer accounts, undermining the purpose of customer identification and verification, ongoing due diligence, and transaction monitoring requirements in protecting the financial system from abuse.

- **Compromised MFA workflow bypass:** Attackers have also been known to identify loopholes in MFA protocols, for example by initiating a denial-of-service attack that causes the MFA workflow to break or its security to degrade.

- **Unknown risks:** Digital ID systems develop and evolve. In many cases, technical design changes introduce operational improvements but bring with them vulnerabilities that are not apparent until they are exploited by bad actors in ways that disclose how the digital ID system has been compromised.

4.3. Broader Issues Presented by Digital ID Systems

Beyond specific risks associated with identity proofing/enrollment and authentication, there are a number of broader issues in the digital space that may impact the integrity or availability of digital ID systems to conduct CDD. These include but are not limited to:

- **Connectivity issues:** The lack of a reliable network infrastructure can undermine digital ID systems at particular customer touchpoints or across larger geographic areas for meaningful periods of time. However, digital ID systems can be designed to support both offline and online transactions, allowing them to function with or without access to the Internet or a mobile network. LFIs should consider the resilience of available networks and systems, including the geographic locations from which customers may be utilizing a digital ID system for authentication, when deciding whether to use a digital ID system for CDD.

- **UAE frameworks for official identity:** The reliability and independence of purely documentary approaches can be undermined by identity theft and the widespread counterfeiting of official identity documents, including where official identity documents either lack advanced security features to prevent tampering or counterfeiting or are issued without adequate identity proofing. Such weaknesses in the reliability of documentary identity evidence can have a cascading effect on the risks posed by digital ID systems, and identity theft from online databases can generate similar risks for both digital ID systems and documentary approaches.

    - The Emirates ID utilizes ultraviolet ink, public key infrastructure, and fingerprint biometrics to prevent tampering or counterfeiting of the card.

    - To further mitigate the risks associated with tampering or counterfeiting of official identity documents, LFIs should use the online validation gateway of the Federal Authority for Identity and

Citizenship when verifying the Emirates ID card, and should keep a copy of the Emirates ID and its digital verification in their records.[8]

- **Data protection and privacy challenges:** Digital ID involves the collection and processing of PII, potentially including biometrics. As such, digital ID systems are subject to local data protection and privacy ("DPP") requirements, including Federal Decree-Law No .34 of 2021 Concerning the Fight Against Rumors and Cybercrime; Federal Decree-Law No. 46 of 2021 On Electronic Transactions and Trust Services; the Internet Access Management (IAM) policy; relevant Emirate-level requirements such as the Dubai Data Law; and Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, where relevant.
    - Under the UAE's DPP framework, LFIs and DISPs are not permitted to transfer or store personal data, including digital or physical copies of Emirates IDs, outside of the UAE, except as permitted by Articles 22 and 23 of the Federal Decree-Law No. 45 of 2021.
    - LFIs should also consult the *Principles on Identification for Sustainable Development*, including Principle 8 regarding the protection of personal data and the maintenance of cyber security,[9] as well as guidance from global standard-setting bodies in their respective sub-sectors.
- **Financial exclusion considerations:** Where digital ID systems do not cover all, or most, persons within a jurisdiction, or where they exclude certain populations, they may drive (or at least fail to mitigate) financial exclusion. The mandatory use of a specific digital ID that is not universally available for CDD presents challenges similar to the prescriptive use of a documentary ID that is not accessible to the entire population.
    - Lack of access to digital technology or low levels of technological literacy may compound exclusion risks. For example, lack of access to mobile phones, smartphones, or other digital access devices, or lack of coverage and/or unreliable connectivity, may exclude poor and rural populations or women as well as those living in fragile and conflict-affected areas, such as refugees and displaced people.
    - Digital ID systems may also contribute to financial exclusion if they use biometric authentication without providing alternative mechanisms for authentication, as certain biometric modalities have greater failure rates for some vulnerable groups. For example, manual laborers may have worn fingerprints, which cannot be read by biometric readers; the elderly may experience frequent match failure, due to altered facial characteristics, hair loss, or other signs of aging, illness, or other factors; and certain ethnic groups and individuals with certain physical characteristics related to darker pigmentation, eye shape, or facial hair experience disproportionate facial recognition failures.
    - Special considerations for LFIs related to financial inclusion are discussed in section 5.2 below.

---

[8] See ica.gov.ae/en/ica-validation-gateway/.
[9] See id4d.worldbank.org/principles. Although developed to support the creation of "good" government-recognized ID systems, FATF's *Guidance on Digital ID* notes that they apply more broadly and can be adopted by both public- and privately-provided and used identity systems and services.

5. Assessing the Reliability and Independence of Digital ID Systems for CDD

Unless otherwise specified,[10] the UAE permits LFIs to adopt digital ID systems of their choosing, provided that they "rely upon technology, adequate governance, processes, and procedures that provide appropriate levels of confidence that the system produces accurate results."[11] This means that there is an appropriate level of confidence

(or "assurance," in the FATF's terminology) that the digital ID system works as it is supposed to and produces accurate results. The digital ID system should also be adequately protected against internal or external manipulation or falsification designed to fabricate and credential false identities or authenticate unauthorized users, including by cyberattack or insider malfeasance.

To this end, LFIs should conduct:

- An **assurance level assessment**, through which the LFI can understand the assurance levels that the digital ID system provides based on its technology, architecture, and governance and determine its reliability and independence; and

- An **appropriateness assessment**, through which the LFI can make a risk-based determination— given the digital ID system's assurance levels—of whether the digital ID system is appropriately reliable and independent for CDD in light of potential ML, TF, fraud, and other illicit financing risks.

As explained in greater detail below, these assessments should be performed sequentially. If an LFI cannot assess a digital ID system's assurance level or determines that it is not sufficiently reliable and independent for its purposes, it should not proceed with using the system for CDD unless it can be adequately strengthened or supplemented; in such a case, it is therefore not necessary to perform an appropriateness assessment until assurance concerns have been resolved.

Both an LFI's assurance assessment of a digital ID system and its determination of the system's appropriateness for CDD given its business and risk profile should be documented—whether as part of the institution's enterprise risk assessment or through a separate process—and updated on a periodic and event-driven basis. LFIs may determine which functional unit or team within the institution is best suited to carry out the assurance and appropriateness assessments; there is no requirement that these assessments be performed by a specific unit, such as an internal audit department.

---

[10] For example, as noted above, when verifying the Emirates ID card, LFIs should use the online validation gateway of the Federal Authority for Identity and Citizenship and keep a copy of the Emirates ID and its digital verification in their records; see ica.gov.ae/en/ica-validation-gateway/.
[11] Available at centralbank.ae/en/cbuae-amlcft; see p. 49.

5.1. Understanding the System's Assurance Levels

Where UAE law, regulation, or supervisory guidance has not mandated or prohibited the use of a specific digital ID system for CDD, LFIs should first determine, for any digital ID system it is considering adopting, the system's assurance levels.[12] In determining the reliability and independence of a given system, LFIs may either:

- Perform the assurance assessment themselves; or
- Obtain audit or certification information on assurance levels from an expert body.

Where an LFI performs the assurance assessment itself, it should conduct appropriate due diligence on the digital ID system provider, including the governance systems in place, and exercise additional caution. An LFI should only use information from an expert body, including another member of the same financial group or an independent third party, if it has a reasonable basis for concluding that the entity accurately applies appropriate, publicly disclosed assurance frameworks and standards.

Digital ID assurance frameworks and technical standards are a set of open source, consensus-driven assurance guidelines and best practices for digital ID systems that have been developed in several jurisdictions and by international organizations and industry bodies, and provide a useful tool for informing an LFI's or expert body's assurance assessment.[13] LFIs are encouraged to consider the reliability of each of the system's main digital ID components separately, as the same degree of reliability may not be required for each component of the digital ID

system (identity proofing/enrollment, authentication, or, if applicable, federation), depending on the relevant risk factors and mitigating measures in place.

Digital ID technology and architecture, and digital ID assurance frameworks and standards, are dynamic and evolving. The standards themselves are flexible and outcome-based in order to facilitate innovation. They permit different technologies and architectures to satisfy the requirements for different assurance levels and are framed in ways intended to help make them as future-proof as possible (e.g., by providing a floor, rather than a ceiling, for reliability).

Digital ID assurance frameworks and standards usually set out various, progressively more reliable assurance levels, with increasingly rigorous technical requirements, for each of the three main steps in a digital ID system. The technical standards provide ID reliability factors, in the form of assurance levels for the basic constituent processes of a digital ID system. Each assurance level reflects a specified level or certitude or confidence in the process at issue; a process with a higher assurance level is more reliable, while a process with a lower assurance level presents a greater risk of failure and is less reliable. This Guidance does not require or recommend any particular assurance level; rather, LFIs are expected to perform an assurance assessment and to determine what assurance levels for which processes are appropriate, given their ML, TF, fraud, and other illicit financing risks.

For illustrative purposes only, the following table summarizes and adapts some of the technical requirements from the NIST Digital ID Guidelines[14] for the **identity proofing and enrollment** stage of a digital ID system, which LFIs might leverage in assessing the degree to which a digital ID system is reliable and independent.

Reliability Factor	No Assurance	High Assurance	Very High Assurance
Presence	No requirements	In-person or remote proofing is permitted	Either in-person or supervised[15] remote proofing is required
Resolution	No requirements	Collection of as many identity attributes as necessary to achieve resolution into a single unique identity (i.e., to achieve de-duplication) is required; knowledge-based verification may be used for added confidence	Same as "High"
Evidence	No identity evidence is collected	Evidence of identity attributes is collected based on the **quality** of the evidence (classified as weak, fair, strong, or superior) and the **number** of documents or **quantity** of digital information relied upon	Same as "High," albeit with higher thresholds for evidence quality and quantity; use of biometrics is mandatory (noted below)
Validation	No validation	Each piece of evidence is validated as genuine and accurate against independent and reliable sources	Same as "High"
Verification	No verification	The identity evidence is verified, confirming that the validated identity relates to the individual applicant[16]	Identity evidence is verified by an authorized and trained credential service provider ("CSP") representative
Address Confirmation	No requirements for address confirmation	Required	Required
Biometric Collection	None	Optional	Mandatory
Security Controls	Not applicable	Moderate Baseline (per NIST Digital ID Guidelines)[17] or equivalent jurisdictional or industry standard	High Baseline (per NIST Digital ID Guidelines)18 or equivalent jurisdictional or industry standard

Likewise, the NIST Digital ID Guidelines set forth technical requirements for authentication protocols and processes (including credential and authenticator issuance and binding) and authenticator lifecycle management (including revocation in the event of loss or theft, and expiration/re-proofing and re-binding). For illustrative purposes only, the following table describes at a high level of generality some of the NIST requirements for **authentication** at various authentication assurance levels.[19]

Assurance Level	General Requirements
Some Assurance	• This assurance level can be achieved through a wide range of authentication technologies and authenticator types, and information security controls at a *low* baseline • Biometrics alone may be used as a single-factor authenticator at this level
High Assurance	• MFA is required (i.e., either a multi-factor authenticator or two single-factor authenticators), using secure authentication protocols that incorporate specified approved cryptographic techniques, and information security controls at a *moderate* baseline • More stringent requirements are imposed on authenticator types at this level[20] • Biometrics may be used as one authentication factor (something you are), with the device authenticated as a second factor (something you have), but cannot serve as the only authenticator type
Very High Assurance	• Requires MFA that uses both a hardware-based authenticator and an authenticator that provides verifier impersonation resistance, based on proof of possession of a key through an approved cryptographic protocol[21] • Claimants prove possession and control of two distinct authentication factors through secure authentication protocols, using approved cryptographic techniques • The authenticators are verifier impersonation resistant, replay resistant, and resist relevant side-channel attacks • When a biometric factor is used, the identity service provider (verifier) makes its own determination that the biometric sensor and subsequent processing meet specified performance requirements • The CSP employs appropriately tailored security controls at a *high* baseline

---

[12] Where the government of the UAE has mandated a specific digital ID system for CDD, as in the case of verifying the Emirates ID card via the online validation gateway of the Federal Authority for Identity and Citizenship, LFIs may rely on the government's assessment of such system's assurance levels.

[13] See, for example, FATF, *Guidance on Digital Identity*, Appendix D (Digital ID Assurance Framework and Technical Standard-Setting Bodies) and Appendix E (Overview of U.S. and EU Digital Assurance Frameworks and Technical Standards), available at: fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

[14] The NIST 800-63 Digital Identity Guidelines consists of a suite of documents: NIST SP 800-63-3 Digital Identity Guidelines (Overview); NIST SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing; NIST SP 800-63B Digital Identity Guidelines: Authentication and Life Cycle Management; and NIST SP 800-63C, Digital Identity

Guidelines: Federation and Assertions. For additional context, see Appendix E of the FATF *Guidance on Digital Identity*.

[15] Supervised remote proofing involves a remote interaction with the applicant that is supervised by an operator in accordance with specified requirements so as to achieve comparable levels of confidence and security to in-person identity proofing. NIST comparability requirements, are provided in Box 19 of Appendix E of the FATF *Guidance on Digital Identity*, at 96.

[16] As noted above, an LFI need not verify the accuracy of every element of identifying information obtained at the collection and resolution stage but should do so for enough information to form a reasonable belief it knows the true identity of the customer.

[17] See FATF, Guidance on Digital Identity, pp. 97-98.

[18] See FATF, Guidance on Digital Identity, pp. 97-98.

[19] Appendix E of the FATF *Guidance on Digital Identity* also presents summary of authentication assurance levels under EU Regulation No. 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.

[20] Under NIST standards, a "High" assurance level permits the use of any of the following multi-factor authenticators: multi-factor OTP device; multi-factor cryptographic software; or multi-factor cryptographic device. When a combination of two single-factor authenticators is used, one authenticator must be a memorized secret authenticator and the other must be possession-based (i.e., "something you have") and use any of the following: look-up secret; out-of-band device; single-factor OTP device; single-factor cryptographic software; or single-factor cryptographic device.

[21] The claimant uses a private key stored on the authenticator to prove possession and control of the authenticator. An IDSP (verifier), knowing the claimant's public key through some credential (typically, a public key certificate) uses an approved cryptographic authentication protocol to verify that the claimant has possession and control of the associated private key authenticator, and asserts the person's verified identity to the RP.

5.2. Determining Appropriate Usage in Context of Risk

Once the LFI is satisfied that it knows the assurance levels of the digital ID system, it should analyze whether the digital ID system is adequate for the purposes of performing CDD in the context of the relevant illicit financing risks associated with the LFI's customers, products and services, geographic areas of operations, and other relevant factors. Depending on the availability of digital ID systems, LFIs may have the option to select from multiple digital ID systems that have different assurance levels for identity proofing and authentication. In such circumstances, LFIs should match the robustness of the system's identity proofing and/or authentication processes to the type of potential illicit activities and level of ML/TF risks.

In choosing among digital ID systems providing the same assurance level, or selecting among varying levels of identity proofing and/or particular credentials and authenticators offered by a single system, LFIs should consider their specific ML/TF risks as they relate to identity proofing and authentication in selecting an option. LFIs may also have the option to choose appropriate digital ID systems for lower-risk scenarios.

Cabinet Decision No. (109) of 2023 on Regulating the Beneficial Owner Procedures

Cab Dec 109/2023 Effective from 16/11/2023 **Status:** In-Force

The Cabinet,

– Pursuant to the perusal of the Constitution;
– Federal Law No. (1) of 1972 on the Competencies of Ministries and Powers of Ministers, and its amendments;
– Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations;
– Federal Decree-Law no. (32) of 2021 on Commercial Companies;

– Federal Decree-Law no. (37) of 2021 on the Commercial Register;
– Cabinet Decision no. (58) of 2020 on the Regulation of the procedures of the Beneficial Owner; and
– Based on the proposal of the Minister of Economy, and the approval of the Council of Ministers,

Has resolved:

Article 1 Definitions

In implementing the provisions of the present Decision, the following terms and expressions shall have the meanings assigned thereto, unless the context otherwise requires:

Country:	The United Arab Emirates.
Ministry:	The Ministry of Economy.
Minister:	The Minister of Economy.
Decree-Law:	Federal Decree-Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations, and its amendments.
Implementing Regulation:	Cabinet Decision No. (10) of 2019 on the Implementing Regulation of Federal Decree-Law no. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations , and its amendments.
Registrar:	Authority having competence to supervise the trade names register for the various types of establishments registered in the Country.
Concerned Entity:	The governmental entity concerned with the implementation of any provision of the Decree-Law and the Implementing Regulation.
Beneficial Owner:	The natural person who ultimately owns or exercises ultimate control over a legal person, directly or through a chain of ownership or control, or other indirect means, as well as the natural person on whose behalf transactions are conducted or who exercises ultimate effective control over a legal person or a legal arrangement, specified in accordance with the text of Article (5) of this Decision.
Nominee Board Member:	Any natural person acting in accordance with the directions, instructions or will of another person. Nominee Board Member is officially appointed or holds a position in the legal person and usually represents shareholders, members or any other relevant entity.
Senior Management:	Decision-making authority of the legal person.
Beneficial Owner's Record:	Special register for the actual beneficiaries of the legal person, that includes all their data.
Register of Partners or Shareholders:	Special register for the partners or the shareholders of the legal person, that includes all their data.
Trustor:	Natural or legal person who transfers the management of his funds to a Trustee by virtue of a deed.

Trustee:	Natural or legal person who enjoys the rights and powers granted thereto by the Trustor or the Trust Fund, according to which such person shall undertake to manage, use and dispose of the Trustor's money in accordance with the conditions imposed on him by either of them.
Trust Fund:	Legal relationship whereby the Trustor places funds under the control of the Trustee for the benefit of a beneficiary or for a specific purpose. Such funds shall be considered as independent from the Trustee's money, and the right to the Trustee's money shall remain in the name of the Trustor or in the name of another person on behalf of the Trustor.
Higher Committee:	The higher committee supervising the national strategy on anti-money laundering and combating the Financing of terrorism.
Complex Ownership Structure:	An institutional mechanism that identifies a legal person as part of a group of different entities that are intricately linked to each other with the aim of concealing the identity of the natural person who owns or controls the legal person.
Governmental Partner:	A federal or local government that contributes or owns shares in the company.

Article 2 Objectives of the Decision

The present Decision aims to:

1- Contribute to the development of the business environment and the country's capabilities and economic standing in accordance with the international requirements by regulating the minimum obligations of the Registrar and legal persons in the country, including the procedures of licensing or registration, and regulation of the Beneficial Owner's Record and the Register of Partners or Shareholders.

2- Develop effective and sustainable executive and regulatory mechanisms and actions for the regulation of the procedures of the Beneficial Owners

Article 3 Scope of Application

1- The provisions of this decision shall apply to the Registrar and licensed or registered legal persons in the country including the commercial free zones.

2- Exempted from the provisions of this decision:

   a- Companies wholly owned by the Federal or Local Government or any other companies wholly owned by such companies.

   b- Financial Free Zones.

   c- Governmental Partner.

Article 4 Registration and Licensing of the Legal Person

1- The legal person, when applying for registration or a license, shall provide the registrar with the following essential data:

a- Name, legal form and articles of association.

b- Head office address or the main workplace, in case of foreign legal person, the name and address of their legal representative in the country shall be mentioned, and supporting documents shall be submitted as evidence to prove the aforementioned matter.

c- The Statute or any other similar documents approved by the Concerned Entity in the country.

d- The names of the relevant persons who hold senior management positions or managers at the legal person, who have the authority to issue decisions and their data is recorded based on the travel document or the civil card, its number, issuer and the date of its issuance and expiry.

2- A legal person may not be licensed or registered under a name that is previously registered in the country or under a name that is similar to an extent that leads to confusion.

3- A legal person shall refrain from using a name other than his registered name, and the name shall be followed by their legal form. The legal person may apply to the Registrar to change their name, and if approved, they shall be prohibited from using the cancelled name, and all their letters and documents shall clearly include their name and address in the country.

4- The legal person shall have a clear and detailed address that is registered in the country, notified to the Registrar, and used to receive all correspondence and notifications thereon.

Article 5 Identifying the Beneficial Owner

1- For the purposes of applying the provisions of this Decision, the Beneficial Owner of a legal person is whoever owns or exercises ultimate control over a legal person, through shares or stocks of direct or indirect ownership by 25% or more of the legal person's capital, or has the right to vote in it by 25% or more, including holding that ownership through a chain of ownership or control, or through control by any other means, such as the right to appoint or dismiss the majority of their Directors.

2- To identify the Beneficial Owner in accordance with Clause (1) of this Article, the risk-based approach of the Registrar shall be taken into account, especially in Complex Ownership Structures of a legal person.

3- The Beneficial Owner may be sued through any number of legal persons or any arrangements of any kind.

4- If more than one person participates in owning or controlling a percentage of the capital in the legal person, they shall all be treated as owners and controllers of this percentage.

5- If all possible means have been exhausted and no natural person with ultimate controlling ownership is identified as set out in Clause (1) of this Article or in case of a doubt that the natural person exercising control over the legal person through other means is the Beneficial Owner, then the natural person who exercises control over the legal person through other means shall be considered as the beneficial Owner.

6- Where no natural person is identified in accordance with Clause (4) of this Article; then the natural person who holds the position of a higher management official shall be deemed as the Beneficial Owner.

Article 6 Transparency and the Beneficial Owner

1- The legal person shall take reasonable measures to obtain and maintain adequate, accurate and up-to-date data on the Beneficial Owner

2- Legal persons licensed or registered in the country and owned by a company that is listed on a regulated market subject to disclosure requirements that impose requirements to ensure sufficient transparency for the Beneficial Owner or a majority-owned subsidiary of that listed company shall be exempt from applying the provision of Clause (1) of this Article.

Article 7 Notifications Relating to the Beneficial Owner

1- If it appears to the legal person that there is a natural person who could be a Beneficial Owner, and their ownership details are not correctly registered in the Beneficial Owner's Record, then the legal person shall inquire about the status of that person as their Beneficial Owner. If a period of (15) Fifteen days from the date of the inquiry lapses without a response, the legal person shall notify them of that.

2- The notification referred to in Clause (1) of this Article shall include the following:

a- Evidence of the issuance of the notification pursuant to this Decision.

b- Details of the data related to him being a Beneficial Owner, which the legal person believes to be correct, with a request to provide the missing data required to complete the data of the Beneficial Owners' Register.

c- Requesting the following from the addressee:

1) An indication of whether or not such addressee is the Beneficial Owner of the legal person

2) Confirmation or correction of any details included in the notification

3) Submission of any missing data in the notification.

3- If the addressee fails to comply with the notification within (15) fifteen days from the date of sending it, the legal person shall include the notified details in the Beneficial Owners' Register.

4- A legal person, for the purpose of determining the identity of the Beneficiary Owner, may rely on the person's response that is written on the notification, unless the legal person has reasonable grounds to suspect that the answer is misleading or incorrect, in which case the legal person shall record details of the nature of ownership of this person as Beneficial Owner and notify said person of that.

Article 8 Owner's Register

1- The legal person shall keep the details of each Beneficial Owner in the record of the Beneficial Owner that they create within (60) sixty days from the date of issuance of this decision or from the date of its existence, and shall update this record and include any change in it within fifteen (15) days from the date of taking knowledge thereof.

2- The Beneficial Owner's Record shall include the data of each Beneficial Owner, as follows:

a- The full name, nationality, and date and place of birth.

b- The place of residence or the address to which notifications are to be sent under this Decision.

c- The number of the travel document or the identity card, as well as the country and date of issuance and expiry

d- The basis and date on which the person became Beneficial Owner of the legal person.

e- The date on which the Person ceased to be a Beneficial Owner of the legal person.

3- If the legal person includes the name of a natural person in the Beneficial Owner Record as Beneficial Owner and this natural person does not provide himself or with his knowledge the data and details related to him, then the legal person shall notify him within (15) fifteen days from the date of including his name.

4- Anyone with a capacity or interest may submit to the Registrar a request to correct the Beneficial Owner's record, in the case that the name of any person is included or deleted from the Beneficial Owner register without sufficient reason on the part of the Registrar.

5- The Legal Person may not register or give effect to any document relating to a change in its ownership, unless a statement is provided by or on behalf of the transferee, which states whether the transfer will result in a change in the Beneficial Owner for the Legal Person, and the nature of such change or no. The said statement shall include the data of the new Beneficial Owner and to be entered into the Register.

Article 9 Nominee Board Members

1- The manager or Board Member who acts as a nominee board member shall notify the legal person that he is a nominee member, and submit all the data referred to in Article (10) of this Decision within (15) fifteen days from the date of acquiring this capacity. The Nominee Board Member that has acquired this status prior to the publication of this decision shall notify the legal person of the matter within (30) thirty days from the date of its publication.

2- The Nominee Board member shall notify the legal person of any change in the data referred to in Article (10) of this Decision, within (15) fifteen days from the date of making this change.

3- A Nominee Board Member shall inform the Legal Person that he ceased to be a nominee Board Member within (15) fifteen days of such cessation.

Article 10 Register of Partners or Shareholders

1- A legal person must maintain the details of data of each partner or shareholder in the Register of Partners or Shareholders, and must update and record any change to the Register within (15) fifteen days of becoming aware of such change. The Register of Partners and Shareholders shall include:

a- The number of shares or stocks owned by each of them, their categories, and associated voting rights.

b- The date of acquiring capacity as a partner or shareholder.

c- For partners or shareholders from among natural persons: The full name according to what is mentioned in the identity card or travel document, as well as the nationality, address, place of birth, and the name and

address of the employer, along with a true copy of a valid identity card or the travel document.

d- For partners or shareholders from among legal persons: Providing the data mentioned in Clause (1) of Article (4) of this Decision.

2- A legal person who has one or more partners or shareholders, acting as a Trustee or as a Nominee Board member shall have his data recorded in the Register of Partners or Shareholders.

3- The register of Partners or Shareholders shall include the data of the persons represented by each Trustee or Nominee Board Member as stated in Clause (2) of Article (8) of this Decision.

Article 11 Provision of Information to the Registrar

1- The legal person shall, within (60) sixty days from the date of enforcement of this Decision or from the date of licensing and registration of the legal person, submit the data of the Beneficial Owner's Records and the Register of Partners or Shareholders to the Registrar, and take reasonable measures to protect their records from damage, loss or destruction.

2- The legal person shall provide any additional data the Registrar requests within (14) Fourteen days from the date of request.

3- Subject to the legislation in force, the legal person shall submit all the data referred to in Clause (1) of Article (4) of this Decision to the Registrar when requesting incorporation, licensing, registration, renewal, modification or other cases as may be deemed as necessary for this purpose by the Registrar.

4- Each legal person shall provide the Registrar with the name of a natural person residing in the country who is authorized to disclose to the Registrar all the data and information required by the aforementioned Law or Implementing Regulation or this Decision, as well as his address, contact details and a valid copy of his travel document or identity card.

5- The licensed or registered Legal Person in the country should not issue bearer share warrants.

6- When issuing shares or stocks in the name of persons or Board members, the legal person shall disclose within (15) fifteen days the details of such shares or stocks and the identity of the persons and Board members to the Registrar.

7- If the legal person is in the stage of dissolution or liquidation, the liquidator shall deliver the Beneficial Owner's Record and the Register of Partners or Shareholders, if any, or a true copy thereof to the Registrar within (30) thirty days from the date of his appointment.

8- The liquidator shall keep Records and all data included in this Decision for a period of (5) five years at least from the date of dissolution or liquidation.

Article 12 Notifications Issued by the Registrar

1- The Registrar shall notify the legal person, its employees, or its authorized agents to submit data or documents related to the Beneficial Owners or Nominee Board Member within the period specified in the notification.

2- The powers conferred upon the Registrar under Clause (1) of this Article shall include the following:

a- Taking copies of the submitted documents according to the conditions that the Registrar deems appropriate.

b- Asking the person who is required to submit data or documents, in case they are not submitted, to indicate their location, to appear at the time and place specified by the Registrar and to answer any questions related to any matters for which data is required to be submitted.

3- Attorneys and other independent legal professionals and independent statutory auditors shall be exempt from submitting any data required in the notification if obtained in the course of their assessment of the legal status of the legal person, his defense or his representation before the judiciary, or the arbitration, mediation or conciliation procedures or the provision of a legal opinion on a matter related to judicial proceedings, including advising on initiating or avoiding such proceedings or inquiring about them whether such data were obtained before, during or after judicial proceedings or in other circumstances in which they are subject to professional secrecy.

Article 13 Obligations of the Registrar

The Registrar shall undertake to:

1- Preparing templates, notifications and guidance manuals by various means related to registration and licensing procedures or organizing the procedures of the Beneficial Owner in the required form that achieves effectiveness in accordance with this Decision and relevant legislation.

2- Provide adequate human resources to enable him to effectively carry out his duties.

3- Automate the data obtained thereby and classify them in a way that facilitates reference to such data and their exchange with the concerned entities upon request.

4- Providing the required data regarding the National Economic Register instantaneously and providing any other data requested by the Ministry immediately.

5- Provide data on the legal persons in the country and make them available to the public as follows:

a- Describing the different types and forms and the basic features.

b- Procedures for the licensing or registration.

c- Providing the basic data mentioned in Clause (1) of Article (4) of this Decision.

d- Measures for obtaining data related to the Beneficial Owner.

6- Maintain the basic data mentioned in Clause (1) of Article (4) of this Decision, ensure that its accuracy, up-to-date and available to the public.

7- Obtain the data of the Beneficial Owner when licensing or registering the legal person, update the data, and ensure its accuracy.

8- Maintain all records received by virtue of Clause (8) of Article (11) of this Decision for a period of (5) five years from the date the legal person is cancelled through dissolution, liquidation or deregistration.

9- Update the basic data mentioned in Clause (1) of Article (4) of this Decision, the data of the Beneficial Owner's Record, the Register of Partners or Shareholders instantaneously, based on the data provided by the legal person, provide them to the Ministry and disclose them at the request of the concerned authorities.

10- Applying a risk-based approach which was approved by the Ministry to all legal persons registered, in order to ensure that the legal person is not misused for the purposes of money laundering and financing of terrorism crimes through the following:

a- Annually Classifying and assessing potential risks related to money laundering and the financing of terrorism operations and addressing and mitigating them.

b- Taking the necessary measures to reduce these risks and prevent their occurrence through assessing the risks of legal persons, verifying and monitoring them.

c- Implementing the procedures required for risk management, and ensuring their effective implementation.

Article 14 Establishment of the Unit of Anti-Money Laundering and the Financing of Terrorism at the Registrar

1- An administrative unit shall be established at the Registrar concerned with implementing policies, procedures, and requirements for anti-money laundering crimes, combating the financing of terrorism, and the financing of illegal organizations in accordance with the provisions stipulated in the Decree Law, its implementing regulations, and relevant supervisory decisions. The Unit must submit reports and developments instantaneously to the Ministry.

2- The Registrar shall issue a decision to specify the mechanism and tasks of the Unit after coordination with the Ministry.

3- The Unit shall report to the higher management at the Registrar.

Article 15 Change of Data

1- A legal person shall keep all basic data under Article (8) of this Decision, the data of the Register of Partners or Shareholders, data of the Beneficial Owner, data of the records associated thereto and any other data or information he may be required to keep under the legislation in force, provided that they are accurate and up to date.

2- The legal person shall submit any amendment or change to the data or information under this Decision to the Registrar within (15) fifteen days from the date of the amendment or change.

Article 16 Data confidentiality

1- The Ministry and the Registrar are prohibited from disclosing the data of the Beneficial Owner Record or the register of partners or shareholders and making them available to any person, unless they obtain written approval from the Beneficial Owner or the nominee management member.

2- Exempted from the provision of Clause (1) in this Article are:

a- Disclosure obligations stipulated in this decision.

b- What is stipulated in the international laws and agreements in force in the country, especially the provisions related to combating money laundering crimes, combating the financing of terrorism, financing illegal organizations, and exchanging information in tax matters.

Article 17 Local and International Cooperation

1- The Ministry shall provide the basic data mentioned in Clause (1) of Article (4) of this Decision, as well as the data of the Beneficial Owner's Record and the Register of Partners or Shareholders, to the concerned entities in the country upon request.

2- The Ministry shall provide means of international cooperation concerning the basic data of the legal person, the data of the Beneficial Owner's Record and the Register of Partners or Shareholders, provided that this cooperation includes the following:

a- Facilitating access by the competent foreign authorities to the basic data available in the records of the legal person upon request.

b- Exchanging data and information about the partners or shareholders of the legal person.

c- Using its powers to obtain all the data of the Beneficial Owner on behalf of the foreign counterparts.

3- The Ministry shall supervise the quality of implementation of international cooperation processes received from other countries with regard to requests to obtain basic data of legal persons and data of their Beneficial Owner, as well as the international cooperation requests regarding knowing the whereabouts of the beneficial owners outside the country.

Article 18 Administrative Penalties

In the event of a violation of the provisions of this Decision, the Registrar may impose one or more penalties from the list of administrative penalties issued by a Cabinet Decision based on the proposal of the Minister of Finance and after coordination with the Minister.

Article 19 Grievance

1- Whoever has capacity may file a grievance with the Registrar to the Grievances Committee on the administrative penalties that were imposed in accordance with the provisions of Article (18) of this Decision within (30) thirty days from the date of notification, and may submit a request to stop the implementation of administrative penalties, and the Committee shall decide on this request within (45) forty-five working days in accordance with the procedures applied thereby.

2- The Minister shall issue a decision in coordination with the Registrar specifying the terms and conditions of grievances against the Decisions on administrative penalties before Grievances Committee with the Registrar.

Article 20 Control Procedures

The Ministry, in accordance with the supervisory role assigned to it, in coordination with the Registrar, may establish the methods and procedures it deems necessary to supervise the extent of the Registrar's compliance with the

provisions of this Decision and the decisions implementing it.

Article 21 Compliance Reports

1- The Registrar shall submit semi-annual reports to the Minister on the extent of his compliance with the requirements of the provisions of this Decision and related legislation.

2- The Minister shall submit reports on the results of the Registrar's compliance to the Higher Committee.

3- The Higher Committee shall submit reports on the results of the Registrar's compliance to the Council of Ministers and/or the Executive Councils in each Emirate, as the case may be.

Article 22 Abrogation

Cabinet Decision No. (58) of 2020 on the Regulation of the procedures of the Beneficial Owner as well as any provision that violating or conflicting with the provisions of this Decision shall be abrogated.

Article 23 Decision Promulgation and Entry into Force

The present Decision shall be published in the Official Gazette, and shall come into force from the day following the date of its publication.

Cabinet Decision 74 of 2020: Terrorism Lists Regulation and Implementation of UN Security Council Resolutions

CAB DEC 74/2020 Effective from 27/10/2020 **Status:** In-Force

The Cabinet:

- Having perused the Constitution,

- Federal Law No (1) of 1972 on the Mandates of Ministries and Powers of Ministers, and amendments thereto;

- Federal Law No. (17) of 2006 on the Establishment of the Supreme Council for National Security;

- Federal Law No. (13) of 2007 on Goods Subjected to Import and Export Control, and amendments thereto;

- Federal Law No. (7) of 2014 on Combating Terrorism Offences;

- Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organizations;

- Cabinet Decision No. (20) of 2019 on Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and Proliferation of Weapons of Mass Destruction, and Relevant Resolutions, and

- Based on the proposal of the Minister of Foreign Affairs and International Cooperation and the Cabinet's approval;

Resolved as follows:

Article 1 - Definitions

In the implementation of the provisions of this Decision, and unless the context otherwise requires, the following terms and expressions shall have the meanings cited against each:

The State: The United Arab Emirates;

The Council: The Supreme Council for National Security;

The Ministry: The Ministry of Foreign Affairs & International Cooperation;

The Competent Court: The Court that has jurisdiction over State Security Offences;

The Office: The Executive Office of the Committee for Goods Subjected to Import and Export Control;

Supervisory Authorities: Federal and Local authorities entrusted as per Legislations, with the supervision of Financial Institutions and Designated Non-Financial Businesses and Professions.

Law Enforcement Authorities: Federal and Local authorities entrusted, as per Legislations with the tasks of combating crime, search, investigation, and collection of evidence in offences, including money laundering, financing of terrorism and the financing of illegal organizations.

Sanctions Committee: Any of the UN Security Council Committees established as per its resolutions, including UNSCRs 1267 (1999) and 1989 (2011) relating to ISIL and Al-Qaida, 1988 (2011) relating to the Security and Stability of Afghanistan, and 1718 (2006) relating to the suppression and combating of proliferation of weapons of mass destruction for the DPRK.

Listed Person: A person or organization listed by the UN Security Council on the Sanctions List, or listed by the Cabinet on Local Lists, as the case may be.

Person: A natural or legal person.

Ombudsperson: The person appointed by the UN Secretary General to assist the Sanctions Committee when examining requests submitted by individuals, groups, undertakings and entities for delisting from the ISIL and Al Qaeda Sanctions List.

Focal Point: The focal point established within the Secretariat pursuant to UNSCR 1730 (2006) to receive petitions from persons or entities in the State or holding the State's nationality, listed on the relevant list, requesting to be de-listed or seeking exemptions for humanitarian reasons, from a travel ban, or from freezing measures or persons claiming to have been wrongfully sanctioned.

Relevant UNSCRs: All current and future UN Security Council resolutions relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.

Listing: Identifying the individual or organization subject to sanctions imposed pursuant to relevant UNSCRs, decisions of the Sanctions Committee, or relevant decisions of the Cabinet, as the case may be, and implementing relevant sanctions against such individual or organization, with a statement of the reasons for listing.

Local Lists: Terrorism lists issued by the Cabinet pursuant to the provisions of Article (63) paragraph (1) of Federal Law No (7) of 2014.

Sanctions List: A list containing the names of individuals and organizations linked to terrorism, financing of terrorism or proliferation of weapons of mass destruction and its financing, and that are subject to sanctions imposed as per UNSCRs and decisions of the Sanctions Committee, along with information related to such persons and reasons for their listing.

Narrative Summary: The declared part of the reasons for Listing an individual or organization on the Sanctions List annexed to the Listing decision by the Sanctions Committee.

Funds: Assets of all types, in whatever form and however acquired, whether corporeal or incorporeal, tangible or intangible, movable or immovable, electronic, digital or encrypted, including national currency, foreign currencies,

documents and legal instruments establishing ownership of such assets or any associated rights, in whatever form, including electronic or digital forms, as well as economic resources considered as assets of any kind, including oil and natural resources, and bank credits, checks, money orders, shares, securities, bonds, drafts, and letters of credit and any interest, dividends, or other income accruing from or generated by such assets, and that may be used to obtain any other funds, goods or services including internet posting services or related services.

Other Measures: Sanction measures other than freezing that must be enforced, and which may be included in relevant UNSCRs or Cabinet decisions regarding the issuance of local lists, such as prohibitions relating to travel, weapons, imports, or provision of fuel supplies and other.

Without Delay: Within 24 hours of the Listing decision being issued by the UN Security Council, the Sanctions Committee or the Cabinet, as the case may be.

Article 2 - Mandate of the Council

1. For the purposes of implementing the provisions of this decision, the Council shall have the following mandate:

    a. Establish one Local List or more, where it proposes the listing, de-listing or re-listing of terrorist persons and organizations and the updating of such list, whether spontaneously or upon the request of another country, or in case the State has an international obligation to list such persons or organizations.

    b. Coordinate with other countries to list a terrorist person or organization in their local terrorist lists.

    c. Propose the listing of terrorist persons or organizations on the Local List to the Sanctions Committee.

    d. Submit requests for de-listing terrorist persons or organizations from the Sanctions List, when it believes that such terrorist persons or organizations do not or no longer meet the designation criteria, while taking into account procedures and criteria set out in relevant UNSCRs.

    e. Conduct a regular review of Local Lists in coordination with the Ministry of Justice. The Council is entitled to request any clarifications or document it deems suitable from Law Enforcement Authorities and concerned entities in the State to review such, provided that the period for review does not exceed one year.

2. The Council shall exercise its powers set forth in sub-paragraphs a, b and c of paragraph 1 of this Article in accordance with the rules and procedures set forth in Relevant UNSCRs, whenever there are reasonable grounds for such, irrespective of the existence of criminal proceedings.

Article 3 - Proposing Listing and Re-listing on Local Lists and Updating Such

Subject to the provisions of Article (2) Paragraph (2) of the present Decision, the Council shall coordinate with any entity it deems suitable in the State and abroad to obtain information regarding the designation of terrorist persons and organizations that meet the designation criteria for the purpose of preparing a proposal for listing on Local Lists according to the following procedures:

1. The Council shall, unilaterally and without prior notice to the Listed Person, establish one Local List or more where it proposes the Listing of terrorist persons and organizations, or propose Listing upon the request of another country, whenever the Council is satisfied with the presence of reasonable grounds or sound basis for suspicion or when it believes that such person or organization meets the designation criteria for Listing, or if the State is internationally committed to list such persons and organizations. The Council shall take such decision as swiftly as possible.

2. In the Listing process, the Council shall take into account the designation criteria contained in UNSCR 1373 (2001), which include the following:

    a. Any person or organization that commits, attempts to commit, participates in or facilitates the commission of terrorist acts.

    b. Any organization directly or indirectly owned or controlled by a person or organization as set out in sub-paragraph (a) of paragraph (2) of the present Article.

    c. Any person or organization acting on behalf of or at the direction of any person or organization as set out in sub-paragraph (a) of paragraph (2) of the present Article.

3. The Council shall coordinate with the Ministry of Justice with regard to proposed Listing on Local Lists, if the Council determines that a person or an organization meets the designation criteria referred to in paragraph (2) of the present Article. The Council then forwards the proposal to the Ministry of Presidential Affairs for consideration and issuing by the Cabinet.

4. In case Local Lists were issued by the Cabinet, the Office shall be notified for publication, Without Delay, as per its established procedures.

5. The procedures set forth in the present Article shall be implemented when Local Lists are updated, and when re-listing any previously de-listed person, in case there are reasons requiring their Listing in such lists, in accordance with the provisions of paragraph (2) of the present Article.

Article 4 - De-listing From Local Lists

The Council may de-list a Listed Person from Local Lists according to the following procedures:

1. The Council shall notify the Ministry of Presidential Affairs of reasons to de-list, if it considers that the information or evidence regarding a Listed Person on the Local List no longer require their listing, and once it has verified that the reasons for the Listing no longer exist.

2. The Ministry of Presidential Affairs shall be in charge of submitting the proposal to de-list the Listed Person from the Local Lists to the Cabinet, in order for the Cabinet to decide whether to approve or reject the request.

3. The Office shall be notified of the de-listing decision referred to under paragraph (2) of the present Article, immediately upon issuance thereof, to circulate the decision, lift freezing and any other measures taken, as per its established procedures.

Article 5 - Enforcement and Publication of Local Lists

1. Decisions to list, de-list and re-list on Local Lists, and to update such lists shall be effective from the date of their issuance, or from the date determined by the Cabinet, and shall be published in the Official Gazette.

2. Decisions to list, de-list and re-list on Local Lists, and to update such lists shall be published in the media, in both Arabic and English, as per the regulations established by the Council.

Article 6 - Grievances Against Decisions to List on Local Lists

Anyone whose name is listed on Local Lists may file a grievance against such decision according to the following procedure:

1. The Listed Person may submit, in person or through a legal representative, a written grievance application to the Office, in accordance with the latter's established mechanism, attaching thereto all documents supporting the grievance.

2. The Office shall refer the grievance to the Council for review and examination. Both the Office and the Council shall have the right to request any clarifications or further documentation from the applicant, or from Law Enforcement Authorities or other relevant entities in the State, for the purposes of deciding on the application.

3. The Council shall receive the grievance application, verify whether it is new or recurring, and may reject it, if it was recurring and did not include additional information other than the information contained in the previous grievance, or for any other reasons.

4. If the Council, during its review of the grievance application, determines that the information or evidence regarding the Listed Person on Local List no longer require their listing, and once it has confirmed that the reasons that called for the Listing no longer exist, the Council shall notify the Ministry of Presidential Affairs.

5. The Minister of Presidential Affairs shall be in charge of submitting the grievance application, along with the Council's opinion to the Cabinet, as per its established submittal mechanisms, in order for the Cabinet to make a decision to either approve or reject the grievance.

6. In case of approval of the grievance by the Cabinet, the name of the Listed Person shall be removed from Local Lists and freezing and other measures taken in accordance with the Listing decision shall be lifted. The Office shall be notified immediately upon issuance thereof to notify the applicant and publish the decision as per the Office's established procedures.

7. In case the grievance is rejected or if no response is received regarding the application within sixty days from the date of its submission, the applicant may appeal the Cabinet's Listing decision before the Competent Court within sixty days from the date he/she was notified of the rejection, or from the expiry of the response period.

8. The court's decision regarding the grievance shall be not be subject to appeal. If a grievance is rejected, a new grievance may only be submitted after six months from the date of rejection of the previous grievance, unless a serious reason that is accepted by the president of the court arises before the expiry of such period.

9. An appeal against a Listing or re-Listing decision shall not be accepted before a grievance against it is filed and rejected, or before the period given to respond expires, as set out in the present Article.

Article 7 - Lifting Freezing and Other Measures in the Case of False Positives on Local Lists

Any person or organization inadvertently affected by freezing or other measures due to a similarity between their name and the name of a Listed Person on Local Lists, and any person or organization that has been affected by such measures may cancel such procedures as follows:

1. Submitting a written request to the Office, in person or through a legal representative, to lift freezing or any other measures taken against them, along with all supporting documents.

2. The Office shall refer the request to the Council for examination. Both the Office and the Council may ask for any clarifications or additional documents from the applicant, Law Enforcement Authorities or relevant entities in the

State, for the purpose of deciding on the request.

3. After examining that the applicant or his/her funds are not related to the Listing, the Council shall issue its decision to accept or reject the request, and shall send such decision, within thirty days from date of receipt of the request to the Office, which would in turn notify the applicant of the outcome in writing.

4. In case the request is accepted by the Council, the Office shall address the entity where the funds are frozen, Law Enforcement Authorities and the entities concerned with Other Measures, to lift the actions taken against the applicant. The addressed entity should immediately execute the decision.

5. In case the request is rejected by the Council, or if no response to the request is received within thirty days from date of its submission, the applicant may file a grievance before the Competent Court within sixty days from the date of notification of the rejection, or from the expiry of the response period.

6. The court's decision on the grievance shall be not be subject to appeal, and if the court ruled to reject the grievance, a new grievance may only be filed after six months from the date of rejection of the grievance, unless a serious reason that is accepted by the president of the court arises before the expiry of such period.

7. An appeal against a decision to apply freezing and Other Measures shall not be accepted before a grievance against such is filed and rejected, or before the period given to respond expires, as set out in the present Article.

Article 8 - Permission to Use Funds Frozen pursuant to Listing on Local Lists

1. Any Listed Person on Local Lists, or their legal representative, and any interested party may submit to the Office a written request to use the Listed Person's frozen Funds. The Office shall refer the request to the Ministry of Justice, provided such request includes all supporting documents.

2. The Ministry of Justice shall examine the request, its reasons and the amounts to which access is requested and may reduce such amounts or reject the request based on justified reasons.

3. Following coordination with the Council, The Ministry of Justice may approve the request to use the frozen funds of a Listed Person on Local Lists, for any of the following purposes:

    a. To cover necessary or basic expenses, such as the amounts payable for foodstuff, rent, mortgage, medicine, medical treatment, taxes, insurance premium, educational or judicial fees, or public utility fees.

    b. To pay professional fees or costs relating to legal services rendered or other extraordinary expenses within reasonable limits; or fees for services relating to safekeeping or management of frozen Funds.

4. The Ministry of Justice shall notify the Office of the approval or rejection of the request, and the Office shall in turn notify the applicant of the decision in writing.

5. In case the request is rejected, or if no response to the request is received within thirty days from date of its submission, the applicant may file a grievance before the Competent Court within thirty days from the date when he/she was notified of the rejection, or from the expiry of the response period.

6. An appeal against the rejection of the request shall not be accepted before a grievance against it is filed and rejected, before the period given to respond expires, as set out in the present Article.

7. In all cases, the procedures set forth in UNSCR 1452 (2002) and any successor resolutions shall be taken into account.

Article 9 - Request to Listing on Another Country's List

Subject to paragraph (2) of Article (2) of the present Decision, the Council may, unilaterally, request a foreign country to list a person or organization that meets the designation criteria under UNSCR 1373 (2001) on the local list of such country, through the following procedures:

1. Communicate through diplomatic or established security channels with the country of nationality or previous or current residence of the person or organization, to obtain, as much as possible, information supporting the Listing request.

2. The Listing request should include as much details as possible on the grounds and justifications of such request and may include the following:

    a. Specific information supporting links to terrorist organizations, individuals or activities or otherwise establishing that the person or organization meets the designation criteria.

    b. Evidence or documents supporting the Listing request such as reports from Law Enforcement Authorities, security services, the Judiciary, the media and others.

3. The Council shall attach to the Listing request all personal information to enable accurate and positive identification of the person requested for listing, along with all data and information supporting that the person requested for listing meets the designation criteria set forth in UNSCR 1373 (2001).

4. The Council shall send the Listing request to the Ministry, which would in turn address the concerned country and notify the Council upon receipt of the response.

Article 10 - Proposal for Listing to the Sanctions Committee

Subject to paragraph (2) of Article (2) of the present Decision, and if the Council is satisfied that there are reasonable grounds or a sound basis to suspect or believe that a person or organization meets the designation criteria for Listing on the Sanctions List, the Council may, unilaterally and without prior notice, propose Listing on the relevant Sanctions List of any person or organization, by submitting such proposal to the Security Council or the concerned Sanctions Committee such as those established pursuant to UNSCRs 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and 2231 (2015) for designation and successor resolutions, while taking into account the relevant designation criteria and using the standard forms approved by the relevant committee for Listing in accordance with the following procedures:

1. The Council shall seek to collect information about the person or organization proposed for Listing using the assistance of Law Enforcement Authorities and relevant entities in the State, for the purposes of preparing the proposal for Listing on the Sanctions List.

2. The Council shall communicate, through diplomatic or established security channels with the country of nationality or current or past residence of the proposed person in order to obtain information, if possible.

3. The Listing proposal must include a detailed statement of the case to support the proposed Listing, and the specific criteria on the basis of which the name of the person or organization was proposed for Listing, including:

a. Specific results and reasons showing fulfillment of the Listing criteria as set out in relevant UNSCRs or by the relevant Sanctions Committee.

b. Evidence or documents supporting the Listing proposal such as reports of Law Enforcement Authorities, security services, the Judiciary, the media and others.

c. Details on any relationship with a person currently listed on the Sanctions List.

4. The Council shall work on providing a statement of information to the extent possible as per the Consolidated Form for the purposes of Listing on the relevant Sanctions List.

5. The Listing proposal must include a statement by the State as to whether the Sanctions Committee can disclose that the State is the entity requesting the listing or not.

6. The Council shall send the Listing proposal to the relevant Sanctions Committee through the Office.

Article 11 - Mandate of the Office

For the purposes of implementing the provisions of the present Decision, the Office - as a National Coordination Body - shall have the following mandate:

1. Take necessary measures to implement UN Security Council resolutions, Without Delay and without prior notice to the Listed Person, in accordance with the requirements thereof, particularly resolutions related to Terrorism, Terrorist Financing and the Prevention, Suppression and Disruption of Proliferation of Weapons of Mass Destruction and its Financing.

2. Publish the Sanctions List and the updated Local Lists on the Office's website, Without Delay.

3. Notify a Listed Person residing in the State of their Listing, after the completion of the Funds freezing procedures, and provide such Listed Person with the Narrative Summary directly, or with the necessary information on the reasons for their listing, and explain the implications of their Listing on the Sanctions List, the procedures that the Sanctions Committee follows in considering requests for de-listing from the Sanctions List, including the possibility of submitting such requests to the Ombudsperson or Focal Point, as the case may be, in addition to the possibility of using part of the Funds frozen in accordance with the provisions of the present Decision , by making this information available on the Office's website.

4. Receive and process notifications relating to measures taken in implementation of the relevant UNSCR or Local Lists.

5. Receive grievances against Listing on Local Lists, requests for lifting freezing or Other Measures taken against persons with names similar to the names of Listed Persons, in addition to requests for using frozen Funds.

6. Internal coordination and exchange of information between concerned entities regarding the implementation of the provisions of the present Decision, including coordination to develop typology reports on the evasion of freezing and Other Measures, and cooperation with the Financial Intelligence Unit (FIU) in developing red flags at financial institutions and DNFBPs related to evading freezing and Other Measures.

7. Collect the results of supervision and enforcement measures from Supervisory Authorities related to implementing the provisions of the present Decision and coordinate efforts in this regard.

8. Communicate and engage with FIs, DNFBPs and the public with regards to the implementation of the provisions of the present Decision, including by providing training, outreach and awareness raising in coordination with

Supervisory Authorities, in order to enhance effectiveness at the level of receiving notifications from the Office related to the Sanctions List and Local Lists, Without Delay; and issue the necessary instructions on compliance and collect statistics related to the implementation of the present Decision.

Article 12 - Publication of the Sanctions List, Local Lists, and Implementation of Related Decisions

1. The Office shall publish Sanctions List and Local Lists by sending them using the means it deems appropriate to Supervisory Authorities, financial institutions and DNFBPs for the implementation of the freezing decision, and to Law Enforcement Authorities for the implementation of Other Measures, Without Delay and without prior notice to the Listed Person.

2. Law Enforcement Authorities and Supervisory Authorities shall provide the Office with any information, if applicable, regarding the outcome of the implementation of the freezing or Other Measures, as the case may be, within five business days from the date of implementation.

3. The Office shall send the data and information received from Supervisory Authorities and Law Enforcement Authorities to the UN Security Council and the Sanctions Committee, as the case may be, through the Ministry.

4. The Office shall send information and data received from Supervisory Authorities and Law Enforcement Authorities regarding measures taken in relation to Local Lists, to the Council.

Article 13 - Declared Procedures Relating to Sanctions List

The Office shall state, on its official website, procedures for submitting requests for de-listing from the Sanctions List, including the following procedures:

1. Guiding Listed Person as per relevant UNSCRs to submit a de-listing request to the Ombudsperson or Focal Point directly, as the case may be, showing the applicable steps to submit a request as indicated below:

    a. Submit a request to the Focal Point or the Ombudsperson, as the case may be, to verify such, coordinate with the concerned states and present the request to the relevant Sanctions Committee.

    b. The Office shall receive, from the Ombudsperson or the Focal Point, the additional information request related to the Listed Person's request for de-listing.

    c. The Office shall coordinate with the concerned authorities it deems appropriate to examine the request for additional information during the period specified by the Ombudsperson or Focal Point, and provide them with its observations and to what extent the Listed Person or organization is entitled to be de-listed. The Office may ask any questions or ask for more clarifications from the Listed Person submitting the request and shall respond to any other queries raised by the Ombudsperson or Focal Point.

2. Procedures to lift freezing measures imposed due a false positive.

3. Cases where access to frozen Funds is permitted and cases of exemption from Other Measures.

4. Mechanisms for notifying Supervisory Authorities, Law Enforcement Authorities, Financial Institutions and DNFBPs of cases of de-listing or lifting of freezing measures.

Article 14

1. The Office shall submit a request for de-listing a deceased person or a defunct organization from the Sanctions List and Local Lists, to the Ombudsperson or Focal Point, as the case may be, along with a death certificate for natural persons and any information proving that the organization no longer exists or is no longer active.

2. The Office shall take necessary actions to ensure, in coordination with concerned entities, that the funds that were in the possession of the Listed Person are not transferred or at any time distributed to other persons listed on the Sanctions List or Local Lists, including ensuring that none of the legal heirs or beneficiaries of the Funds is listed on the Sanctions List or Local Lists, and the Office should notify the Ombudsperson or Focal Point, as the case may be, to such effect.

3. The Office shall take necessary actions to lift the freezing of Funds of Listed Person referred to in the present Article, after receiving the response of the Ombudsperson or Focal Point, as the case may be. If the State was the party that proposed the Listing on the Sanctions List, and a de-listing request was submitted to the Ombudsman or Focal Point, the Office shall examine the request in coordination with the Council and shall proceed with the actions mentioned the present Article.

Article 15 - Freezing Funds As per the Sanctions List & Local Lists

1. Any person shall, Without Delay and without prior notice, freeze Funds as per the Sanctions List and Local Lists without limiting such measure to funds that may only be used to perpetrate a certain act, conspiracy, threat or agreement related to terrorism and its financing or WMD proliferation and its financing. The freezing measure shall include the following:

    a. Funds owned or controlled, wholly or jointly, directly or indirectly, by the Listed Person or funds owned or controlled, wholly or jointly, directly or indirectly, by a person or organization acting on behalf or at the direction of the Listed Person;

    b. Funds derived or generated from funds under sub-paragraph (a) of the present Article.

2. Any person must notify the Office of any freezing measures taken pursuant to Paragraph (1), within five business day of the date of the freezing.

3. No person shall make funds available or provide financial or other related services, whether in whole or in part, directly or indirectly, to any of the persons or entities mentioned in paragraph (1) of the present Article, except upon authorization from the Office in line with the provisions of the present Decision, and after coordination with the Council or the UN Security Council or the relevant Sanctions Committee, and in line with Cabinet decisions regarding the issuance of Local Lists, or relevant UNSCRs, as the case may be.

4. In all cases, the rights of bona fide third parties shall be taken into account when implementing any freezing measure.

Article 16

1. The implementation of freezing measures pursuant to UNSCRs 1718 (2006) and 2231 (2015) shall not prevent adding to the frozen account any interest, profits or other payments due under contracts, agreements or obligations that arose prior to the date on which the account was subject to provisions of the said resolutions,

provided such additions are immediately frozen and reported to the Office.

2. In all cases, procedures set forth in UNSCRs 1452 (2002), 2231 (2015), 1718 (2006) and 2270 (2016) and any successor resolutions must be observed.

Article 17

The implementation of a freezing order pursuant to UNSCR 1737 (2006), continued pursuant to UNSCR 2231 (2015) or taken pursuant to UNSCR 2231 (2015), shall not prevent a Listed Person or organization from making a payment due under a contract that was concluded prior to their listing, subject to the following conditions:

1. The Office has determined that the contract is not related to any prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investments, brokerage or services referred to in UNSCR 2231 (2015) or any future successor resolution.

2. The Office has determined that the payment is not received, directly or indirectly, by any person or organization listed pursuant to Paragraph (6) of Appendix B of UNSCR 2231 (2015).

3. The Office has submitted a prior notification to the UN Security Council, including its request to make or receive such payments or to authorize, where appropriate, the unfreezing of funds for this purpose, within ten business days before the issuance of such authorization.

Article 18 - Lifting the Freezing of Funds & Other Measures Taken in Cases of False Positives on the Sanctions List

The mechanism for lifting freezing and any other measures taken against a person or organization bearing a name similar to that of a listed person, shall be as follows:

1. The affected person shall submit a written request to the Office in person or through a legal representative, to lift freezing or any other measures taken against him, along with all documents supporting a false positive.

2. The Office shall examine the request, and for the purposes of deciding on the request, may ask for any clarifications or additional documents, it deems suitable from the applicant, the UN Security Council, the relevant Sanctions Committee or any other party.

3. The Office shall issue its decision to reject or approve the request to lift the freezing measures within thirty days from date of receipt of the request and shall notify the applicant accordingly.

4. The Office shall communicate the decision to approve the request, to the entity where the funds are frozen, Law Enforcement Authorities and concerned agencies. The addressed organization shall immediately execute the decision to lift freezing and other measures taken against the applicant due to a false positive.

5. In case the request to lift freezing and Other Measures is rejected, or remained without a response for thirty days from date of its submission, the applicant may file a grievance before the Competent Court within sixty days from the date on which he/she was notified of the rejection of the request, or from the expiry of the response period.

6. The court's decision regarding the grievance shall not be subject to appeal. If a grievance is rejected, a new grievance may only be submitted after six months from the date of rejection of the previous grievance, unless a

serious reason that is accepted by the president of the Court arises before the expiry of such period.

7. An appeal against a decision regarding freezing or Other Measures shall not be accepted before a grievance against such is filed and rejected, or the period for responding to such grievance has elapsed, as set out in the present Article.

Article 19 - Permission to Use Funds Frozen as Per the Sanctions List

1. The Office may approve a person's request to access funds frozen as per the Sanctions List, in the following cases:

    a. To cover necessary or basic expenses, such as the amounts payable for foodstuff, rent, mortgage, medicine, medical treatment, taxes, insurance premiums, educational or judicial fees, or public utility fees.

    b. To pay professional fees and costs relating to rendered legal services within reasonable limits; or services relating to the safekeeping or management of frozen Funds.

    c. To cover extraordinary expenses other than those mentioned in sub-paragraphs (a and b) of this paragraph.

    d. In the case of sanctions imposed pursuant to UNSCRs 1718 (2006) and 1737 (2006), and continued as per UNSCR 2231 (2015), and in addition to the measures mentioned above, if access was requested to use frozen funds which are subject to mortgage, or a judicial, administrative or arbitral lien or ruling, and if the funds will be used, exclusively, to satisfy the expenses of that lien or judgment, and provided that the mortgage or the ruling entered into effect at a time prior to the date of the listing in accordance with the referenced resolutions, and that the funds are not used for the benefit of any Listed Peron, and after the Office notifies the UN Security Council or the relevant Sanctions Committee, as the case may be.

2. Requests for the purpose of deciding on any of the items under paragraph (1) of this article, shall be submitted directly to the Office, by the Listed Person or their legal representative, along with all supporting documents.

3. The Office shall examine the requests referred to in paragraph (2) of this article, their reasons, and the requested amounts, and may reduce or reject such amounts, based on justifiable grounds.

4. In the event that the submitted request is related to the expenses mentioned in sub-paragraphs (a, b, and d) of paragraph (1) of the present Article, the Office must notify the UN Security Council or the Sanctions Committee of its intention to approve the submitted request following consideration thereof in accordance with the provisions of paragraph (3) of this article, and in case the sanctions committee does not object, or issue a decision of rejection within five business days from the date of its notification, the funds that the Office agreed to unfreeze shall be unfrozen and the entity holding the frozen funds shall be immediately notified in writing to such effect and asked to implement the decision immediately. Such entity shall notify the Office of the actions taken in this regard.

5. In case the submitted request relates to the expenses mentioned in sub-paragraph (c) of Paragraph (1) of the present Article, the Office shall notify the Sanctions Committee of its intention to approve the submitted request following consideration thereof in accordance with the provisions of Paragraph (3) of this article, and obtain the Sanctions Committee's written approval.

6. For the purposes of paragraphs (4) and (5) of this article, the Office must notify the person requesting the use of funds frozen as per the Sanctions List, or their legal representative, in writing, of its approval of the request or its

justified rejection of such, as soon as possible.

7. The Office may revoke its decision to approve the request to use funds frozen under the Sanctions List, any time there are reasonable grounds for suspicion that the funds are used for financing terrorism or financing WMD proliferation.

8. In case the request to use funds frozen under the Sanctions List is rejected, or remains without response for thirty days from date of its submission, the applicant may file a grievance before the Competent Court within sixty days from the date on which he/she was notified of the rejection of the request, or from the expiry of the response period.

9. The Court's decision on the grievance may not be appealed, and if the court ruled to reject the grievance, a new grievance may only be filed after six months from the date of rejection of the grievance, unless a serious reason that is accepted by the president of the Court arises before the expiry of such period.

10. An appeal against a decision to refuse the use of frozen funds shall not be accepted before a grievance against such is filed and rejected, or the period for responding to such grievance has elapsed.

11. In all cases, the procedures set forth in UNSCRs 1452 (2002), 1718 (2006) and 2231 (2015) and any successor resolutions, shall be observed.

Article 20

The Office may set any controls it deems appropriate for the exemptions and payments stipulated in this Decision, to prevent the use of the funds for financing terrorism or WMD proliferation.

Article 21 - Obligations of Financial Institutions and DNFBPs

For the purposes of implementing the present Decision, financial institutions and DNFBPs shall abide by the following:

1. Register on the Office's website in order to receive notifications related to new listing, re-listing, updating, or de-listing decisions issued by the UN Security Council, the Sanctions Committee or the Cabinet.

2. Regularly screen their databases and transactions against names on lists issued by the UN Security Council, the Sanctions Committee or the Local Lists, and also immediately when notified of any changes to any of such lists, provided that such screening includes the following:

    a. Searching their customer databases.

    b. Search for the names of parties to any transactions.

    c. Search for the names of potential customers.

    d. Search for the names of beneficial owners.

    e. Search for names of persons and organizations with which they have a direct or indirect relationship.

    f. Continuously search their customer database before conducting any transaction, or entering into a serious business relationship with any person, to ensure that their name is not listed on the Sanctions List or Local Lists.

3. Implement freezing measures, without delay, and without prior notice to the Listed Person, immediately when a match is found through the screening process referred to in paragraph (2) of this article.

4. Implement decisions to lift freezing measures without delay, pursuant to Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists.

5. Immediately notify the Supervisory Authority in the following cases:

    a. Identification of funds and actions that have been taken as per requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists, including attempted transactions.

    b. Detection of any match with listed persons or entities, details of the match data and actions that have been taken as per the requirements of Relevant UNSCRs and Local Lists, including attempted transactions.

    c. If it was found that one of its previous customers or any occasional customer it dealt with, is listed on the Sanctions List or Local Lists.

    d. If it suspects that one of its current or former customers, or a person it has a business relationship with is listed or has a direct or indirect relationship with the Listed Person.

    e. No action has been taken due to a false positive, and the inability to dismiss such false positive through available or accessible information.

    f. Information relating to funds that have been unfrozen, including their status, nature, value and measures that were taken in respect thereof, and any other information relevant to such decisions.

6. Establish and effectively implement internal controls and procedures to ensure compliance with the obligations arising from this Decision.

7. Establish and implement policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third party that freezing or any Other Measures shall be implemented in accordance with the provisions of this Decision.

8. Cooperate with the Office and the Supervisory Authority in verifying the accuracy of submitted information.

Article 22 - Obligations of Supervisory Authorities

Supervisory Authorities shall abide by the following:

1. Receive all information from FIs and DNFBPs regarding frozen funds, or any measures taken in compliance with prohibition requirements pursuant to the present Decision, including attempted transactions and send such information to the Office within five working days from the date of its receipt.

2. Supervise, monitor and follow-up to ensure compliance with the provisions of this Decision, through onsite and offsite inspection, and imposing appropriate administrative sanctions in case of violation or failure to implement such provisions.

3. Establish a list of cases detected, as per the provisions of this Decision, by FIs and DNFBPs, where the customer or beneficial owner was a Listed Person or organization.

4. Identify any funds related to a Listed Person that have been detected and frozen by FIs and DNFBPs, and whether or not relevant reports were submitted to the Office in line with the provisions of the present Decision.

5. Submit reports to the Office at least semiannually on results of supervision, monitoring and follow-up on the implementation of FIs and DNFBPs of their obligations under the present Decision.

Article 23 - General Provisions

1. Any person who, due to the nature of their work, has access to, or becomes aware of, any information provided or exchanged pursuant to the provisions of the present Decision, whether directly or indirectly, shall not disclose this information in any form, unless for the purposes of implementing the present Decision.

2. A person who, in good faith, freezes Funds, denies disposal thereof, refuses to provide financial services relating thereto, or declines to perform any other obligation in compliance with the provisions of the present Decision, shall be exempt from any damages or claims resulting from such actions.

3. Violating the provisions of the present Decision shall result in the implementation of penal and administrative sanctions stipulated in Federal Decree Law No. (20) of 2018.

Article 24 - Administrative Measures

1. Both the Council and the Office may, within the limits of their respective mandates, issue procedures and instructions concerning the implementation of the present Decision.

2. Procedures, criteria and templates adopted by the UN Security Council and its Committees are considered the main reference for implementing the provisions of the present Decision and any other related procedures.

3. Subject to relevant UNSCRs, the Council or the Office, as the case may be, may ask the Ministry of Justice to appoint whoever it deems appropriate to manage frozen Funds, if necessary.

Article 25 - Repeal of Conflicting Provisions

Cabinet Decision No. (20) of 2019 referred to above is hereby repealed as any provisions conflicting with the provisions of the present Decision are repealed.

Article 26 - Publication and Entering into Effect

The present Decision shall be published in the Official Gazette, and shall come into effect on the day following the date of its publication.

Registered Hawala Providers Regulation

C 24/2019 Effective from 14/6/2019 **Status:** In-Force

The Chairman of the Board of Directors of the Central Bank,

Having perused provisions Federal Law No. (7) of 2014 regarding Combating Terrorism Crimes;

Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities;

Decretal Federal Law No. (20) of 2018 on Anti-Money Laundering and Countering the Financing of Terrorism and Illegal Organizations and its Executive Regulations;

The Central Bank Board of Directors' Resolution No 20/2/2019 regarding approving the Registered Hawala Providers Regulation; and

National Anti-Money Laundering Committee's decision in its meeting of 14 June 2012.

Has decided the following:

Objective:

The objective of this Regulation is to provide a regulatory framework for Hawala Providers in the UAE in order to operate within the UAE financial sector in a robust and prudent manner. As such, the framework set out in this Regulation is aimed at protecting the customers of Registered Hawala Providers and the reputation of the financial system of the UAE.

This Regulation is issued by the Central Bank pursuant to the powers vested in the Central Bank Law.

Where this Regulation includes a requirement to provide information or to take certain measures, or to address certain items listed at a minimum, the Central Bank may impose requirements, which are additional to the list provided in the relevant article.

Application:

This Regulation applies to any person carrying out Hawala activity in the UAE.

Article 1: Definitions

The following terms and phrases shall have the definitions assigned to them for the purpose of this Regulation:

Central Bank: The Central Bank of the United Arab Emirates;

Central Bank Law: Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities;

Hawala Activity: The arrangements for transfer and receipt of funds or equivalent value and settlement through trade and cash;

Hawala Provider Certificate: The certificate issued by the Central Bank for carrying on Hawala activity in the U.A.E;

Juridical Person: A juridical person in accordance with Article 92 of Federal Law No. 5 of 1985 Concerning the Issuance of the Civil Transactions Law as amended. For the purpose of this Regulation, this definition only refers to Juridical Persons in the UAE;

Registered Hawala Provider: Any natural person holding a valid residency visa or Juridical Person, who is registered in the Central Bank's Hawala Providers Register in accordance with the provisions of this Regulation, including its agents or a network of agents;

Registered Hawala Provider's Agent: Any natural or Juridical Person carrying out activity on behalf of a Registered Hawala Provider, whether by contract with or under the direction of the Registered Hawala Provider; and

Regulations: Any resolution, regulation, circular, rule, instruction, Standard or notice issued by the Central Bank.

The terms mentioned in the Central Bank Law shall bear the same meanings ascribed thereto in the said Law when used in this Regulation, unless a definition otherwise is stated herein.

Article 2: Registration and Certificate Requirements

2-1 A resident natural person or a juridical person may not carry on Hawala activity in the UAE unless he holds a Hawala Provider Certificate issued by the Central Bank in accordance with the provisions of this Regulation.

2-2 Any natural person or juridical person may apply for registration and obtain a Hawala Provider Certificate. The said application shall be made on the Central Bank's prescribed form for this purpose and be accompanied by the following documents:

a. A statement showing the nature and scope of the Hawala activity carried out by the applicant, in addition to any plans he may have for future business expansion, and details of the applicant's arrangements for management of his business;

b. The applicant's name, address, age and occupation, along with a true copy of his UAE ID card and/or passport, for natural persons, and a true copy of the commercial license for juridical persons;

c. An undertaking by the applicant:

i. to guarantee all transfers for its customers;

ii. that the Central Bank bears no responsibility whatsoever towards customer funds regardless of their value;

iii. to maintain an account with a bank operating in the UAE to be used for settlement and provide the Central Bank with details of such account;

iv. to abide, alike with its agents, by all UAE established laws, including civil laws, commercial companies' law, federal laws on AML/CFT, and Central Bank Regulations;

v. to notify the competent authorities of the violation of said laws and Regulation;

vi. to make his records and documents available for examination by the Central Bank's staff or any third party authorized to act on its behalf;

vii. to provide any information or documents the Central Bank may require for the purposes of deciding on the application for registration;

viii. to amend the license provided by the relevant economic department to reflect Hawala activity; and

ix. to install all security systems (alarm system/CCTV), in accordance with the relevant authority requirements and use authorized cash transit Service providers for bulk currency transfers.

3-2 A Hawala Provider Certificate shall only be granted if the following conditions are met:

a. The applicant undertakes to provide the Central Bank, electronically via the Central Bank's Remittance Reporting System and/or other applicable Central Bank system, with the data and information on remitters and beneficiaries required as per the forms prepared by the Central Bank for this purpose;

b. The applicant is not of UAE nationality and is legally competent and officially residing in the UAE;

c. The applicant is of good conduct and behavior and has not been convicted of any crime of honor or honesty and has not failed to honor his liabilities towards financial institutions or any other creditors. Furthermore, the applicant should not have been declared bankrupt nor reached a settlement agreement with his creditors or have his property confiscated or put under court receivership;

d. The applicant has a reasonable level of education, administrative, and professional experience.

Article 3: Notification of Approval/Rejection and Certificate Conditions

3-1 The Central Bank may agree or decline to issue a Hawala Provider Certificate.

3-2 In case of approval or rejection of the application for a Hawala Provider Certificate, the Central Bank shall notify the applicant in writing indicating reasons in case of rejection.

3-3 The Central Bank shall issue a Hawala Provider Certificate valid for one year, renewable for similar periods. The Central Bank may include in the Hawala Provider Certificate whatever terms and conditions it deems appropriate.

Article 4: On-Going Obligations of Registered Hawala Providers

4-1 A Registered Hawala Provider should strictly abide by the following:

a. Its commercial name should not include any financial activity term, such as bank, exchange house or any other licensed activity by the Central Bank (for juridical persons);

b. Manage his business personally and never assign such task to another person;

c. Not to change his address, place of residence/business, sponsor or commercial activity without obtaining the Central Bank's approval;

d. Carry out his activity in suitable premises that enables the Central Bank's staff to visit and examine his records;

e. Upload electronically to the Central Bank the details of all transfers, remitters and beneficiaries in the Central Bank's prescribed systems on a daily basis;

f. Receive all applications for money value transfers as per official vouchers for each transaction. Such vouchers should be appropriately stored;

g. Verify identities of remitters and beneficiaries using Emirates ID or passports;

h. Deposit funds received from its customers in the account designated for settlement;

i. Submit to the Central Bank statements of his settlement account on a quarterly basis along with other required forms;

j. Provide the Central Bank with any data, information or statistics it may require at any time and for any specific period. Such data and information shall be regarded as confidential and shall be treated accordingly. A Registered Hawala Provider may not disclose such information except in accordance with the law;

k. A Registered Hawala Provider must exercise due diligence when approving an agent and provide the Central Bank a current list of its agents and the countries in which they operate;

l. Submit to the Central Bank an application for renewal of the Hawala Provider Certificate within a period not less than two months from the date of expiry of the original certificate or any renewals thereof; and

m. Abide, alike with its customers and agents, by all UAE laws, including civil laws, Commercial Companies' Law, federal laws on AML/CFT, and Central Bank Regulations particularly with regard to notifying the competent authorities of any violation thereof.

Article 5: Specific Obligations with Regard to ML/FT Risks

5-1 In addition, a Hawala Provider registered in the Central Bank's Hawala Providers Register must strictly comply with Decretal Federal Law No. (20) of 2018 on Anti-money Laundering and Countering the Financing of Terrorism and Illegal Organizations and its executive regulations, and any Regulations and directions issued by the Central Bank in this regard.

5-2 Hawala Providers may be guided by the Financial Action Task Force (FATF) Standards on anti-money laundering and countering the financing of terrorism and proliferation and to abide by guidance issued by the Central Bank in this regard.

Article 6: Supervision and Examination

6-1 The Central Bank shall have the right to examine the business of the Hawala Providers and their agents and customers whenever it deems appropriate to ensure proper implementation of the provisions of this Regulation.

Article 7: Enforcement and Sanctions

7-1 Violation of any provision of this Regulation may be subject to supervisory action as deemed appropriate by the Central Bank. In addition, without prejudice to other sanctions stated in any other laws in the UAE, the Central Bank may impose administrative and financial sanctions and penalties in accordance with the Central Bank Law and the Regulations issued in implementation thereof.

Article 8: Interpretation of the Provisions of the Regulation

8-1 The Regulatory Development Division of the Central Bank shall be the reference for interpretation of the provisions of this Regulation.

Article 9: Cancellation of Previous Resolutions

9-1 The Central Bank Board of Directors' Resolution No 109/5/2002 regarding the preparation of a simple regulation for licensing and monitoring of Hawala intermediaries is cancelled.

9-2 This Regulation replaces "Hawala Intermediaries Regulation" issued on 2 July 2012.

Article 10: Publication and Application

10-1 This Regulation shall be published in the Official Gazette in both Arabic and English and shall come into effect one month from the date of publication

Best Practices for Licensed Financial Institutions on Implementing Role-Based AML/CFT/CPF Training

Effective from 7/11/2025 **Status:** In-Force

1. Introduction

A comprehensive anti-money laundering ("AML") and combating the financing of terrorism ("CFT") and countering proliferation financing ("CPF") training program is critical to the overall effectiveness of a licensed financial institution's ("LFI's") compliance program. AML/CFT/CPF training helps employees understand their responsibility to combat money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") through identifying

ML/TF and PF red flags and managing ML/TF and PF risks in the context of their job functions. As such, all employees—spanning from the LFI's Board of Directors, owners/partners/shareholders, senior management, new employees, to external staff—should receive AML/CFT/CPF training through a combination of the following types of AML/CFT/CPF training:

- New hire training (including existing employees who take on new roles or positions);
- Annual enterprise-wide AML/CFT/CPF training;
- Global mandatory AML/CFT/CPF training (for LFIs that fall under a Group);
- Localized training, targeting specific local ML/TF and PF risks;
- Board of Directors, owners/partners/shareholders[1], and senior management training[2]; and
- Role-based training (including on-the-job training, especially if the risks are specific to a certain role);

LFIs should adopt a risk-based approach to their AML/CFT/CPF training programs, ensuring that the content, frequency, and intensity of training is commensurate with the ML/TF/PF risks faced by different roles and functions within the organization. Understanding that there are different types of training that comprise an LFI's AML/CFT/CPF training program, this Best Practices document specifically focuses on best practices associated with role-based AML/CFT/CPF training. The purpose of role-based AML/CFT/CPF training is to ensure that employees across an LFI's organization receive training that is tailored to their responsibilities and specific ML/TF and PF risk exposure. Such role-based training provides employees with the relevant expertise and judgement required to meet the specific needs of their different AML/CFT/CPF-related responsibilities.

---

[1] AML/CFT/CPF training should be required for owners, partners, and shareholders carrying out an active role in the management of the LFI. Training is not mandatory for passive shareholders.
[2] For the purposes of this Best Practices document, Board of Directors and senior management training is discussed in the context of role-based training.

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Best Practices document is to **assist** the understanding and effective performance and compliance by the United Arab Emirates Central Bank's ("CBUAE") LFIs and registered hawala providers ("RHPs"), of their statutory obligations under the legal and regulatory framework in force in the UAE specific to role-based AML/CFT/CPF training. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[3] As such, while this Best Practices document neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this document and the legal or regulatory frameworks currently in force, the latter will prevail. This Best Practices document may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the CBUAE. It provides additional guidance to help LFIs effectively meet their AML/CFT/CPF training obligations as stipulated in the legal and regulatory frameworks.

Furthermore, this Best Practices document takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), as LFIs should ensure that their role-based training programs not only meet local regulatory requirements but also reflect global best practices to enhance their effectiveness. These standards and guidance are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations. The CBUAE may issue supplementary guidance materials, such as outreach sessions and thematic reviews, to support LFIs in implementing the role-based training requirements. LFIs should stay informed of any such updates to ensure their training programs remain compliant and effective.

This Best Practices document comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate it has taken concrete efforts to come into compliance with its requirements within one month from its coming into effect (e.g., development of policies, procedures, and training materials).

---

[3] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers;
- Insurance companies, agencies, and brokers; and
- Other covered financial institutions not specified above, or any other entities that are licensed or registered by the CBUAE and are engaged in financial activities that fall under AML/CFT/CPF regulations.

For LFI's with operations outside the UAE, this guidance applies to their UAE-based activities and should inform group-wide standards, while adhering to applicable regulations in the local jurisdiction.

1.3. Legal Basis

This Best Practices document builds upon the provisions of the following laws and regulations:

- Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Federal Decree Law No. (26) of 2021 ("AML-CFT Law");
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision") and its amendments;
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments; and
- Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58").

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CFT	Combating the financing of terrorism
CPF	Countering proliferation financing
FATF	Financial Action Task Force
FCC	Financial crimes compliance
LFI	Licensed financial institution
ML	Money laundering
PF	Proliferation financing
RBA	Risk-based approach
RHP	Registered Hawala Provider
TF	Terrorist financing
UN	United Nations

2. Scope of the Role-Based AML/CFT/CPF Training

Role-based AML/CFT/CPF training is important as it helps ensure that an employee's technical knowledge (i.e., understanding specific ML/TF/PF risks associated with different roles, familiarity with regulatory requirements, and the ability to apply internal policies and procedures effectively and understanding of ML/TF and PF risks, global standards, regulatory requirements, and internal policies) and the LFI's AML/CFT/CPF compliance program are accurate and up to date. It also enables an employee to understand their responsibility to identify ML/TF and PF risks and red flags—both generally and specific to the LFI—in the context of their role within an LFI. As such, unlike other training that provides a general introduction on AML/CFT/CPF requirements and ML/TF/PF red flags, LFI's role-based training should be tailored to the specific responsibilities of its employees who are exposed to ML/TF and PF risks and are responsible for performing AML/CFT/CPF-related functions within the LFI. Role-based training can also take the form of ad-hoc training, tailored to an LFI's specific team or department to enhance awareness on specific topics.

This Best Practices document discusses the components of role-based AML/CFT/CPF training and how an employee's responsibilities should be understood in the context of:

- UAE regulatory requirements and supervisory guidance;
- Financial crimes compliance ("FCC") global standards;
- Internal policies, procedures, and processes; and
- LFI's products, services, customers, and geographic locations.

2.1. UAE Regulatory Requirements, Supervisory Guidance, and Global Standards

Educating LFI staff on local regulatory requirements, relevant supervisory guidance and FCC global standards, is a key component of an effective AML/CFT/CPF training program. Accordingly, training content should be appropriately tailored to an LFI's specific profile (including but not limited to; risk exposure, product offering and size) and cover requirements from the jurisdictions where the LFI operates, including the LFI's branches and majority-owned subsidiaries. As such, an LFI's role-based trainings should focus on educating LFI staff, Board members, owners/partners/shareholders[4], and senior management on UAE AML/CFT/CPF laws, regulations, and supervisory

guidance as well as ML/TF and PF trends and typologies common to the UAE. LFI's may also consider training material and guidance documents published by international bodies like FATF.

- **UAE AML/CFT/CPF Framework**: The UAE has several laws and regulations that address AML/CFT/CPF, including the AML-CFT Law and AML-CFT **Decision. The training provided must ensure that the LFI's employees are aware, and have an appropriate understanding, of** their legal and regulatory responsibilities and obligations and the consequences of non-compliance. For example, training should include specific examples such as UAE Federal Decree Law No. 20 of 2018 on Anti-Money Laundering, the CBUAE's thematic reviews, and sector-specific risk assessments to illustrate regulatory expectations and compliance requirements. Furthermore, the LFI's AML/CFT/CPF trainings should also cover CBUAE-issued guidance or feedback[5] on ML/TF and PF risks, such as thematic reviews. Finally, trainings should be developed in the context of the UAE's National ML/TF and PF Risk Assessments and the CBUAE's Sectoral Risk ML/TF and PF Assessments.

  LFIs should ensure key compliance staff attend the various training and outreach sessions provided by the CBUAE and Executive Office for Control and Non-Proliferation ("EOCN") on these topics. The schedule of training and outreach sessions can be found at the AML/CFT Supervision website of the CBUAE.[6]

- **FCC Global Standards:** Global standards for FCC encompass a collection of standards that originate from intergovernmental organizations and industry groups. These global standardssetting bodies issue recommendations and guidance for jurisdictions and LFIs to adopt as part of implementing an effective AML/CFT/CPF regime. LFI's may consider FCC global standards and general ML/TF and PF trends, typologies, and best practices identified by global standards-setting bodies which may be relevant to the LFI. Local compliance training programs should also consider best practices and recommendations set by international standards-settings bodies, when developing training programs and content, as they complement local UAE laws and regulations. FCC global standards-setting bodies include:

  - The **United Nations Security Council (UNSC)**, is one of the six principal bodies of the United Nations and the only authority issuing resolutions that are binding on member states as mentioned in Article 16 and 28 of Decree Federal Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisation;

  - The **Financial Action Task Force**, the leading AML/CFT standards-setter at the international level, established by the Group of Seven ("G7") to examine and combat ML;

  - The **Basel Committee on Banking Supervision** ("BCBS"), a committee of Central Banks and other banking regulatory authorities from 28 jurisdictions and has 45 members;

  - The **Wolfsberg Group**, an association of 13 of the world's largest banks; and

  - The **Egmont Group of Financial Intelligence Units**, a body of financial intelligence units ("FIUs") from around the world.

---

[4] AML/CFT/CPF training should be required for owners, partners, and shareholders carrying out an active role in the management of the LFI. Training is not mandatory for passive shareholders.
[5] Available at: https://www.centralbank.ae/en/cbuae-amlcft
[6] Available at: https://www.centralbank.ae/en/cbuae-amlcft

2.2. Internal Policies, Procedures, and Processes

LFIs should provide ongoing training to employees on the LFI's AML/CFT/CPF policies and procedures. Trainings should address how employees are expected to comply with the LFI's policies and procedures, consequences for

not adhering to these policies and procedures, and where employees can locate policies and procedures and learn more about the LFI's AML/CFT/CPF compliance program.

In addition to covering the policies and procedures relevant to an employee's day-to-day job function, the training material should also cover the specific systems and controls being utilized by the LFI, including the use of internal and external tools, relevant to the LFI's AML/CFT/CPF compliance program and the specific work carried out by its employees. An employee should understand how to perform their roles and responsibilities through the use of the LFI's systems and controls, such as for onboarding customers; updating a customer's risk rating and customer due diligence/know your customer ("CDD/KYC") file; performing sanctions screening; transaction monitoring; and investigating and reporting suspicious activity and transactions, including attempted transactions.

To be effective, training should include real-life and role-specific scenarios employees may encounter while performing their day-to-day job function and include interactive content wherever possible. In response to any updates to the LFI's AML/CFT/CPF compliance program, the LFI should also offer refresher training so that the LFI helps promote a culture of compliance and that employees are knowledgeable of any changes to the LFI's ML/TF and PF risks, policies, and procedures, including gaps identified as part of regulatory examinations, quality assurance review or independent audits.

LFIs should have a structured process for distributing and tracking updates to AML/CFT/CPF policies and procedures. Refresher training should be conducted regularly and whenever there are updates to the AML/CFT/CPF compliance program. This training should address any changes to policies, procedures, and systems, as well as any identified gaps from regulatory examinations or audits. In addition to scheduled trainings, an LFI should regularly communicate any changes or updates to the LFI's AML/CFT/CPF policies, procedures, systems, and controls, to employees via email, notices, or bulletins and where applicable following-up with employees to ensure that the information has been read and understood. Following any updates to policies and procedures, LFIs should implement mechanisms to verify employee understanding.

2.3. LFI's Products, Services, Customers, and Geographic Locations

LFIs are required to identify, assess, and manage ML/TF and PF risks associated with their products, services, customers, and geographic locations as part of implementing a risk-based approach ("RBA"). Under the RBA, institutions that face higher ML/TF and PF risks are expected to develop enhanced measures to mitigate such risks by expanding the range, degree, frequency, and intensity of their mitigating controls. Conversely, institutions that face lower ML/TF and PF risks may choose to implement simplified measures, provided that these measures are consistent with minimum legal and regulatory obligations.

Employees should understand how the LFI's RBA is applied in the context of their roles, how they contribute to assessing and managing the risks that may be present in the LFI's business activities, and that employees whose job functions expose them to higher ML/TF/PF risks receive training commensurate with the level of risk typically involved. Role-based training should incorporate the principles of the RBA by addressing how employees' specific roles contribute to managing risks associated with products, services, customers, and geographic locations. Role-based training should highlight how to apply enhanced or simplified measures based on the assessed risk level. An LFI's employees should be trained on risks associated with:

- The size, complexity, and risk profile of the LFI's sector and business lines;
- Characteristics of the LFI's customer base, including any concentration of customers in highrisk segments, industries, and professions;
- Vulnerabilities of products and services (specifically, generally higher risk services such as private banking or cross-border wire transfers), as informed by the LFI's enterprise-wide AML/CFT/CPF risk assessment and

CBUAE's ML/TF Sectoral Risk Assessment; and

- Countries the LFI's customers are exposed to and the LFI's own locations around the world, including the LFI's nexus to high-risk geographies (For example, countries assessed as highrisk jurisdictions for ML/TF and PF by the FATF, financial secrecy havens, etc.).

Employees handling high-risk customers and jurisdictions should receive specialized training focused on enhanced due diligence and risk management strategies. This would ensure that training is tailored to the specific challenges posed by high-risk scenarios, thereby enhancing the institution's overall risk management framework. LFIs should ensure that training is developed addressing emerging risks and new typologies that are specific to the LFIs business model, customer types, products, services, and geographies. The content should be updated based on internal and external data and sources.

3. Role-Based Training

Role-based training should be determined based on factors identified as part of an annual training needs assessment, focusing on areas vulnerable to ML/TF and PF. The training needs assessment identifies areas within an LFI that are vulnerable to ML/TF and PF and require enhanced training. A training needs assessment should be conducted annually and should include a review of the LFI's risk assessment, regulatory findings, audit results, and feedback from senior management. This assessment will help identify areas that require enhanced role-based training and ensure that training programs are updated accordingly. The factors used to identify the enhanced training needs are, for example, an LFI's enterprise-wide AML/CFT/CPF risk assessment, regulatory examination or independent audit findings, and feedback from key stakeholders, such as an LFI's senior management. First line of defense employees and business units should also be able to engage an LFI's Compliance team to request additional AML/CFT/CPF trainings if required. Training programs can also gather feedback from current and past participants to gauge the effectiveness of the training and if participants felt training helped prepare them to carry out their job function with respects towards the AML/CFT/CPF controls. Further, the CBUAE has a mailbox where LFIs can request and submit information feedback regarding the LFI's training needs. Additionally, the LFI should utilize the CBUAE's mailbox for submitting feedback and requesting guidance on training needs. This helps ensure that training programs are responsive to emerging risks and regulatory expectations. Requests and feedback can be submitted to amlcfttraining@cbuae.gov.ae. CBUAE will review and monitor requests and feedback submissions from LFIs in order to improve and provide tailored outreach and training sessions.

Generally, employees with increased exposure to ML/TF and PF risk should receive specific role-based training, including review of real-world case studies (such as trade finance and correspondent banking functions and tellers handling cash transactions). At a minimum, however, a comprehensive training program should ensure that role-based training is provided to the following groups:

- Board of Directors, owners/partners/shareholders, and senior management;
- First line of defense employees with heightened exposure to ML/TF and PF risk (For example, bank tellers, relationship managers, executives);
- Second line of defense employees (i.e., employees in an LFI's compliance department);
- Third line of defense employees (i.e., independent testing function); and
- Staff responsible for testing, tuning and validation of the LFIs financial crime compliance framework including systems and model.

3.1. Board of Directors/Owners and Senior Management

An LFI's Board of Directors, including an LFI's owners/partners/shareholders, acts as an independent body that exercises oversight of an LFI, including its AML/CFT/CPF compliance program. Meanwhile senior management functions under the mandate of the Board of Directors and ensures that an LFI's AML/CFT/CPF compliance program has policies, processes, systems, and controls needed to effectively manage the LFI's ML/TF and PF risks. Board of Directors, owners/partners/shareholders, and senior management require ongoing training to enhance their knowledge and understanding the LFI's ML/TF and PF risk profile and applicable regulatory requirements. It is critical that an LFI's leaders are familiar with AML/CFT/CPF regulatory expectations in order to effectively direct the LFI's AML/CFT/CPF strategy, make informed decisions about the LFI's risk appetite, and oversee an LFI's AML/CFT/CPF compliance program. Additionally, training for the Board of Directors, owners/partners/shareholders, and senior management should emphasize how they foster a culture of compliance within the LFI.

To this end, an LFI's Board of Directors, owners/partners/shareholders, and senior management should receive periodic training that, at a minimum, covers:

- Their responsibility for overseeing the AML/CFT/CPF compliance program, including that the LFI has appropriate policies, processes, systems, and controls to mitigate ML/TF and PF risks;
- Findings from the LFI's enterprise-wide AML/CFT/CPF risk assessment and the impact of the LFI's business operations on its ML/TF and PF risk profile;
- Emerging ML/TF/PF trends;
- Their role in monitoring and ensuring that recommendations from internal AML/CFT/CPF audits are effectively and timeously implemented;
- Any new developments with respect to FCC global standards, any UAE AML/CFT/CPF regulatory updates, and supervisory expectations for AML/CFT/CPF compliance; and
- Their role in fostering a culture of compliance, specifically of communicating and reinforcing the compliance culture established by the Board of Directors or owners/partners/shareholders, and senior management's role in implementing and enforcing the Board-approved AML/CFT/CPF compliance program. Training should include specific strategies for fostering a culture of compliance, such as setting a tone at the top through visible commitment, integrating compliance into business strategies, and encouraging open communication about compliance issues among staff.

Training for the Board of Directors, owners/partners/shareholders, and senior management should be conducted on a need basis or at least annually and a record of attendance and material discussed should be kept; however, it is important that the Board of Directors, owners/partners/shareholders, and senior management receive ongoing updates and communications regarding the status of AML/CFT/CPF regulatory issues and ML/TF and PF risks posed to the LFI. Such updates and communications could be included as part of periodic Board Meeting packs, which should include Management Information on Key Risk Indicators reporting on the strengths of the LFI's control framework and other relevant metrics.

3.2. First Line of Defense

First line of defense employees (for example, customer-facing staff, tellers, relationship managers, and business executives) play a critical role in the management of customer risk and the timely escalation of potentially suspicious activity or transactions. One of the core duties of the first line of defense is the implementation of due diligence processes to identify and verify customers and assess their risk profiles, as first line of defense employees are on the front line for detecting and preventing ML/TF and PF. First line of defense training should be tailored to address the varying risk levels within different functions. For example, higher-risk roles such as those in private banking or trade finance should receive more intensive training on red flags and reporting requirements compared to lower-risk roles. Therefore, it is essential for first line of defense employees to be cognizant of red flags associated with their

specific function and understand their obligations to not "tip off" a customer. For example, bank tellers should understand red flags associated with a customer's efforts to avoid cash reporting requirements. Similarly, a relationship manager should understand red flags associated with false, insufficient, or misleading CDD/KYC information during the onboarding process and beyond. LFI's must provide adequate training to first line of defense employees on ML/TF and PF red flags and their responsibility to identify and report potentially suspicious activity. Training programs should incorporate real-life and role specific case studies and scenarios to illustrate ML/TF and PF risks, enhancing the practical understanding of employees and bridge the gap between theoretical knowledge and practical application, thereby improving the effectiveness of training. The LFI may consider incorporating case studies relevant to the staff day-to-day responsibilities, such as conducting customer due diligence or identifying suspicious transactions. Role-play or simulation exercises may help employees understand and react better to potential real-world situations.

Appropriately trained employees are well-placed to identify suspicious transactions and activity. Rolebased AML/CFT/CPF training is especially important for employees in higher-risk lines of business, such as private banking, lending, foreign correspondent banking, and trade finance, and for employees or agents in risk-sensitive areas, such as those that handle cash and are involved in customer transaction activities. To this end, first line of defense employees should receive periodic training which at a minimum covers:

- The definition of a suspicious activity or transaction and the nature and importance of the suspicious transaction or activity reporting requirement;
- How to implement an LFI's due diligence processes to verify the identity of customers and assess their risk profiles;
- Examples of ML/TF and PF that enable employees to identify red flags associated with customers, products, services, delivery channels, and geographies;
- Best practices in investigating and dispositioning name screening, transaction screening and transaction monitoring alerts, using case studies and practical scenarios where possible to help application of knowledge and skills learned;
- Identification of ML, TF, and PF red flags and typologies, as well as information on key financial crime compliance regulatory and industry developments both globally and locally;
- Information on the LFI's procedures to escalate suspicious activity to management and specific compliance personnel;
- Specific staff responsibilities (first/second/third line of defense) and roles of relevant individuals with responsibility for AML/CFT/CPF, including the Money Laundering Reporting Officer ("MLRO");
- Specific information, typologies, and controls tailored to employees in higher risk lines of business, e.g., analysts focusing on trade finance should receive in-depth training on Trade-Based Money Laundering;
- UAE specific AML/CFT/CPF regulatory requirements (existing and upon issuance/ update of regulations or guidance's); and
- ML/TF and PF risks posed to their business line and associated vulnerability of products and services offered by the business line, as informed by the LFI's enterprise-wide AML/CFT/CPF risk assessment.

Training programs should also include mechanisms for collecting and integrating feedback from first line employees. This feedback can provide insights into emerging risks, practical challenges, and effectiveness of current training materials, allowing for continuous improvement of the training program.

3.3. Second Line of Defense

Employees within the second line of defense (For example, MLRO/Compliance Personnel) are responsible for implementing an LFI's AML/CFT/CPF compliance program. As part of this role, second line of defense employees are expected to provide advisory support to the lines of business—ranging from queries on the LFIs policies to payment advice—and thus should be aware of AML/CFT/CPF regulatory requirements and ongoing developments. In this capacity, the second line of defense is also charged with monitoring risks facing the LFI, such as non-compliance with UAE laws and regulations, and reporting directly to senior management on the LFI's risk exposure. Notably, it is particularly important the Compliance Officer/ MLRO has sufficient knowledge and understanding of the UAE's AML/CFT/CPF statutory and regulatory requirements in addition to the ML/TF and PF risks arising from the LFI's business.

To this end, second line of defense employees should receive periodic training which covers:

- Any new developments in FCC global standards and emerging ML/TF and PF risks, trends, and typologies, ensuring that training is tailored to the employee group's jurisdiction;
- Information sharing efforts and the resulting intelligence between the LFI, its peers, and law enforcement;
- UAE AML/CFT/CPF regulatory requirements, supervisory expectations for AML/CFT/CPF compliance, and information from relevant law enforcement advisories;
- Best practices in investigating and adjudicating sanctions screening and transaction monitoring alerts; authoring strong suspicious activity and transaction reports; potential interaction with law enforcement; information sharing efforts; and identifying red flags and other issues or inconsistencies in a customer's CDD/KYC file; and
- The importance of the compliance function in implementing and maintaining an effective AML/CFT/CPF compliance program
- Emerging technologies related to financial crime compliance.

Please note, as part of receiving the abovementioned training, second line of defense employees may seek to obtain professional certifications (For example, ACAMS certifications) and participate in industry webinars or attend professional events to further deepen and expand their specific skillsets and expertise in the field of financial crimes compliance. Providing ongoing professional development and continuing education opportunities to the second line of defense, such as advanced courses and workshops in financial crime compliance, is critical for staff to stay abreast of the latest trends and best practices in the field. Second line of defense employees should also be provided with resources and access to current information on global standards, emerging trends, and best practices. This can include subscriptions to industry journals, participation in relevant webinars, and engagement with professional networks.

3.4. Third Line of Defense

The independent testing or internal audit function is responsible for evaluating the design and operational effectiveness of an LFI's AML/CFT/CPF compliance program controls, including technical compliance with AML/CFT/CPF policies and procedures. This function serves as a "third line of defense" to identify gaps and weaknesses in controls owned or overseen by an LFI's business, operations, and compliance function, and should report to an LFI's Board of Directors or owners/partners/shareholders. An LFI's independent testing or internal audit function is typically overseen by a Head of Internal Audit/Chief Internal Auditor. Depending on the size of the LFI, an LFI's Internal Audit Department may be organized by global, regional, and country-specific teams. An LFI may also have an Internal Audit Department with internal auditors or teams of internal auditors that have specific

specializations (credit, operations, IT/systems audits). The third line of defense also supports compliance functions by validating the closure of audit findings through an LFI's implementation of remedial actions and internal control enhancements.

To this end, third line of defense employees should receive training that covers:

- Improvements and current developments in internal audit standards, procedures, and techniques in response to emerging ML/TF/PF risks;
- The LFI's Internal Audit Charter, Manual, Methodology, and Plan;
- UAE AML/CFT/CPF regulatory requirements and supervisory expectations for AML/CFT/CPF compliance;
- Methods on how to test an LFI's compliance with policies and procedures related to AML/CFT/CPF; and
- Cross-functional training covering all aspects of the AML/CFT/CPF program.

As part of receiving the abovementioned training, third line of defense employees should also complete external training and obtain professional certifications and designations (For example, such as designations offered by the Institute of Internal Auditors (IIA)), as appropriate, in order to understand industry expectations and best practices for independent testing.

Third line of defense training should emphasize the need to continuously update internal audit methodologies and procedures in response to emerging ML/TF and PF risks. This includes adopting new audit techniques and revising audit plans to address identified vulnerabilities and regulatory changes.

4. Documenting the AML/CFT/CPF Training Program

4.1. Training Plan

LFIs should develop and document an annual plan for their AML/CFT/CPF training program. An LFI's training plan should cover how the LFI intends to deliver AML/CFT/CPF training to employees, including employees in departments like IT and other support functions, which provide support to AML/CPF/CFT systems and any external staff performing AML/CFT/CPF functions on the LFI's behalf. External staff includes an LFI's vendors, temporary staff, contractors, and third parties (especially those sourcing new business). The training plan should be approved by the LFI's Board of Directors, owners/partners/shareholders, or senior management annually and tracked through a designated training coordinator or platform to ensure timely completion by all required training participants. Regular updates on training completion should be reported to senior management to ensure oversight and accountability. Specifically, the training plan should contain the following information:

- Training participants (i.e., individuals required to complete the training, along with their respective departments or business functions);
- Training topics and any relevant materials:
- Methods for training delivery;
- Objectives for each training;
- Minimum training standards (For example, timing and material covered) by department and role;
- Frequency and dates for delivering training; and

- Whether and how employees will be assessed following the training.

LFIs must maintain records of training and report training attendance and completion (passing or failing) of requisite post-training assessments to the appropriate managers. LFIs should also implement mechanisms to verify employees' understanding of the training content. This may include quizzes, acknowledgment forms, or briefings designed to confirm that employees have read and comprehended the updated information.

4.2. Updates to the AML/CFT/CPF Training Program

In order to determine the training participants, topics, and training delivery methods, the annual training plan should be informed by the LFI's training needs assessment performed by staff responsible for the LFI's AML/CFT/CPF training program. The training needs assessment assesses an LFI's training needs, including the overall risk profile of the LFI and the relevant skills and experience of the LFI's employees, such as areas of increased risk exposure within the LFI or areas where an LFI's personnel have indicated the requirement for additional guidance or support. The training needs assessment also considers regulatory examination or independent audit findings concerning training-related gaps in order to identify high-risk areas of the LFI that require targeted training. LFIs should document the methodology, findings, and outcomes of their training needs assessment. Updates to the training needs assessment should be documented in a report that is reviewed and approved by the MLRO or their designee to ensure that updates are aligned with the LFI's risk profile. In addition to the training needs assessment, an LFI's MLRO or designee should be responsible for annually evaluating the adequacy of an LFI's AML/CFT/CPF training program to determine if the program meets designated training objectives and that the trainings are commensurate with the LFI's risk exposure. LFIs should implement a process to regularly review and update their training materials to reflect the latest changes in UAE AML/CFT/CPF laws, regulations, and supervisory guidance. This review should occur at least annually or more frequently if significant regulatory changes occur.

Accordingly, an LFI should regularly review its AML/CFT/CPF training program to reflect the following, which should be used as a basis for providing refresher trainings for employees to remain up to date with changes to ML/TF and PF risks, updates to policies and procedures, and the UAE's legal framework:

- Changes to the LFI's ML/TF and PF risk profile and business model (including when a new product, service or technology is introduced);
- Findings from the LFI's enterprise-wide AML/CFT/CPF risk assessment;
- Information on emerging ML/TF and PF risks, trends, and typologies;
- Regulatory developments and updates to FCC global standards and CBUAE supervisory guidance;
- Regulatory examination or independent audit findings concerning training-related gaps; and
- Changes to the LFI's internal policies, procedures, processes, systems, and controls.

In addition to an LFI regularly reviewing and updating its AML/CFT/CPF training program, certain events may also trigger an employee's training requirements, such as:

- An employee moves between jobs or responsibilities within an LFI;
- New ML/TF and PF risk indicators relevant to a particular business line emerge, including information about ML/TF and PF risks in the sector;
- An employee fails to comply with requirements and expectations specific to the LFI's AML/CFT/CPF program (such as repeatedly failing to report suspicious activity or tipping off a customer); and

- CBUAE issues guidance on ML/TF and PF risks in the sector.

An LFI may also consider instituting a dynamic, continuous feedback loop from employees and stakeholders throughout the year, which would complement the annual assessment and help ensure that training needs are proactively recognized as new risks and regulatory changes occur. This approach can provide practical insights and reinforce the training importance in shaping and implementing the AML/CFT/CPF strategy.

4.3. Methods for Training Delivery

Based on the training needs assessment, methods for providing AML/CFT/CPF training should be tailored to suit the LFI's specific training needs. An LFI's training plan should describe the training methods and include a course abstract or description that addresses what the training intends to achieve. Methods of delivery include:

- **Instructor-led training:** Instructors can be employees of the LFI or an external third-party service provider who provides training to employees either in person or virtually.

- **Self-directed learning**: Self-directed learning provides training where employees register for online courses or use other materials to guide them through the training. Self-directed learning could take place on e-learning platforms that add simulations and gamification. Such platforms can also leverage data analytics to monitor and evaluate how effective training modules are, how many times employees take the modules, and how long it takes, on average, to complete the module.

The choice of training method should be guided by the employee's responsibilities, exposure to ML/TF risks, and learning preferences. Instructor-led training may be suitable for positions with high ML/TF/PF risk exposures, while self-directed learning may be effective for lower-risk roles or refresher courses.

If the LFI chooses to use a third-party service provider for instructor-led training, the LFI should ensure that the service provider has appropriate qualifications to provide sufficiently rigorous training and that the content of this training is tailored to the LFI and audience being trained. Before engaging a third-party service provider, it is best practice to conduct appropriate due diligence to ensure that the third-party service provider has sufficient AML/CFT/CPF experience and expertise to conduct the training in accordance with the LFI's expectations. Due diligence should also investigate if the third-party provider will track attendance and conduct post-training assessment and ensure that the provider will share the information with the LFI. The Compliance function should vet and approve the training content to ensure that the third-party service provider sufficiently adapts training content to UAE regulatory requirements; the LFI's internal AML/CFT/CPF policies, procedures, processes, systems, and controls; and the LFI's AML/CFT/CPF risk assessment. The LFI should also seek to monitor the third-party service provider as part of the LFI's overall governance arrangements, which could include regular reviews of the third-party service provider's training content. Best practices include checking the provider's track record, reviewing their training content for relevance and quality, and assessing their ability to customize training for the LFI's specific needs. The Compliance function should also regularly review and evaluate the provider's performance and training effectiveness.

Formal instructor-led and self-directed training should be supplemented with on-the-job training where more experienced employees provide guidance to junior staff on best practices in implementing AML/CFT/CPF measures and controls specific to their role. LFIs are encouraged to consider using multiple delivery methods to enhance effectiveness and engagement.

4.4. Training Records, Documentation, and Assessment

LFIs should document their training programs, track and record attendance for every participant, and followup on instances of non-completion. An LFI should evaluate what method to employ for appropriately tracking and identifying employees who attend each training. As part of this tracking process, an LFI should determine a timeline by when specific trainings (for example, new hire training and role-based training) should be completed and develop

a mechanism for following-up with employees and escalating noncompliant employees who fail to complete a mandatory training within required timelines. If an employee fails to complete training within the required timeline, the LFI should implement a follow-up process that includes additional training sessions and re-assessment. Records of these follow-up actions should be maintained, including reasons for delays and corrective measures taken. An LFI should also institute consequences for non-compliance with an LFI's training requirements, which could ultimately lead to an employee's termination from the LFI. Consequences for continued non-compliance should be clearly outlined and communicated to employees as part of the training policy.

Specifically, the LFI should maintain:

- A record of the training that has been delivered (for example, the date the training took place, a list of the participants who received the training, and the topics that were covered as part of the training). Training records should be available for independent audit or regulatory examinations.

- Documentation related to employees who failed to take the required training in a timely manner and a record of any corrective actions taken.

Training effectiveness should be assessed through various methods, such as feedback surveys, post-training assessments, and performance evaluations. As part of tracking an employee's training attendance, an LFI should determine which AML/CFT/CPF trainings should include some form of assessment upon completion. These assessments should measure employees' understanding of key concepts and their ability to apply knowledge in practice. The results of these assessments should be used to determine specific training needs for individual employees or used to refine training content and delivery methods to better address identified gaps and improve overall training outcomes. Assessment opportunities help cement understanding of new concepts and ensure that participants do not receive credit for an AML/CFT/CPF training unless they have mastered the respective AML/CFT/CPF-related concepts. Should participants fail the assessment, appropriate measures, like additional training, must be implemented to ensure that employees properly understand the specific training, before re-assessment.

LFIs should retain training-related documents including records, training needs assessments, and any other relevant materials, for the duration specified by UAE recordkeeping requirements. The integration of digital tools may be considered for enhancing the efficiency of tracking and retaining training records and documentation. LFIs should demonstrate compliance with this Best Practices document by providing evidence of their role-based training programs, including training materials, attendance records, and assessment results. Regular internal and external audits should be conducted to verify adherence to the guidelines outlined in this document.

5. Annexure 1: Synopsis of the Best Practice

introduction	Purpose and Scope of the Best Practices	The purpose of this Best Practices is to assist the understanding and effective performance by CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	This Best Practices applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, virtual asset service providers, registered hawala providers; and insurance and re-insurance companies, agencies, and brokers.
	Legal Basis	▪ Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments;

		▪ Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organizations and its amendments; ▪ Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution and its amendments; ▪ Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58").
	Definitions and Acronyms	▪ Several frequently used terms and phrase are defined, and a list of acronyms used in the Best Practices is provided.
Role-Based Training	Introduction	▪ An annual training needs assessment determines how role-based training is conducted and which groups (e.g., board of directors, first line of defense) receive certain types of training. ▪ A reminder to LFIs that CBUAE welcomes requests for training guidance and feedback via an email mailbox.
	Board of Directors/Owners and Senior Management	▪ This section notes the responsibilities of the board of directors and senior management to ensure the LFI's compliance with AML/CFT/CPF regulatory requirements and to foster a culture of compliance. ▪ The section also gives examples of training that an LFI's Board of Directors, owners/partners/shareholders, and senior management should receive.
	First Line of Defense	▪ This section discusses the employees who are typically considered part of the first line of defense (e.g., bank tellers, relationship managers) and the kind of training they should receive to enable them to identify and report red flags and suspicious activity. ▪ The section also includes several examples of specific training that can be conducted for first line staff.
	Second Line of Defense	▪ This section discusses the employees who are typically considered part of the second line of defense (e.g., MLRO, compliance personnel) and the kind of training they should receive to enable them to provide advisory support to an LFIs lines of business. ▪ The section also includes several examples of specific training that can be conducted for second line staff. ▪ The section also notes the external resources and certifications that are available for external staff to enhance staff competency regarding AML/CFT/CPF topics.
	Third Line of Defense	▪ This section discusses how an LFIs independent testing or internal audit function is typically considered the third line of defense and the kind of training the associated personnel (e.g., Chief Internal Auditor) should receive to enable them to perform their function in an AML/CFT/CPF context. ▪ The section also includes several examples of specific training that can be conducted for third line staff to efficiently test an LFIs AML/CFT/CPF policies and procedures.
Documenting the AML/CFT/CPF Training Program	Training Plan	▪ This section discusses how an LFI can develop and document a training plan, and that it should require approval from the board of directors.

		▪ Several examples are given of what information should be included in a training plan.
	Updates to the AML/CFT/CPF Training Program	▪ LFIs must regularly review and update their training program based on an updated training needs assessment. ▪ The section discusses what is included in a training needs assessment (e.g., audit findings, regulatory examinations, LFI staff requests for additional training). ▪ The section also gives examples of sources an LFI should use to update its training program as well as examples of triggers events that would trigger staff training requirements (e.g., issuance of new CBUAE guidance on ML/TF/PF sector risks).
	Methods for Training Delivery	▪ This section details the methods an LFI can use to deliver training, specifically discussing the instructor-led training and self-directed learning methods. ▪ The section provides guidance to LFIs on leveraging third-parties for training development and delivery, emphasizing the need to thoroughly vet the company and material provided.
	Training Records, Documentation, and Assessment	▪ LFIs must document training programs and show that staff attendance is recorded and tracked and that the LFI follows up with staff who do not complete training requirements, with escalation and disciplinary measures in place for staff who are continually non-compliant. ▪ The training programs must include mechanisms to measure staff understanding of training concepts and their ability to apply the material in practice. ▪ The section discusses the importance of evaluating the effectiveness of training sessions/material and the evaluations and staff feedback used to enhance future training.

Best Practices for Licensed Financial Institutions on Implementing a Risk-Based Approach and Conducting Risk-Based Institutional Risk Assessments

Effective from 7/11/2025 **Status:** In-Force

1. Introduction

To implement an effective anti-money laundering ("AML")/combating the financing of terrorism ("CFT")/countering proliferation financing ("CPF") compliance program, a licensed financial institution ("LFI") should apply a risk-based approach ("RBA") to manage its money laundering ("ML"), terrorist financing ("TF"), proliferation financing ("PF"), and other illicit financial activity risk exposure. A reasonably designed RBA provides a framework for identifying the potential risks associated with an LFI's business model and activities, represented by the LFI's customers, products and services, delivery channels, geographic locations and markets, and operating structure. This understanding helps an LFI develop measures based on those risk factors that pose the greatest ML/TF/PF risk.

While the RBA is the overall framework and process that an LFI uses to manage ML/TF/PF risk, the ML/TF/PF risk assessment is a specific part of the RBA. A well-developed ML/TF/PF risk assessment assists LFIs in identifying ML, TF, PF, and other illicit financial activity risks. Based on this assessment of risk, an LFI is well-positioned to identify gaps or opportunities to further improve and develop appropriate risk mitigation measures—including an LFI's

policies, procedures, processes, systems, and controls—in accordance with the nature and extent of the LFI's risk exposure.

1.1. Purpose and Scope

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Best Practices document is to assist the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") LFIs of their statutory obligations under the legal and regulatory framework in force in the UAE, of developing a risk assessment methodology, conducting a riskbased institutional risk assessment, and implementing a risk-based approach. It should be read in conjunction with the CBUAE's Procedures for *Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations (issued by Notice No. 74/2019 dated 19/06/2019) and Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Best Practices document neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the expectations of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this document and the legal or regulatory frameworks currently in force, the latter will prevail. This Best Practices document may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Best Practices paper takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators identified by the FATF. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Best Practices document comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.

1.2. Applicability

Unless otherwise noted, this Best Practices paper applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, stored value facilities, retail payment service providers, card schemes, virtual asset service providers ("VASPs"), registered hawala providers and other LFIs not explicitly mentioned; and
- Insurance and re-insurance companies, agents, and brokers.

1.3. Legal Basis

This Best Practices document builds upon the provisions of the following laws:

- Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended.

- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AML-CFT Decision") and its amendments

- Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions of July 2023.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CPF	Countering proliferation financing
EDD	Enhanced due diligence
FATF	Financial Action Task Force
KYC	Know your customer
LFI	Licensed financial institution
ML	Money laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically exposed person
PF	Proliferation financing
RBA	Risk-based approach
SAR	Suspicious activity report
STR	Suspicious transaction report
TBML	Trade-based money laundering
TF	Terrorist financing
TFS	Targeted Financial Sanctions
VASP	Virtual Asset Service Provider

2. Implementing a Risk-Based Approach

2.1. Definition and Purpose

A Risk-based approach ("RBA") requires LFIs to identify, assess, and manage the ML/TF/PF risks to which they are exposed and subsequently apply AML/CFT/CPF measures commensurate with those risks in order to manage them effectively. A reasonably designed RBA will provide a framework for identifying the degree of potential ML/TF/PF risks associated with an LFI's customers, products and services, delivery channels, geographic locations and markets, and operating structure and enable an institution to focus on those risk factors that pose the greatest ML/TF/PF risk. As a general principle, where there are higher risks, LFIs should take enhanced measures to manage and mitigate those risks, while where the risks are lower, simplified measures (i.e., measures that still meet the core obligations and objectives of UAE laws and regulations but may involve less frequent monitoring or shallower levels of customer due diligence) may be permitted. The RBA thus allows LFIs, consistent with minimum legal and regulatory requirements, to adopt a more flexible set of measures in order to utilize their human, technological, and financial resources more effectively and apply AML/CFT/CPF preventive measures that are commensurate to the nature and level of their risks. As the purpose of the RBA is to allow an LFI to direct the most resources to the highest levels of assessed risk, LFIs should regularly review and update their frameworks to ensure that measures remain effective in managing ML/TF/PF risks.

Under the RBA, institutions that face higher ML/TF/PF risks are expected to develop enhanced measures to mitigate such higher risk by expanding the range, degree, frequency, and intensity of their mitigating controls. Conversely, institutions that face lower ML/TF/PF risks may choose to implement simplified measures, provided these are consistent with minimum legal and regulatory obligations.

As discussed in this Best Practices document, an RBA consists of the following steps:

- Conducting a risk-based institutional ML/TF/PF risk assessment (Section 3); and
- Applying an RBA (Section 4) in the implementation of AML/CFT/CPF controls, ensuring that the LFI's control environment appropriately manages the LFI's identified ML/TF/PF risks.

3. Conducting a Risk-Based Institutional Risk Assessment

3.1. Definition and Overview

As introduced in Section 2.1, an RBA consists of two essential elements: assessing risk and mitigating risk. The risk assessment enables an LFI to identify, assess, and understand the ML/TF/PF risks that may be present in the institution's business activities and clients. In order to do so, LFIs should periodically conduct a risk assessment that, at a minimum, takes into consideration the following:

- The LFI's customers and their characteristics;
- Products and services;
- Delivery channels and transaction-related risks;
- Geographic locations and markets; and

While the RBA is the overall framework and process used to manage ML/TF/PF risk, the conduct of the ML/TF/PF risk assessment is a specific part of the RBA. A risk assessment consists of identifying an institution's inherent ML/TF/PF risks based on the LFI's specific characteristics, business model, and activities; reviewing the design and operational effectiveness of an LFI's control framework to manage these risks; and determining the residual risk that remains after an LFI's controls are applied to its inherent risk. The results of the risk assessment are used to inform the development and implementation of the LFI's risk-based control framework and to continuously monitor and update this framework as necessary. An institutional risk assessment does not need to be complex, but following RBA principles, it should be commensurate with the nature and the size of the institution's operations.

For example, simpler risk assessments may be sufficient for smaller or less complex institutions that carry similar categories of customers or whose activities are circumscribed to a particular jurisdiction or service. Conversely, complex institutions, which service a diverse pool of clients, provide different types of services, or operate in several jurisdictions, will need to perform risk assessments that are sophisticated and aligned with the LFI's complexity. Simpler risk assessments for smaller or less complex LFIs may use more standardized risk matrices or checklists to evaluate risks, while larger institutions may feel the need to develop more detailed risk models and analyses to address more complex risks. For all LFIs, the integration of technologies such as data analytics and artificial intelligence may be considered as a way to possibly enhance the accuracy and efficiency of risk assessments.

3.1.1. Purpose of ML/TF/PF Risk Assessment

The main purpose of the ML/TF/PF risk assessment is to improve an institution's financial crime risk management by identifying the ML/TF/PF risks that an institution is facing, determining how these risks are mitigated by an institution's AML/CFT/CPF controls, and establishing the residual risks that remains for the institution. The results of the risk assessment can be used for a variety of purposes, such as:

- Identifying gaps or opportunities for improvement in AML/CFT/CPF policies, procedures, processes, systems, and other mitigating controls;
- Developing an accurate risk appetite statement that adequately reflects an institution's ML/TF/PF risk tolerance and allows it to implement effective controls and allocate resources on the basis of risk;
- Understanding how a business unit's AML/CFT/CPF compliance program aligns with its risk profile;
- Lowering an institution's residual risk exposure by developing effective risk mitigation strategies and/or reducing exposure to inherent risks that cannot be managed effectively;
- Ensuring senior management is informed of the institution's key risks, controls gaps, and remediation efforts;
- Enhancing regulatory compliance and reporting, ensuring that the institution meets all relevant AML/CFT/CPF requirements;
- Assisting senior management with strategic decisions in relation to customer exits and account restrictions; and
- Informing supervisors about key risks, control gaps, and remediation efforts across the institution.

3.1.2. Overview of the characteristics of an effective risk assessment methodology

To implement an effective ML/TF/PF risk assessment, an LFI should have a well-developed risk assessment methodology that documents all the steps of the risk assessment process and the rationale that supports the ML/TF/PF risk assessment, such as reasoning behind chosen risk factors, scoring criteria, and instances when the LFI has chosen to deviate from standard practices. Although there is no standard risk assessment methodology, the ML/TF/PF risk assessment methodology should describe the risk factors assessed, types of quantitative or qualitative data evaluated, stakeholders involved in the development and review of the risk assessment, criteria used to score, weightings applied to distinct risk factors or categories, and any scoring overrides applied. LFIs should consider integrating external sources of information, such as the UAE national risk assessment, sectoral risk assessments, industry reports, and feedback from supervisory authorities, to enhance the accuracy and relevance of the risk evaluation. LFIs should also consider defining and conducting their risk assessment by assessment units[2], if applicable, that can help the LFI assess ML/TF/PF risks specific to an LFI's particular business line, activity, or legal entity. This includes a commitment to continuous improvement, ensuring that the methodology is regularly reviewed and updated to reflect changes in risks, regulatory requirements, and technological advancements. As such, the methodology should outline the assessment units that are in scope and the process for assessing distinct risk factors, types of data, and weightings across the assessment units. Finally, LFIs should note that data and data analytics-based RBA methodologies should meet the definition of risk management models[3] and should be treated in accordance with the requirements set out in the CBUAE's model management standards.

[2] Assessment units refer to distinct segments of an LFI's operations that may be assessed separately, such as specific business lines, departments, or legal entities.
[3] https://www.centralbank.ae/media/0oaarr3a/model-management-standards-attach-to-notice-5052-2022.pdf

3.1.3. Granularity and level of detail in the risk assessment

LFIs have flexibility regarding how they organize their ML/TF/PF risk assessments. Depending on the size, entity type, and complexity of the specific institution, a risk assessment may be organized across business lines or legal entities

(referred to as assessment units) that can be consolidated into an enterprise-level risk assessment. As much as is possible or practical, LFIs should consider adopting standardized methodologies across assessment units, while ensuring that assessment processes retain flexibility across disparate units to allow for a tailored assessment of risk. Accordingly, a larger LFI may implement a global ML/TF/PF risk assessment with multiple sub-enterprise-level assessment units represented by separate regional or country-level ML/TF/PF risk assessments. For larger LFIs in particular, it is crucial to ensure risk assessments are tailored to the specific business and that the data used is relevant to that business line and has been validated and run through assurance checks. Whatever approach is chosen, however, the results of these assessments should be aggregated into an enterprise-level assessment report of inherent risks, mitigating controls, and residual risks.

3.1.4. Consultation, accountability and stakeholders relevant to the Risk Assessment

The decision regarding who manages and owns the risk assessment process may be impacted by how the risk assessment is conducted (i.e., by business lines, country, or region), and the decision will be influenced by the structure, global footprint, and complexity of an LFI. With that understanding, the ML/TF/PF risk assessment process should be managed by the LFI's Money Laundering Reporting Officer ("MLRO")/Compliance Officer, in coordination with the appropriate risk management function, and owned by the LFI's Board of Directors, owners/partners/shareholders, and senior management who are responsible for overseeing the LFI's AML/CFT/CPF program and providing final approval. Additionally, while an MLRO/Compliance Officer or the dedicated Risk Officer conducts the assessment, it is crucial that the LFI engage first line of defense employees, particularly, business line heads, as they are best positioned to offer detailed insights on ML/TF/PF risks facing their respective business lines, include providing customer and transactional data for the risk assessment. Front line engagement is particularly important as the ownership of ML/TF/PF risks remains with the business, who are also responsible for implementing any actions resulting from the gaps or weaknesses identified by the risk assessment exercise.

3.1.5. Frequency of the ML/TF/PF Risk Assessment

An LFI's ML/TF/PF risk assessment should be updated, at a minimum, on an annual basis, and also in response to certain "trigger" events. Trigger events are associated with changes to the following areas impacting an LFI:

- LFI's organizational structure, business model, or strategy, such as due to mergers or acquisitions and expansion into new markets. This may also include global and regional events with a significant bearing on the LFI's activities.

- Activities stemming from the LFI's customer base; introduction of new products, services, or technologies; or the jurisdictions where the LFI operates.

- AML/CFT/CPF program, including updates to applicable AML/CFT/CPF laws and regulations and implementation of new AML/CFT/CPF controls.

- The UAE's National ML/TF/PF Risk Assessment and CBUAE's Sectoral ML/TF/PF Risk Assessment.

As such, an LFI should update its ML/TF/PF risk assessment in response to the abovementioned trigger events to ensure that the risk assessment remains an accurate reflection of the LFI's ML/TF/PF risks and control environment.

3.2. Principles and Best Practices for ML/TF/PF Institutional Risk Assessments

An institutional risk assessment consists of three core steps:

- **Inherent Risk:** an identification and assessment of the ML/TF/PF risks inherent to an LFI's business model and activities, including specific risks associated with an LFI's customers, products and services, delivery channels, geographies, and operating structure.

- **Assessing the Control Environment:** an assessment of the design and operational effectiveness of the policies, procedures, systems, and other controls in place to mitigate the LFI's inherent ML/TF/PF risks.

- **Residual Risk:** an assessment of the risk that remains after an LFI's controls are applied to its inherent risk.



3.2.1. General Best Practices

As noted above, the RBA approach allows LFIs some flexibility in designing and implementing a risk assessment methodology that is tailored to the size, entity type, and complexity of the specific institution. Recognizing that risk assessments will therefore vary in accordance with a given LFI's activities and risk profile, all LFIs should implement the following best practices associated with their ML/TF/PF institutional risk assessment:

- **Data quality:** LFIs should conduct thorough data quality and assurance checks on the data that is utilized for the risk assessment. To this end, LFIs should apply sound scientific methods or algorithms to address any missing or incorrect data. LFIs should also utilize feedback mechanisms to address any inconsistencies or issues observed across data sets. With that understanding, the risk assessment exercise is not the tool for LFIs to rectify and address such data quality issues.

- **Quantitative Calculations:** LFIs should use quantifiable metrics to inform the risk assessment exercise. Specifically, LFIs should establish criteria to measure the effectiveness of each AML/CFT/CPF control. This can involve setting measurable goals for each control with metrics that are quantifiable in nature, such as a reduction in the number of flagged transactions that require no further action (decrease in false positives). LFIs should collect metrics on how each control performs against the established criteria. Such metrics should be linked to an objective assessment regarding the performance of certain controls within the LFI and that are weighted in proportion to their significance to an LFI's overall AML/CFT/CPF program. Please refer to Section 3.2.3 for more information on how to use metrics to assess an LFI's control environment.

- **Workpapers:** LFIs should maintain a record of any workpapers or risk assessment tools utilized to collect data and calculate scores or ratings for the ML/TF/PF institutional risk assessment.

- **Report:** LFIs should prepare a finalized, enterprise-level ML/TF/PF institutional risk assessment report consisting of an assessment of ML/TF/PF inherent risks, mitigating controls, and residual risks, together with any supporting data, observations, and qualitative analysis. LFIs with multiple branches or business lines may maintain risk assessments for multiple sub-enterprise-level assessment units; however, the results of these assessments should be consolidated into an enterprise-level assessment of inherent risks, mitigating controls, and residual risks.

- **Policies and governance documentation:** LFIs should document their ML/TF/PF institutional risk assessment policies and governance structures and processes. Such documentation should clearly indicate required approvals for the risk assessment report and/or methodology, the required frequency for conducting risk assessments, and any follow-up actions the institution takes to address control weaknesses or areas of heighted residual risk identified by the risk assessment.

- **Third-party arrangements**: In cases where an LFI chooses to engage the services of a consultant, the LFI should ensure that the consultant delivers the contracted services under stringent oversight of key personnel nominated by the LFI and that such key personnel have a clear grasp of the services provided by the consultant. LFIs should avoid arrangements with consultants that result in an overreliance/dependency on such consultants. LFIs ultimately own the ML/TF/PF institutional risk assessment process and outcomes.

3.2.2. Assessing Inherent Risk

Global standards emphasize that effective risk management is predicated on a sound understanding of the risks inherent to an entity's business model. While there are different methods to conduct a risk assessment, LFIs are generally expected to evaluate, at a minimum, the differing levels of risk associated with their customers, products and services, delivery channels, geographic locations and markets, and operating structure, as appropriate. Depending on the nature, size, and complexity of their business, LFIs should also take into consideration other risk factors that might have a significant impact on the institution's exposure to ML/TF/PF risks. Some of the additional risk factors include, but not limited to, transaction-related risk (refer to CBUAE Notice 3599); relative size of the LFI's business; introduction of new products or services, new technologies or delivery processes; and the LFI's establishment of new branches and subsidiaries locally and abroad.

The following best practices can assist LFIs in effectively assessing their inherent risks, which is followed by a discussion of specific best practices for each core category of inherent risk.

- The risk assessment should consider high-risk factors and provide a reasonable rationale for situations where high-risk factors are not considered. For example, under the category of customer risk, an LFI may wish to consider the number of customers it has exited for financial crimes compliance ("FCC") reasons during the risk assessment review period and the number customers who have been the subject of a suspicious transaction report ("STR") or suspicious activity report ("SAR") during the risk assessment review period. If the number of customers exited for FCC reasons or STRs/SARs is not included in an LFI's risk assessment due to systems limitations, the risk assessment should note that the inherent risk rating is elevated due to the system limitation.

- The LFI should utilize a standardized approach to assessing its customers, products and services, geographies, and other factors, as applicable, and should, to the extent possible, utilize the same risk segments and risk rating methodologies in the institutional risk assessment as it utilizes as part of its day-to-day AML/CFT/CPF compliance program.

- Within each broad category of inherent risk (such as customer risk, product and service risk, geographies, etc.), the risk assessment should consider more granular risk factors for that category of inherent risk. Examples of granular risk factors for customer risk include a customer's place of residence or incorporation and primary place of business. Granular risk factors are addressed in Sections 3.2.2.1 to 3.2.2.5 under each broad category of inherent risk.

- The LFI should assign each factor a score or weighting that reflects the level of risk associated with that risk factor and the prevalence of that risk compared to other risk factors. Each risk area may then be assigned a weight that reflects the level of importance in the overall risk calculation relative to other risk areas. The risk score or weighting for each factor should be considered in the context of the collective risk assessed and measured by the LFI.

- The risk assessment should consider specific ML/TF/PF and other illicit financial activity risks associated with the LFI's business model and operating environment, including risks specific to the UAE, as identified in national and sectoral risk assessments and by international standard setters such as the FATF.

- While there is flexibility in the structure and flow of a risk assessment document, all LFIs should ensure that the assessment of risk factors includes quantitative data as a basis for evaluating and scoring each inherent

risk category. The quantitative data should apply to the more granular risk factors for each category of inherent risk. For example, a higher weight could be assigned to factors like transaction volume or customer profile if they are deemed to have a greater impact on ML/TF/PF risk

- The risk assessment is a living document to be reviewed periodically and updated as the LFI prepares to add products or services, open locations in a new jurisdiction, or adopt a new piece of technology to serve its customers. An LFI's compliance department should insist upon a completed and approved risk assessment before an LFI adds a major new line of business.

- LFIs are encouraged to consider enhancing their risk assessments by utilizing the data submitted to the CBUAE for its annual institutional risk assessment.

3.2.2.1. Customers

An LFI's customer risk is based on the characteristics of its customer base, including the concentration of customers in risk-rated segments, customers' industries, professions, and entity type, and risk ratings of beneficial owners and other related parties, among other factors. The following are key drivers of inherent ML/TF/PF customer risk:

- Place of residence or incorporation and primary place of business;[4]

- Profession or industry, including but not limited to customers involved in financial services, real estate, export/import, or shipping, or those that are charities or other nonprofit organizations;

- Regulatory status (e.g., as a financial institution, virtual asset service provider ("VASP"), or designated non-financial business or profession ("DNFBP"));

- Business or other income-generating activities;

- Whether a customer is expected to transact with high-risk sectors, as defined by the LFI;

- Historical risk markers, such as being the subject of material negative news;

- Status as or exposure to politically exposed persons ("PEPs"), including through beneficial owners and other related parties;

- Corporate form and ownership structure; and

- Length of customer relationship.

[4] LFIs may opt to address risks stemming from an LFI's exposure to customers resident, incorporated, or operating in higher-risk jurisdictions through their assessment of geographic risks, as discussed below.

3.2.2.2. Products and Services

Product and service risk derives from the range of products and services that an LFI offers its customers and whether those products and services have characteristics that present elevated illicit finance risk. The products and services a company offers are a key means by which illicit actors can exploit a company to introduce ill-gotten gains into the financial system, layer transactions to complicate any investigation into the source of funds or integrate illicit funds to make them appear legitimate. The following are key drivers of inherent ML/TF/PF product and service risk:

- Potential for intermediation (e.g., if an LFI acts as an intermediary in delivering the product or service, or the institution relies on a third party for information about a transacting party);
- Use of a higher-risk medium of exchange, such as cash, gold, or cryptocurrency;
- Use of products or services leveraging emerging technologies and financial innovations;
- Potential for anonymity or limited transparency;
- Cross-border flows of funds;
- Use of services that may enable pooling or obfuscation of funds, or in which multiple or anonymous parties can have authority over the disposition of funds;
- Favour complexity, especially when that complexity is excessive or unnecessary;
- Involvement of multiple currencies or the conversion from one currency to another; and
- Near-instantaneous or irrevocable settlement or processing (also a driver of delivery channel risk).

3.2.2.3. Delivery Channels

Delivery channel risk stems from the extent to which an LFI's methods of account origination/customer onboarding, account servicing, and transaction facilitation limit its understanding of its customers' identities, activities, and counterparties. The following are key drivers of inherent ML/TF/PF delivery channel risk:

- Use of non-face-to-face channels;
- Proportion of unsolicited (e.g., walk-in) customers;
- Reliance on delivery by or through a third party; and
- Near-instantaneous or irrevocable settlement or processing (also a driver of product and service risk).

3.2.2.4. Geographies

Geographic risk stems from an LFI's exposure—through its operating locations (including those of any global affiliates and branches located outside of the UAE), customer base, and transactions—to regions and jurisdictions that present an elevated degree of illicit finance risk. The following are key drivers of inherent ML/TF/PF geographic risk:

- Institutional exposure (i.e., where the financial institution and its affiliates have locations and where it conducts business), including through proximity to higher-risk regions or jurisdiction in which the LFI may not directly operate; and
- Customer exposure (i.e., customers' country of citizenship or residence, locations of incorporation or registration, primary place or business/headquarters, locations of beneficial owners and related parties[5], and jurisdictions from which customers transact with the financial institution).[6]

Measuring Inherent Risk

An LFI may choose to assess its inherent risk based on the likelihood that a ML/TF/PF risk event occurs and the impact should a ML/TF/PF risk event materialize, referred to as "risk scenarios."

- **Likelihood** is the potential for ML/TF/PF being present.
- **Impact** is the damage incurred if ML/TF/PF occurs.

To extent possible, the likelihood should be assessed on a relative scale and should be based on objective and/or quantifiable information. Subject matter expert inputs may be utilized to map likelihood scores to a rating category on a multi-scale system such as the following:

- **Very High:** Almost certain that a ML/TF/PF risk event will occur several times a year.
- **High:** High chance that a ML/TF/PF risk event will probably occur several times a year.
- **Moderate:** Moderate chance that a ML/TF/PF risk event will occur once a year.
- **Low:** Low chance but not impossible that a ML/TF/PF risk event will occur.
- **Incidental:** Relatively no chance that a ML/TF/PF risk event will occur.

Based on the risk factors discussed below in Section 3.2, certain risk factors contribute to lower or higher likelihood for ML/TF/PF risk. For example, customers in higher-risk professions or industries (as discussed in Section 3.2.2.1) will have a higher likelihood for ML/TF/PF risk. Furthermore, certain products and customer segments may pose a greater likelihood that an ML/TF/PF event will occur due to the value, volume, pattern of usage or the customer behavior associated with the products. Understanding likelihood, an LFI should then rate the impact if a ML/TF/PF event indeed occurs.

The impact can be assessed based on the possible regulatory, legal, financial, and reputational effects that could result if a ML/TF/PF event occurs. A five-level scale is provided as an example, but an LFI should adapt this scale to its business and activities.

- **Catastrophic:** The most severe damage (such as resulting in the loss of a license).
- **Major:** Significant damage.
- **Moderate:** Moderate level of damage.
- **Minor:** Minimal level of damage.
- **Incidental:** Little or no damage.

In this way, the LFI can determine the inherent risk rating of a risk factor. For example, the likelihood of an LFI's new CDD/KYC system or payment screening system suffering an extended outage may range from low to moderate depending on factors such as historical production incidents, existence of a data governance function and sophisticated application performance management capabilities etc.), but the impact that an outage would have on the LFI's operations is major. Please see the below matrix as an illustrative example for plotting likelihood and impact of a risk scenario to arrive at an LFI's inherent risk rating.

Inherent Risk Rating as a Function of Likelihood and Impact

		Impact				
		Incidental - 1	Low - 2	Moderate - 3	Major - 4	Catastropic - 5
Likelihood	Very High - 5	Moderate - 5	High - 10	High - 15	Very High - 20	Very High - 25

	High - 4	Moderate - 4	Moderate - 8	High - 12	High - 16	Very High - 20
	Moderate - 3	Low - 3	Moderate - 6	Moderate - 9	High - 12	High - 15
	Low - 2	Very Low - 2	Low - 4	Moderate - 6	Moderate - 8	High - 10
	Very Low - 1	Very Low - 1	Very Low - 2	Low - 3	Moderate - 4	Moderate - 5
Risk Score						

LFIs may adapt this inherent risk rating matrix for all types of customers, products and services, delivery channels and transactions, and geographies. For instance, a customer engaged in high-risk industries such as cryptocurrency trading might be rated as having a 'High' likelihood of ML/TF/PF risk, with an impact rating of 'Major' due to potential legal and reputational damage if involved in illicit activities.

---

[5] Related parties defined here as "Group and its Controlling Shareholders, Members of its Board and Senior Management, (and their First-Degree Relatives) and persons with control, joint control or significant influence over the Bank (and their First-Degree Relatives".
[6] LFIs may opt to address risks stemming from an LFI's exposure to customers resident, incorporated, or operating in higher-risk jurisdictions through their assessment of customer risks, as discussed below.

3.2.3. Assessing the Control Environment

Once inherent risks have been identified and assessed, LFIs should assess mitigating controls to determine how effectively they manage the institution's risks. Mitigating controls include the LFI's policies, procedures, processes, systems, and other risk-mitigating measures, including overall governance and management oversight, customer due diligence ("CDD")/know your customer ("KYC"), internal controls (including suspicious transaction reporting and recordkeeping), training, and independent testing or independent audit. The following best practices can assist institutions in effectively assessing their mitigating controls, followed by specific best practices for each core controls category.

- To the extent possible, LFIs should map controls to specific drivers of inherent ML/TF/PF risk to ensure adequate coverage of mitigating controls, consistent with the RBA, and should assess controls both for appropriate design and for operational effectiveness.

- Each control area assessed should be assigned a score that reflects the relative strength of that control as well as a weighting based on the importance that the institution places on that control, given the institution's overall risk profile and risk appetite. The LFI should develop a table defining the scores used and the rationale applied when assigning a score to a given control's effectiveness.

- Where the LFI identifies a coverage gap in its existing control framework or determines that a specific control is not designed appropriately or operating effectively, the LFI should raise an action to remedy the deficiency if an action is not already underway.

- Control effectiveness assessments should be based on objective and quantifiable information tied to the controls. Examples of quantifiable factors include but are not limited to the following (the following is a non-exhaustive list of control effectiveness factors provided as examples. LFIs should develop detailed factors commensurate with their own customer, business and risk profiles):

    - The ratio of AML and sanctions related alerts flagged as deficient by independent quality assurance checks/assessments

    - The time taken to perform regulatory gap assessments and implementing the remedial measures identified by such assessments

- The rolling rate of STR/SAR to total alert ratio and noteworthy alert to total alert ratio
- The number of audit and compliance assurance issues and the time taken to address these issues
- The rate of false positives in transaction monitoring systems
- The ratio of low/medium risk rated customers that subsequently had STRs/SARs filed and/or high number of payments rejected by correspondent banks

3.2.3.1. Governance

An LFI's organizational structure and governance are key components to understanding and implementing AML/CFT/CPF controls and building an institution-wide culture of compliance. An LFI's organizational structure and governance should ensure that:

- Program documentation provides a clear framework for AML/CFT/CPF regulatory obligations— even through legal and regulatory changes or evolving compliance expectations and changes in compliance leadership—and is approved by the Board of Directors or an appropriate Board-level committee;
- The risk assessment process gives an LFI a baseline understanding of its risks and provides for the foundational framework for establishing a risk-based approach for both designing an AML/CFT/CPF compliance program and allocating resources to manage related risks;
- The compliance function is led by individuals with deep expertise in AML/CFT/CPF issues and the function has the appropriate authority and independence to manage AML/CFT/CPF risks, as established through clear reporting lines and communications ultimately up to the Board of Directors or a designated Board-level committee; and
- All levels of the institution understand and support the AML/CFT/CPF compliance mission through culture of compliance that is woven into the ordinary course of business, including through:
    - The responsibilities of the Board of Directors and/or designated Board-level committee(s) are explicitly discussed;
    - The clear support and commitment of senior and mid-level management that sets a "tone from the top" in support of compliance objectives;
    - Adequate human, technological, and financial resources to execute on compliance-related responsibilities; and
    - Effective communication, incentives, and consequence management that together reinforce the culture of compliance.

Considerations to determine whether an LFI's governance controls are adequate and effective include:

- The LFI's risk appetite statement refers to ML/TF/PF risks and is subsequently integrated in the LFI's policies.
- The LFI performed an AML/CFT/CPF risk assessment that is documented, has been regularly updated, and evaluates the LFI's risk exposure across ML/TF/PF.

- The LFI has designated a MLRO/Compliance Officer who has his/her designation reported to CBUAE.
- The LFI operates across a three lines of defense model with roles that are appropriately segregated and enforced across the institution, such that the MLRO/Compliance Officer and the Compliance function are independent from business and first line activities.
- The MLRO/Compliance Officer reports directly to the Board of Directors, Board-designated committee, or owners/partners/shareholders.
- The LFI has developed an appropriate plan to address findings from any external compliance reviewer and a way to track the status of the remediation.
- Policies and procedures are updated and approved in a timely fashion and by the correct authority within the LFI.

3.2.3.2. CDD/KYC

Mitigating measures related to CDD/KYC are a key element of AML/CFT/CPF risk management, providing vital information about each customer. A robust CDD/KYC program establishes the LFI's understanding of risks associated with each customer as well as each customer's expected activity, better enabling the institution to detect unusual or potentially suspicious transactions. Effective CDD/KYC programs allow LFIs to segment customers by risk, apply appropriate Enhanced Due Diligence ("EDD") measures to customers designated as posing elevated levels of risk, and to give management a thorough understanding of the institution's customer base.

An effective CDD/KYC program has four essential elements:

- Customer identification and verification;
- Beneficial ownership identification and verification;
- Understanding the nature and purpose of customer relationships (including the identification of potential politically exposed persons ("PEPs") to develop a customer risk profile; and
- Ongoing monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information.

In addition to baseline CDD/KYC requirements that apply to all customers, LFIs are expected to apply specific and enhanced due diligence ("EDD") measures on the basis of a given customer's risk profile, as assessed at onboarding and on an ongoing basis thereafter.

Considerations to determine whether an LFI's CDD/KYC controls are adequate and effective include:

- The LFI has a clear client acceptance policy, and it is followed.
- The LFI undertakes adequate CDD/KYC for individual customers and legal entity customers.
- The LFI undertakes the appropriate measures to understand the customer's ownership and control structure and identify and verify the identity of the customer's beneficial owners.
- The LFI has appropriate measures to understand the purpose of the business relationship and nature of a customer's business.

- The LFI applies CDD/KYC measures not just prior to beginning any business relationships but on an ongoing basis, where appropriate.

- The LFI has a proper process to screen customers at onboarding and on an ongoing basis for sanctions and adverse media.

- The LFI undertakes adequate specialize due diligence and EDD for high-risk customers (such as for PEPs, correspondent banking relationships, etc.).

3.2.3.3. Internal Controls

Mitigating measures related to internal controls entail policies, procedures, and processes designed to limit and control risks associated with core operational elements of the LFI's AML/CFT/CPF program and achieve compliance with relevant laws and regulations. In addition to policies and procedures, effective internal controls also encompass technological systems that an LFI uses to identify, assess, and manage compliance risks, including the LFI's approach to suspicious activity monitoring, investigation, and reporting; other reporting and information sharing; recordkeeping and record retention; and risk assessment.

- The suspicious activity monitoring program helps the LFI validate its risk assessment on a client- by-client and institution-wide basis to inform the suspicious activity reporting program;

- Suspicious activity reports and information sharing provide valuable leads to law enforcement agencies and help shape investigative priorities and inform prosecutions; and

- The recordkeeping and record retention obligations require documentation and trail of information to evidence the investigation conducted by LFIs which led to the regulatory reporting. LFIs should evaluate whether records are complete, accurate, and readily accessible for the required retention period. This includes checking that records support the investigation and reporting of suspicious activities and are compliant with regulatory requirements.

Overall, the policies, procedures, and processes that comprise the LFI's system of internal controls also have implications for the institution's organizational structure, including staff to ensure appropriate allocation of resources to appropriately address risks and ensure effective implementation of controls. In addition to baseline internal controls that apply to all operations, LFIs are expected to apply specific and enhanced monitoring to higher-risk areas.

Considerations to determine whether an LFI's internal controls are adequate and effective include:

- The LFI maintains consistent and complete customer data in relevant systems and has a sufficient alert workflow to manage and close/escalate the alerts.

- The LFI monitors all business relationships (including employee accounts) on an adequate basis with a monitoring system/process that is up to date and adequately designed to detect ML/TF/PF transactions and activity in line with the LFI's ML/TF/PF risk assessment and business.

- The LFI has an adequate process in place to report suspicious transactions and activity to the Financial Intelligence Unit and to decide whether an investigated account should be maintained, closed or subject to further monitoring.

- The LFI effectively implements its sanctions screening regime in accordance with regulatory requirements, such that the sanctions screening regime is configured to detect and manage the specific sanctions risks to which the LFI is exposed and is calibrated to the size, nature, and complexity of the LFI.

- The LFI implements Targeted Financial Sanctions ("TFS") during: (i) alert screening at customer onboarding and throughout the business relationship; and (ii) payment screening.

- The LFI maintains all customer records such that transactions recorded in the customer's account can evidence the investigation conducted by LFIs which led to the regulatory reporting.

3.2.3.4. Training

Global standards consistently emphasize the need for an enterprise-wide AML/CFT/CPF training program for all appropriate personnel within an LFI. Comprehensive mitigating measures related to training are critical to the overall effectiveness of an AML/CFT/CPF compliance program. Training should be provided on an ongoing basis and include changes to regulations, internal policies or procedures, and an understanding of evolving AML/CFT/CPF risks to which the LFI is exposed.

At a minimum, a comprehensive AML/CFT/CPF training program should ensure that:

- All new employees receive the LFI's required AML/CFT/CPF training within a specified time from their onboarding date;

- All staff within an LFI receive AML/CFT/CPF awareness training at least annually;

- The LFI provides targeted and role-based training to employees in the relevant compliance functions;

- The LFI provides targeted and role-based training to front-line staff with heightened exposure to AML/CFT/CPF risk;

- The LFI provides AML/CFT/CPF training an ongoing basis to the third line of defense; and

- The LFI provides AML/CFT/CPF training to the LFI's board of directors and senior management.

Considerations to determine whether an LFI's training controls are adequate and effective include:

- The LFI provides compulsory AML/CFT/CPF induction training and ongoing refresher AML/CFT/CPF training to all staff, including the Board of Directors and senior management;

- The LFI provides certain specialized and role-based training programs for relevant staff with AML/CFT/CPF responsibilities (e.g., TBML and PF awareness training for teams facilitating trade- finance).

- The LFI maintains training attendance and assessment records, and follows up on employees who repeatedly do not attend or fail trainings

- AML/CFT/CPF trainings are customized to the LFI's risk and the nature of its operations, including local regulatory requirements.

3.2.3.5. Independent Testing

Independent Testing is a risk-based, objective evaluation of the overall strength and quality of an LFI's AML/CFT/CPF program. Testing includes reviewing the LFI's policies, procedures, systems, and controls that mitigate and manage an LFI's ML/TF/PF risks and identifying any areas of the compliance program that may require remediation or improvement. Best practices suggest periodic testing of the AML/CFT/CPF program every 12-18 months or in light of significant changes to the LFI's risk profile, policies, procedures, systems, controls, or compliance staff. Although many LFIs have internal audit departments that execute independent testing, outside auditors, consultants, or other qualified independent parties can also conduct independent testing and/or audits.

Institutions should take steps to ensure the autonomy of the independent testing function by separating the resources dedicated to testing from those that create the policies, procedures, systems, and controls subject to testing. For LFIs that use external auditors or consultants for independent testing, the audit/independent testing program should ensure that there is no conflict of interest between the external auditors and the LFI. Conflicts of interest may include external auditors providing additional services such as training or helping the LFI develop and implement its compliance policies, procedures, systems, and controls.

At a minimum, a comprehensive audit/independent testing program should assess:

- The overall integrity and effectiveness of the institution's AML/CFT/CPF program, including policies, procedures, and processes;
- The LFI's risk assessment for reasonableness given the LFI's risk profile;
- The LFI's adherence to global standards regarding identifying, investigating, and reporting different types of suspicious transactions and maintaining relevant records;
- Management's efforts to resolve violations and deficiencies identified in previously conducted independent testing and audit reports; and
- The integrity and accuracy of the LFI's information technology systems and automated programs used to identify suspicious transactions and possible sanctions hits to satisfy AML/CFT/CPF compliance requirements.

The findings identified in the independent testing of the AML/CFT/CPF program should be promptly provided to the LFI's Board of Directors or owners/partners/shareholders in a comprehensive audit report. The audit report should contain the methodology of the independent testing and mention any violations; inconsistencies between policy, procedures, and processes and the way they are applied; and any other program deficiencies found during the assessment. Most importantly, the comprehensive report should assist the LFI's Board of Directors, owners/partners/shareholders, and senior management in identifying, prioritizing, implementing, and tracking corrective actions meant to address these deficiencies.

Considerations to determine whether an LFI's independent testing controls are adequate and effective include:

- The LFI has established an effective audit function which is independent of all operations.
- The audit function is appropriately staffed and organised.
- The audit function has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the LFI's ML/TF/PF risks.
- The audit function performs periodic inspections, and testing covers all aspects of the LFI's AML/CFT/CPF compliance program, which is supported with a comprehensive methodology and testing plan.
- The LFI's audit plan and audit report have been approved by the LFI's Board of Directors, Board- designated committee, or owners/partners/shareholders.

Quantifying Control Effectiveness

To quantify control effectiveness, an LFI should consider applying the following steps:

1. **Identify Key Controls**: LFIs should list all relevant controls that have been implemented to mitigate identified risks. These controls may include CDD/KYC procedures, transaction monitoring systems, employee training

programs, and compliance auditing mechanisms.

2. **Define Effectiveness Criteria**: LFIs should establish criteria to measure the effectiveness of each control. This can involve setting specific, measurable goals for each control, such as reduction in the number of flagged transactions that require no further action (decrease in false positives), or the speed and accuracy of identifying high-risk transactions or clients.

3. **Measure Performance Against Criteria**: LFIs should collect data on how each control performs against the established criteria. This can involve quantitative measures such as the number of STRs/SARs filed, the rate of compliance with CDD/KYC requirements, or qualitative assessments through internal audits and external reviews.

4. **Scoring System for Controls**: LFIs should develop a scoring system to rate the effectiveness of each control based on its performance. For example, you might score controls on a scale from 1 (ineffective) to 5 (highly effective) based on how well they meet the effectiveness criteria.

5. **Aggregate Control Scores**: LFIs should calculate an overall control effectiveness score by aggregating the scores of individual controls. This can be done through a weighted average if certain controls are deemed more critical than others based on your institution's risk profile.

6. **Adjust for Interdependencies**: LFIs should recognize that controls might be interdependent. The effectiveness of one control might enhance or depend on the effectiveness of another. Consider these relationships when evaluating overall effectiveness.

7. **Feedback and Improvement Cycle**: LFIs should use the results from the quantification exercise to identify areas where controls could be improved. LFIs should then implement feedback loops where control effectiveness data is regularly reviewed and used to adjust control mechanisms.

8. **Regular Updates and Reviews**: Control effectiveness should be an ongoing concern, with regular updates and reviews, to ensure that controls are adapting to evolving risks, regulatory changes, and operational requirements.

9. **Documentation and Reporting**: LFIs should keep detailed records of the evaluation process, results, and any subsequent actions taken to improve control effectiveness.

3.2.4. Determining Residual Risk

3.2.4.1. Approach

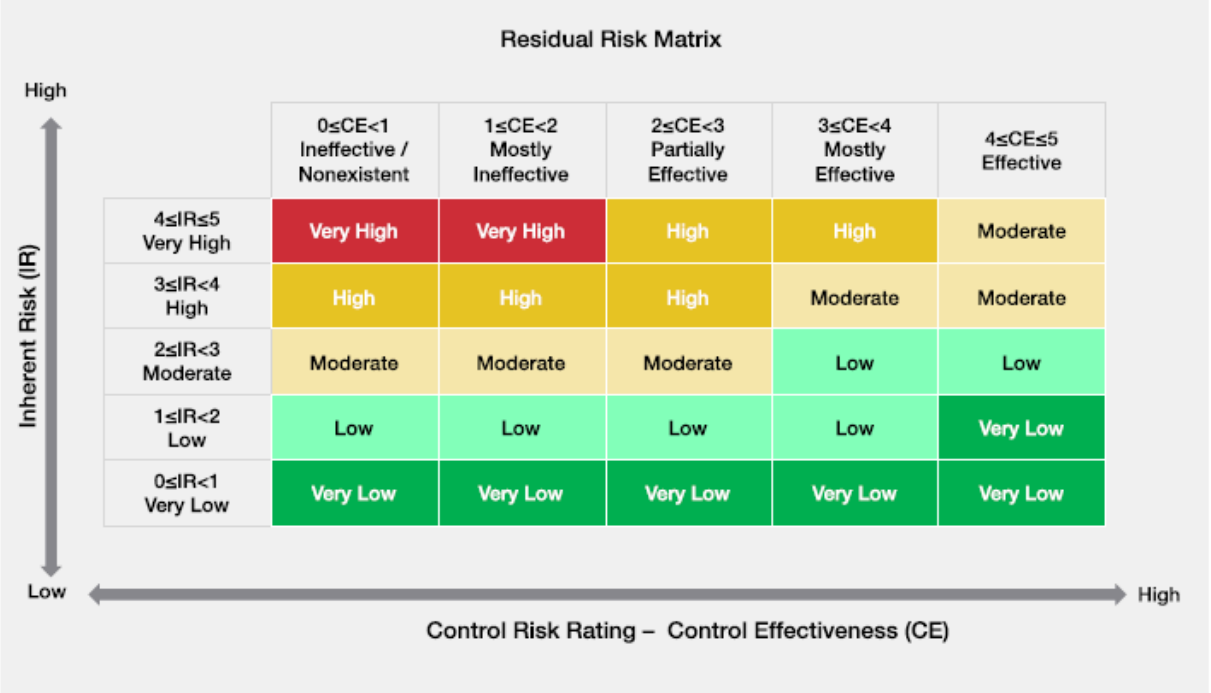
Once both the inherent risk and the design and effectiveness of an entity's mitigating controls have been considered, risk assessments should determine the entity's overall residual risk. Overall enterprise-wide residual risk is a function of the total inherent risk to which the LFI is exposed—through the customers, geographies, products, services, delivery channels, transactions, and operational factors—and the extent to which its controls effectiveness limits the real risk that the inherent exposure will cause harm.

Determining residual risk is important to identify the nature and extent of ML/TF/PF risks so that an LFI's AML/CFT program can include tailored and effective risk mitigating measures, dedicating additional human, technological, and financial resources to the areas of the entity's highest risk. To that end, the outputs and findings of an LFI's risk assessment should be reasonable, and wherever the results are different than expected, these discrepancies should be rationally explained. LFIs should also retain previous versions of risk assessments to quickly and succinctly demonstrate to regulators or third-party assessors how the LFI's risk environment, related mitigating

controls/measures, and residual risk have evolved over time. Senior management and the Board of Directors or owners/partners/shareholders can also reference previous versions when considering the LFI's risk appetite.

3.2.4.2. Residual Risk Matrix

A common practice for determining overall residual risk is the utilization of a residual risk matrix that aligns inherent risk and mitigating controls ratings or scores to generate a residual risk rating or score along a standardized assessment scale. Below is a sample residual risk matrix that utilizes a five-level scale for assessing inherent risks, mitigating controls, and the resulting residual risks. The below graphic is one example of a matrix that an LFI could leverage, and it is not meant to be mandatory or definitive. If an LFI, in the process of conducting its risk assessment, concludes a different risk rating matrix is more suited to its operating environment, an LFI should develop a risk rating matrix, which meets the minimum regulatory standards. The process for developing the risk rating matrix and rationale behind such a process should be clearly and thoroughly documented in an LFI's risk assessment methodology.



4. Application of an RBA

Once the LFI has identified and assessed the ML/TF/PF risks it faces, an LFI's Board of Directors, owners/partners/shareholders, or senior management should revisit the LFI's risk appetite statement to ensure it adequately reflects an institution's ML/TF/PF risk. The LFI's Board of Directors, owners/partners/shareholders or senior management should also assess whether they would like to lower the LFI's residual risk exposure by developing or updating AML/CFT/CPF controls and/or reducing exposure to inherent risks that cannot be managed effectively.

Based on this understanding, the LFI should develop a detailed action plan for the Board of Directors or owners/partners/shareholders that outlines new or updated AML/CFT/CPF controls for addressing inherent risks identified in the ML/TF/PF risk assessment and includes an estimated timeline of implementation. This action plan should take into account an RBA, such that if an LFI's residual risk increases, for instance, revealing that an LFI faces higher ML/TF/PF risks, the LFI may seek to develop enhanced measures to mitigate such higher risk by expanding the range, degree, frequency, and intensity of its AML/CFT/CPF controls. If possible, LFIs should consider leveraging advanced technology and data analytics to enhance its controls and measures. LFIs should clearly define the roles and responsibilities of different parts of the business in developing and executing changes to AML/CFT/CPF controls. Development and execution of changes to an LFI's AML/CFT/CPF controls may be tasked to different parts of an LFI's business, but the MLRO/Compliance Officer should maintain oversight and undertake coordination of

these efforts. LFIs should prioritize controls and measures implementation based on where the assessment identified program gaps and deficiencies with increased levels of residual risk.

In accordance with an RBA, LFIs should mitigate identified risks through the implementation and updating of controls and measures tailored to these risks, such as:

- CDD/KYC processes, including customer and beneficial ownership identification and verification and developing an understanding the nature and intended purpose of the business relationship to establish a customer risk profile;
- EDD measures in higher-risk scenarios to obtain additional information on the customer and ensure enhanced ongoing monitoring and oversight of the customer relationship;
- Ongoing CDD monitoring to maintain current, accurate, and complete customer information and identify changes to the customer risk profile, which includes a risk-based frequency of sanctions and negative news screening of customers as well as routine transaction monitoring to develop averages of values/volumes transacted;
- Transaction monitoring controls and measures that detect and alert the LFI when customers have transactions based on the size, frequency, or patterns that may indicate unusual or potentially suspicious activity as well as activity that may be inconsistent with a customer's risk profile and/or history;
- Sanctions screening controls and measures for screening customers and transactions against relevant lists (e.g., the UN Consolidated List and the Local Terrorist Lists), reviewing potential sanctions matches, and escalating and reporting true sanctions hits;
- Suspicious activity monitoring systems and processes that are aligned to the institution's ML/TF/PF risk assessment and tailored to individual customer risk profiles, together with effective processes for reporting suspicious transactions or activity;
- Appropriate governance arrangements under which responsibility for AML/CFT/CPF is clearly allocated and senior leadership is closely involved in developing and implementing the RBA across the institution;
- Processes to recruit and vet staff in line with the institution's level and type of ML/TF/PF risk, to incentivize the advancement of compliance objectives, and to monitor the integrity of staff;
- Ongoing and role-based training for AML/CFT/CPF staff on the institution's business activities, risks, regulatory obligations, and policies and procedures;
- Controls to test the overall effectiveness of the institution's AML/CFT/CPF policies, procedures, and processes, including independent testing or auditing of the design and implementation of the institution's AML/CFT framework.

An effective RBA will help LFIs to address emerging risks and potential gaps or weaknesses in the AML/CFT/CPF framework that can be mitigated by introducing additional risk mitigation controls (new IT systems, supplemental job aids and desktop procedures, additional ML/TF/PF trainings on a particular topics, etc.), deploying additional resources (such as resources to support with CDD/KYC backlogs and late regulatory filings), and/or reducing exposure to inherent risks that cannot be managed effectively, as appropriate.

5. Conclusion

An ML/TF/PF risk assessment provides a snapshot of an LFI's ML/TF/PF risks and highlights gaps or weaknesses in an LFI's AML/CFT/CPF control environment. It is important that risk assessment findings are shared with an LFI's

business lines, senior management, and Board of Directors, Board-designated committee, or owners/partners/shareholders, including other relevant stakeholders involved in the risk assessment process. Such stakeholders should be informed about the LFI's residual risk and on whether the risk assessment findings have changed or remained the same. Additionally, LFIs may wish to conduct a comparative analysis between the most recently conducted risk assessment and the one that preceded it, in order to keep a record of how the LFI has addressed it's AML/CFT/CPF program gaps and deficiencies over time.

Once an LFI has updated AML/CFT/CPF controls and based on the findings of the ML/TF/PF risk assessment, the LFI should review and test any new or revised controls. Such testing—whether conducted internally or by an independent third party—should be completed before the LFI's next risk assessment in order for the LFI to properly assess whether gaps from the risk assessment are addressed and aligned with the LFI's risk appetite. Findings from an LFI's risk assessment will also inform an LFI's business strategy, spanning customer exit decisions, monitoring and testing plans, and management information system data collected across an LFI. As such, LFIs should implement a robust ML/TF/PF risk assessment and pay particular attention to high-risk areas identified in the ML/TF/PF risk assessment in order to target the LFI's human, technological, and financial resources more effectively.

6. Annexure 1: Synopsis of the Best Practice

Introduction	Purpose and Scope of the Best Practices	The purpose of this Best Practices document is to assist the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") LFIs of their statutory obligations under the legal and regulatory framework in force in the UAE, of developing a risk assessment methodology, conducting a risk-based institutional risk assessment, and implementing a risk-based approach.
	Applicability	This Best Practices applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, virtual asset service providers, registered hawala providers; and insurance and re-insurance companies, agencies, and brokers.
	Legal Basis	▪ Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations as amended. ▪ Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Federal Decree Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations, as amended by Cabinet Decision 24 of 2022 ("AMLCFT Decision") and its amendments. ▪ Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations Guidelines for Financial Institutions of July 2023.
	Definitions and Acronyms	▪ Several frequently used terms and phrase are defined, and a list of acronyms used in the Best Practices is provided.
Conducting a Risk-Based Institutional Risk Assessment	Definition and Overview	▪ This section details that a risk assessment consists of identifying an institution's inherent ML/TF/PF risks based on the LFI's specific characteristics, business model, and activities; reviewing the design and operational effectiveness of an LFI's control framework to manage these risks; and determining the residual risk that remains after an LFI's controls are applied to its inherent risk. ▪ A broad example is provided of what risk assessments may look like for smaller, less complex institutions versus larger, more complex institutions. ▪ This section also provides several examples of how LFIs can leverage the results of a risk assessment (e.g., developing an accurate risk appetite statement).

		▪ This section describes the granularity expected in a risk assessment, the relevant stakeholders in the risk assessment, and the frequency with which LFIs should conduct risk assessments.
	Principles and Best Practices for ML/TF/PF Institutional Risk Assessments	▪ This section outlines the three steps of a risk assessment: Measuring Inherent Risk; Assessing the Control Environment; Assessing Residual Risk. ▪ General best practices are discussed, such as data quality and documentation. ▪ There is extensive discussion and examples of an LFI assessing the inherent risk related to its customers, products, services, delivery channels, and geographies. A stand-alone text box and graphic provide aids for LFIs in conceptualizing inherent risk measurement. ▪ There is discussion of assessing control effectiveness as it relates to an LFI's five-pillar AML program, including what should be included in the program and what supervisors may look for in an adequate program. ▪ Finally, the section provides guidance on the approach for assessing residual risk and a graphic to aid LFIs in quantitatively measuring residual risk.
Application of an RBA	Application of an RBA	▪ This section notes that once a risk assessment is complete, the board of directors/senior management should revisit the LFI's risk appetite statement to ensure it adequately reflects an institution's ML/TF/PF risk as well as if the LFI needs to develop or update AML/CFT/CPF controls as a result of the assessment. ▪ Several examples of how controls and measures could be updated are provided. ▪ This section also encourages an LFI to develop a detailed action plan for the implementation or update of AML/CFT/CPF controls and that the MLRO should own the plan.

Guidance for Licensed Financial Institutions on Correspondent Banking and Expectations for Managing Correspondent Banking Relationships

Effective from 7/11/2025 **Status:** In-Force

1. Introduction

Correspondent banking relationships are essential to the global payment system and international economy, helping financial institutions facilitate cross-border transactions and serve their customers' payment needs. Correspondent banking involves financial institutions providing services on behalf of other financial institutions, usually in different countries. To this end, correspondent banking is fundamental to international trade and commerce, particularly for emerging markets and developing economies.

Depending on the services provided in a correspondent banking relationship, the types of transactions conducted through a correspondent account, and the adequacy of a financial institution's financial crimes compliance ("FCC") compliance program, the level of risk posed by a correspondent banking relationship varies. In addition, because regulatory and supervisory regimes governing the operation of foreign financial institutions differ greatly, not all foreign financial institutions engaging in correspondent banking relationships are subject to the same anti-money laundering, counter the financing of terrorism, and countering the financing of proliferation ("AML/CFT/CPF") requirements as licensed financial institutions ("LFIs") in the United Arab Emirates ("UAE").

In the UAE, correspondent banking relationships are subject to AML/CFT/CPF measures, and LFIs are required to identify and manage the money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") risks

associated with these business relationships. To this end, this Guidance has been developed to assist LFIs with identifying and understanding the different risks in correspondent banking relationships. LFIs that offer correspondent banking services should therefore use this Guidance to design and appropriately tailor their policies, procedures, and processes to manage the specific risks associated with their correspondent banking relationships and to identify and report suspicious activities.

1.1. Purpose of the Guidance

Article 44.11 of the Cabinet Decision No. ("10") of 2019 Concerning the Implementing Regulation of Decree Law No. ("20") of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to assist in the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") LFIs of their statutory obligations under the legal and regulatory framework in force in the UAE, focusing notably on the operationalization of the statutory obligations. It should be read in conjunction with the CBUAE's Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations ("issued by Notice No. 74/2019 dated 19/06/2019") and Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions ("issued by Notice 79/2019 dated 27/06/2019") and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the expectations of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), international best practices, and other relevant international bodies.[2,3] These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs and registered hawala providers ("RHPs") should perform their own assessments of the manner in which they should meet their statutory obligations consistent with their risk exposure.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from coming into effect. The CBUAE will review and amend this guidance, as appropriate, to reflect emerging and evolving risks.

[1] Available at https://www.centralbank.ae/en/cbuae-amlcft.
[2] For example, please see https://db.wolfsberg-group.org/assets/d39a5072-7fb6-4e31-9a87-9e54021ce71f/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf.
[3] For example, please see https://www.bis.org/bcbs/publ/d405.pdf.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers; and

- Insurance companies, agencies, and brokers;

- Other covered financial institutions not specified above, or any other entities that are licensed or registered by the CBUAE and are engaged in financial activities that fall under AML/CFT/CPF regulations.

This Guidance applies to LFIs operating within the UAE and globally, including those acting as intermediaries in correspondent banking chains. For LFIs with operations outside the UAE, this guidance applies to their UAE-based activities and should inform group-wide standards, while adhering to applicable regulations in the local jurisdiction.

The term "Licensed Financial Institution (LFI)" covers all entities listed in this section (i.e., Section 1.2. – Applicability).

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");

- Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;

- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments; and

- CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

LFIs must understand that non-compliance with these laws can result in severe penalties, including fines and loss of license.

This Guidance also considers international standards and guidelines related to correspondent banking, including from the FATF Recommendations, the Basel Committee on Banking Supervision, and the Wolfsberg Group.

1.4. Acronyms and Definitions

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CPF	Countering proliferation financing
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ISO	International Organization for Standardization
LFI	Licensed financial institution
ML	Money laundering
MVTS	Money or Value Transfer Services (MVTS)
NBFI	Non-bank financial institution
PEP	Politically exposed person

RMA	Relationship Management Application
RHP	Registered hawala provider
SAR	Suspicious activity report
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council

Correspondent institution: A financial institution that provides financial services ("the correspondent institution") to another financial institution ("the respondent institution"). A correspondent institution can conduct business transactions, accept deposits, and gather documents on behalf of the respondent institution.

Correspondent banking: Correspondent banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, either domestically or internationally, for the execution of third-party payments and trade finance, and processing of paper clearing needs in a particular currency. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currency), international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

Derisking: The termination or restriction of business relationships, including correspondent banking relationships, by financial institutions to avoid risk, rather than manage it. Correspondent banking is an activity that has been negatively impacted by de-risking in certain regions and sectors.

Nested (or "downstream") activity: Activity where a financial institution's correspondent relationship is used by one or more indirect respondent institutions (i.e., nested banks) through their relationships with the financial institution's direct respondent institution to conduct transactions or obtain access to other financial services.

Non-resident accountholders: Customers primarily resident in a different jurisdiction from where financial services are being provided.

Payable-through (or "pass-through") accounts: Correspondent accounts that can be accessed directly by third parties to transact business on their own behalf.

Proprietary: Activity where a respondent institution is using the correspondent account to conduct

2. Understanding Correspondent Banking

As a global financial centre, the UAE relies on international correspondent banking networks to provide customers with access to cross-border products and services in different jurisdictions. To this end, correspondent banking supports international trade and business, increases financial inclusion, and furthers the UAE's financial connectivity with the international economy. While correspondent banking offers significant benefits, it may also pose significant risks, including higher exposure to financial crimes risks and the imposition of regulatory penalties, and require LFIs to implement robust risk management strategies to address these challenges.

Correspondent relationships involve the provision of financial services by one LFI, the "correspondent institution," to another, the "respondent institution" through a bilateral agreement between the two financial institutions. In its capacity as a correspondent institution, a bank or other LFI, may provide respondent institutions with a wide variety of services, including cash management, cross-border wire transfers, check clearing, loans, letters of credit, and foreign exchange services. It is important to note, although the ML/TF/PF risks may be lower, LFIs should still conduct due diligence on their correspondent and their parent institutions, following a risk-based approach. In the context of this guidance however, correspondent banking mostly refers to ongoing, contractual relationships where a correspondent institution provides a range of financial services to a respondent institution. Correspondent banking is especially relevant when an LFI or their customers lack a direct banking or other business relationship

with the other transacting party, for example, where the payment beneficiary does not hold an account at the originator's financial institution or when the transaction must be denominated in a particular currency.

The Wolfsberg Group establishes that "correspondent banking is the provision of a current or other liability account, and related services, to another financial institution, including affiliates, used for the execution of third-party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency."[4, 5]

Correspondent banking does not include one-off transactions or the exchange of the SWIFT Relationship Management Application keys ("RMA") as discussed in Section 6. *SWIFT and Non-Customer RMA Relationships*. Correspondent banking is defined by its ongoing, repetitive nature, and in this capacity, correspondent banking relationships can be understood as taking three main forms:

- **Traditional correspondent banking**: In traditional correspondent banking relationships, the correspondent institution enters into an agreement with a respondent institution for the respondent institution to execute payments on behalf of its customers (third-party transactions) or on its own behalf (proprietary transactions). The respondent institution's customers in traditional correspondent banking relationships do not have direct access to the respondent institution's correspondent banking account.

  Figure 1: Traditional Correspondent Banking: Proprietary Transactions

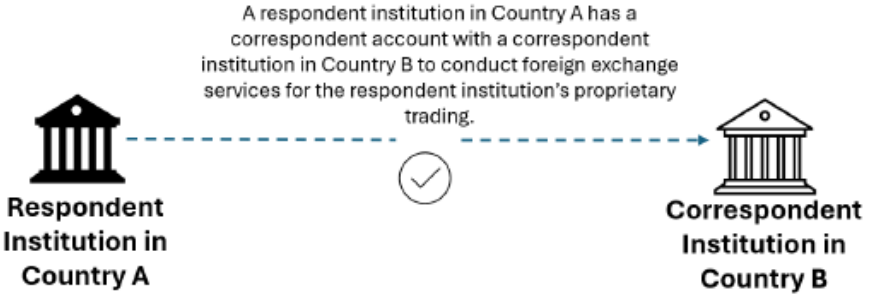
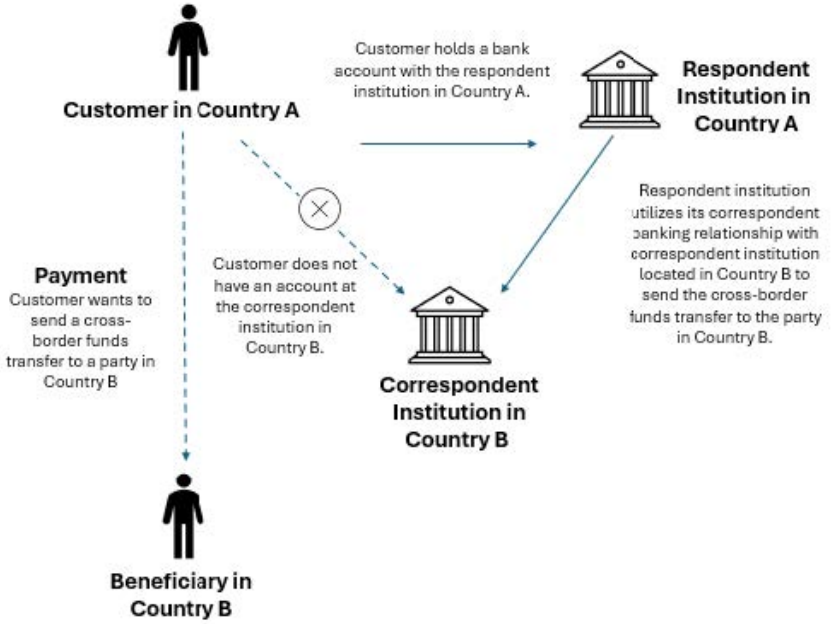


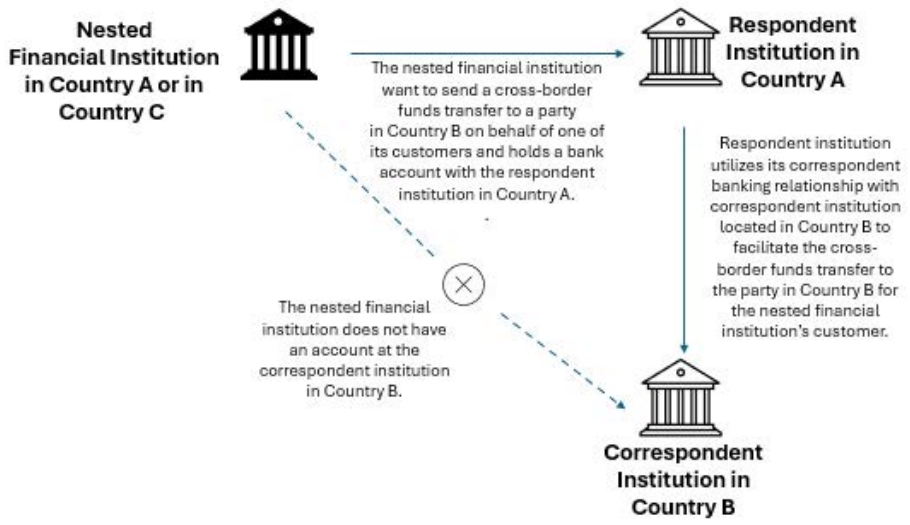
  Figure 2: Traditional Correspondent Banking: Third-party Transactions



- **Nested correspondent banking**: In this scenario, a correspondent institution's account with the respondent institution is used by one or more indirect respondent institutions or "nested" institutions. Specifically, the "nested" institutions obtain access to financial services through their relationship with the respondent institution, which they can then use for their own customers. Nested institutions do not have a direct relationship with the correspondent institution. Nested relationships are commonly found where one or more of

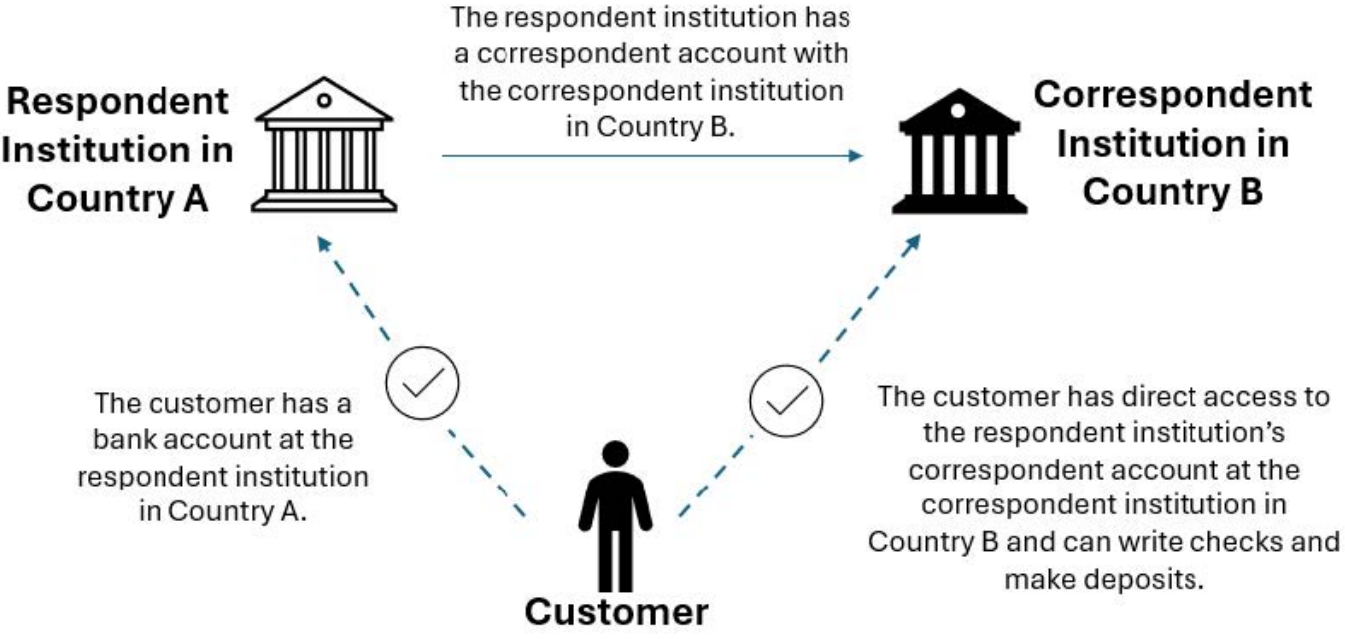
the transacting parties holds an account at a smaller institution that must pass through larger intermediary institutions in order to transact with the ultimate beneficiary.

Figure 3: Nested Correspondent Banking



- Payable-through or pass-through accounts: Payable-through accounts are similar to nested correspondent banking relationships, but in this case, the respondent institution allows its customers to directly access the correspondent banking account. In so doing, the respondent institution's customers can conduct their own transactions through the correspondent banking account.

Figure 4: Payable-through Account



LFIs should note that nested correspondent banking relationships and payable-through accounts pose heightened ML/TF/PF risks due to reduced transparency of the underlying transactions. LFIs allowing such arrangements should implement enhanced due diligence ("EDD") measures.

In light of the risks posed by correspondent banking relationships, banks may be tempted to derisk by severing relationships notably with higher-risk respondent institutions, but doing so can undermine their global reach and financial inclusion in emerging markets. LFIs should be aware of the potential negative impacts of de-risking. While managing risks is crucial, wholesale termination of correspondent banking relationships could lead to financial exclusion and push transactions into less-regulated channels.

[4] Wolfsberg Group, *Wolfsberg Financial Crime Principles for Correspondent Banking*, 2022, https://db.wolfsberg-group.org/assets/d39a50727fb6-4e31-9a87-9e54021ce71f/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf.

[5] For the purposes of this Guidance, and according to FATF, correspondent banking relationships also include Money or Value Transfer Services ("MVTS") providers when they act as intermediaries for other providers, or where they are accessing banking or similar services through the account of another MVTS customer of the bank.

3. Cross-Border Payments

Particularly relevant in the context of correspondent banking, LFIs often turn to their correspondent banking relationships to conduct cross-border payments for their customers or the financial institution's own crossborder activities. When considering the risks and requirements of correspondent banking relationships, it is important to understand how cross-border payments are executed, and an LFI's obligation to collect and monitor information associated with cross-border payments. LFIs must ensure compliance with all applicable AML/CFT/CPF regulations while conducting cross-border payments, emphasizing the importance of thorough monitoring and documentation to mitigate risks of financial crime.

For the purposes of this Guidance, cross-border payments are financial transactions where the originator and remitter/beneficiary are based in separate countries. Cross-border payments cover both wholesale and retail payments, including cross-border remittances.

Background on SWIFT Payment Messages

The vast majority of cross-border interbank transactions are made using the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") messaging system. SWIFT maintains a proprietary secure network with standardized data fields and protocols that allows LFIs and other participants to send secure payment instructions and other relevant transaction information to counterparties around the world. Importantly, the SWIFT network is a messaging infrastructure, and not a settlement system. The actual movement of funds is completed at the account level, through correspondent banking relationships between the transacting parties.

SWIFT messages are called "MT" messages (stands for "message text") and the first letter of the MT xxx number reflects the type of a message used. For example, for customer-initiated payments, financial institutions use MT 1xx and for intrabank settlements – MT 2xx. SWIFT has developed and regularly updates the formatting standards used for each type of message that dictates the mandatory versus optional fields, the length of fields, and information that should be reflected in each.

Historically, due to less stringent standards in the format of certain SWIFT payment messages, intermediary financial institutions did not always have access to minimum originator and beneficiary information. Under this legacy messaging system for cross-border payments, ordering institutions would send two types of messages:

- **SWIFT MT 103**: An ordering institution would use this message type when initiating a transaction on behalf of an ordering customer, by sending this message directly to the financial institution of the beneficiary customer. MT 103 is a longer message type (when compared to MT 202 discussed below) and would require an originating financial institution to include numerous data points about the transfer and remitter/beneficiary.
- **SWIFT MT 202:** SWIFT standards require financial institutions to use this type of MT message when initiating transfers for its own account. A MT 202 message contains very few mandatory fields, only identifies financial institutions engaged in the funds transfer, and does not reference the originator or the beneficiary.

In the mid-2000s, various regulatory authorities and industry groups noted that the use of MT 103 and MT 202 messages allowed for non-transparent funds transfers or even transfers where certain information was intentionally manipulated or withheld from correspondent banks. To address the financial transparency concerns associated with the use of the MT 202 message type and underlying non-bank payments (i.e., payments initiated by bank's customers), in November 2009, SWIFT adopted a new message format, the MT 202 COV.

The MT 202 COV contains mandatory fields for originator and beneficiary information. Financial institutions originating cross-border funds transfers on behalf of their customers are now required to use the MT 202 COV for any financial institution-to-financial institution payment for which there is an associated MT 103, thus providing intermediary financial institution with the information they need to perform sanctions screening and suspicious activity monitoring. Financial institutions may continue to rely on MT 202, a shorter message format, when the associated funds transfer is truly a transfer between two financial institutions acting on their own behalf.

Of note, the use of MT messages for cross-border payments will end in November 2025. After this date, SWIFT will no longer support most MT messages, and the MX standards (ISO 20022) will become the new standard for payment messaging. With ISO 20022 migration, the equivalent MX message formats are PACS008 for customer credit transfer and PACS009 for financial institution credit transfer. LFIs should consider both MT and MX standards for comprehensive coverage of SWIFT messaging. Please, refer to Annex 3 Transition from SWIFT to the ISO 20022 Payment Standard for further details.

3.1. Funds Transfer Requirements and the Role of Financial Institutions Processing Cross-Border Funds Transfers

LFIs have specific requirements when processing cross-border fund transfers. In order to manage the risks associated with cross-border payments, it is essential that all LFIs in the transaction chain—including intermediary financial institutions that may lack a direct customer relationship with the ultimate originator or beneficiary—be able to screen and monitor the identities and locations of all transacting parties. Intermediary financial institutions play a critical role in ensuring the integrity of cross-border transfers by screening, monitoring and passing on all relevant information, even if they lack a direct relationship with the originator or beneficiary.

Under Articles 27-29 of the AML-CFT Decision, qualifying cross-border wire transfers equal to or exceeding AED 3,500 (or equivalent in any other currency) should always contain the following:

- The name of the originator;
- The originator's account or unique transaction number. In the absence of an account, the transfer must include a unique transaction reference number which allows the process to be tracked;
- The originator's identity number or travel document, date and place of birth, and address;
- The name of the beneficiary; and
- The beneficiary's account or unique transaction number. In the absence of the account, the transfer must include a unique transaction reference number which allows the process to be tracked.

As per Chapter 16 of the CBUAE Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business, exchange houses are subject to stricter due diligence requirements, and should screen all transfers, inwards or outward.

The quality of information provided in payment messages is critical. LFIs must ensure that all required data is accurate and complete to facilitate effective monitoring and compliance with AML/CFT obligations.

Regarding the role of financial institutions processing cross-border wire transfers, originating financial institutions are responsible for using the right format for payment messages. To this end, originating financial institutions should require that information on an originator and beneficiary accompanies wire transfers messages. Other parties in the payment chain—such as an intermediary financial institution that may lack a direct customer relationship with the ultimate originator or beneficiary—are required to monitor the payments they process based on this information. In particular, the quality of information provided in payment messages helps facilitate and should be used as a basis for an LFI's ongoing monitoring program.

Article 28 of the AML-CFT Decision also requires intermediary financial institutions to take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Intermediary financial institutions are required to actively monitor all cross-border wire transfers for compliance with information requirements and must implement robust procedures to identify and address any deficiencies in originator or beneficiary information. Intermediary institutions must also have risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer; and the appropriate follow-up action. These procedures should consider factors such as the completeness and accuracy of originator/beneficiary information and the presence of sanctions alerts.

As it relates to correspondent banking, a correspondent institution as an intermediary financial institution in the payment chain should:

- Monitor the payment messages transmitted by the respondent institution for the purpose of detecting those which lack required originator and/or beneficiary information, including meaningless fields.

- Verify the reliability of the respondent institution's controls, for instance via sample testing (e.g., take a closer look at a few transactions to identify cases where they do not comply with the wire transfer information requirements). Sample testing may also help the correspondent institution to adjust the level and type of monitoring, including the timing of ex-post reviews.

The respondent institution, acting as the ordering financial institution, remains responsible for performing CDD/KYC on the originator and must verify originator information for accuracy, obtain relevant information on the beneficiary in a manner that is consistent with straight-through processing, and maintain this information in accordance and Article 27 of the AML-CFT Decision. Furthermore, in cases where there is higher risk associated, the respondent institution is required to undertake EDD measures warranting for documented understanding of the purpose of transaction and the involved parties i.e., originator, beneficiary and any other party affiliated with the transaction.

To address risks related to a lack of transparency in the international payments system, LFIs should implement policies, procedures, processes, and technology to apply increased transparency for crossborder cover payments and adhere to the Message Standards, as noted in interagency guidance by the Wolfsberg Group and Clearing House (a banking association and payments company owned by the largest commercial banks). The standards stipulate that:[6]

- LFIs should not leave out, delete, or change information in payment messages or orders for the purpose of avoiding having that information be detected by any other financial institution in the payment chain;

- LFIs should not use any payment message for the purpose of avoiding having that information be detected by any other financial institution in the payment chain; and

- Subject to all applicable laws, LFIs should cooperate with other financial institutions in the payment process when requested to provide information about the parties involved in a payment; and

- LFIs should strongly encourage their foreign correspondent banking customers to observe these principles.

- LFIs should leverage technology solutions to enhance the monitoring of cross-border payments, ensuring that systems are in place to automatically detect transactions that lack required information, include inaccurate originator and beneficiary information, or exhibit suspicious patterns.

Failure to comply with the established funds transfer requirements may result in enforcement actions, including fines and restrictions on operations, increased scrutiny from regulators, and potential reputational damage for LFIs, thereby underscoring the importance of adherence to these guidelines.

[6] Wolfsberg Group, Clearing House, Statement on Payment Standards, 2007, please see https://db.wolfsberg-group.org/assets/973cf236-7292430b-ae56-100e434fa983/13.%20Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf

4. Policy and Procedures

It is essential for LFIs to develop a robust financial crime framework to identify, prevent, and effectively manage risk, rather than merely avoiding risk through derisking. LFI's are required to develop risk-based internal policies and procedures for correspondent banking relationships, that should be approved by senior management or the board. The policies and procedures should include:

- **Implementation across the organization:** LFIs should implement robust monitoring mechanisms to ensure the effective and consistent implementation of the policies and procedures across the organization, including branches, subsidiaries, and other entities in which LFIs hold a majority interest.

- **Communication:** LFIs should clearly communicate the policy and procedures to all relevant employees and external or outsourced service providers; by providing regular training to all relevant employees or external service providers to ensure they understand and can effectively implement the policies and procedures.

- **Review and Update:** LFIs should review and update the policies and procedures in a timely manner in response to events or emerging risks and ensure that such updates are communicated to employees and external or outsource service providers on a timely basis to ensure they are informed and act accordingly.

- **Formal Review Process:** LFIs should implement a formal review process at least annually of the policies and procedures to assess the effectiveness of said policies and procedures, identify gaps or weaknesses, and make necessary updates, with necessary changes being subject to approval at appropriate levels where changes are material.

- **Exceptions and Deviations:** LFIs should identify and document any exceptions or deviations from the policies and procedures related to the LFI, including a remedial action plan; these should be approved by senior management.

- **Local and International Regulatory Requirements:** LFIs should develop internal policies and procedures for correspondent banking relationships that align with local requirements as well as international best practices, including FATF recommendations, to ensure compliance with applicable local and international regulatory requirements.

The policy and procedures should be risk-based and regularly reviewed to ensure they align with evolving regulatory requirements, emerging risks, and mitigation measures. This approach will strengthen and maintain dynamic financial crime prevention framework that meets international standards, regulatory expectations, and industry best practices.

5. Correspondent Banking Risk Factors

Different types of correspondent banking relationships present varying levels of ML/TF/PF risk. The following section examines common risk factors associated with correspondent banking relationships by reviewing aspects of a respondent institution's risk profile, including transactions, geography, ownership and management structure, products and services, and customers that contribute to ML/TF/PF risk. LFIs should conduct a comprehensive risk assessment of their correspondent banking relationships, considering all relevant risk factors and determine whether their correspondent banking relationships should be subject to additional EDD measures. Additional measures are necessary because cross-border correspondent banking relationships are inherently higher risk than domestic correspondent relationships. Simplified due diligence measures are not suitable in the context of cross-border correspondent banking. An LFI may also decide to suspend transaction activity or exit a correspondent

banking relationship if risks cannot be sufficiently mitigated. LFIs should incorporate this assessment into their AML/CFT/CPF program and update their policies, procedures, and processes with the aim to manage associated illicit financing risks. To ensure effective risk management, LFIs should establish clear criteria for implementing EDD measures based on specific risk factors, such as transaction types and volumes, geographic location, ownership structures, and the nature of the respondent institution's customer base.

5.1. Respondent Institution's Third-Party Transaction Risk

Correspondent banking relationships involving the execution of transactions and the provision of other financial services for the respondent institution's customers (otherwise referred to as "third-party transactions") introduce specific ML/TF risks. This third-party risk is present across traditional correspondent banking relationships, nested correspondent banking relationships, and payable-through or pass-through accounts.

For third-party transactions, the correspondent institution is effectively acting as the respondent's "agent," executing payments or other transactions for the respondent's customers that can be individuals, legal entities, or other financial institutions. Without appropriate controls, a correspondent institution may allow a respondent institution's customers to access the international financial system without first obtaining—or ensuring that the respondent institution has obtained—an adequate understanding of the customer's identity and risk profile and is implementing adequate controls to manage such risk.

In traditional correspondent banking relationships, for example, the correspondent institution acts as an intermediary for underlying customers of the respondent institution, often with very limited information about those ultimate customers. In this case, the correspondent institution has no direct relationship with the underlying parties to a transaction and is not able to verify their identities and purpose of the transaction, relying instead on the due diligence performed by the respondent institution.

Notably, use of third parties is one method that money launderers and terrorist financiers employ to launder the proceeds of crime. By relying on other parties to conduct transactions, illicit actors can distance themselves from the transactions that can be directly linked to the suspected ML/TF offence. Money launderers and terrorist financiers may turn to nested correspondent banking relationships and payable-through or pass-through accounts. With respect to the risks presented by third-party transactions, LFIs should implement EDD, including obtaining detailed information about the respondent institution's customers, their risk profiles, and the controls in place to manage risks.

5.1.1. Nested Relationships

As a type of third-party relationship, a correspondent institution that establishes a correspondent relationship with a foreign financial institution (respondent institution) may not know whether the respondent institution is permitting other financial institutions to operate through the respondent institution's correspondent account or relationship. Such "downstream" or "nested" relationships place additional layers of intermediation between the correspondent institution and the ultimate customer, further increasing the risk that the correspondent is allowing third parties to access the international financial system without an adequate understanding of the customer or the AML/CFT/CPF controls needed to manage such customer risk. The risk in this activity is that the correspondent institution is at least one step further removed from the institution that has conducted due diligence on the transacting party, thereby limiting the correspondent institution's visibility into the parties involved in the transaction who could be abusing the lack of transparency afforded to them to conduct illicit activity.

To manage the risks posed by nested relationships, a correspondent institution should require that the respondent institution disclose the existence of nested relationships as part of account opening and ongoing account activity reviews. Correspondent institutions should conduct reviews of nested relationships at least annually, assessing the risk associated with nested financial institutions and ensuring that adequate AML/CFT/CPF controls are in place to mitigate risks. Correspondent institutions should take reasonable steps to understand the types of financial institutions to whom a respondent institution offers downstream services and assess the strength and effectiveness of the respondent institution's AML/CFT/CPF controls to mitigate these risks. LFIs should also ensure that payment

instructions are formatted in a manner that is transparent to enable easy identification of involved parties for the purpose of effective monitoring and screening. Additionally, correspondent institutions should consider the degree to which the respondent institution examines the AML/CFT/CPF controls of those financial institutions. For example, the correspondent institution should ensure that the respondent institution allowing nested relationships conducts correspondent banking due diligence on the nested institutions as well as its parents, subsidiaries, and affiliates. These steps may also include consideration of institution types, scale of services, and geographic location of downstream financial institutions and their customers. To this end, the correspondent institution may consider the following factors, among others, when assessing the risk of a respondent institutions offering downstream financial services:

- The number, type, and jurisdictions of the nested financial institutions a respondent institution serves;
- If the nested financial institutions are located outside of the UAE, the correspondent institution should assess if those countries are (a) high risk for ML/TF and (b) have an adequate AML/CFT/CPF supervisory regime;
- Types of services the respondent institution offers to nested financial institutions (if they are proprietary only, the ML/TF risks are reduced than if the nested financial institutions engage in third-party transactions); and
- The length of the relationship between the correspondent and respondent institution (i.e., a well-established relationship enables the correspondent institution to have a better understanding of the respondent institution's expected activity and ML/TF risk associated with the relationship than a new relationship).

Understanding the risks associated with nested relationships, downstream correspondent banking relationships can be a generally legitimate part of correspondent banking. Nested relationships may be a way for global financial institutions, for instance, to help smaller financial institutions within the respondent institution's region obtain access to the international financial system or to facilitate transactions where no direct relationship exists between financial institutions.

Best Practices: Nested Relationships

Following a risk-based approach, a correspondent institution may apply the following enhanced measures:

- A correspondent institution should request a respondent institution's list of nested financial institutions receiving downstream services and perform internal watchlist, negative news, politically exposed person ("PEP"), and sanctions screening on these institutions.
- A correspondent institution, on a risk-sensitive basis, may request further information from the respondent on their customer due diligence and AML/CFT/CPF controls of the underlying nested financial institution(s) in order to inform their own assessment of the nested financial institution(s).
- A correspondent institution can communicate to the respondent institution that nested financial institutions' AML/CFT/CPF programs should be updated periodically and that information on their AML/CFT/CPF programs should be provided to the correspondent institution upon request.
- A correspondent institution may wish to collect a statement from the respondent institution affirming that payment instructions for transactions on the correspondent account will be formatted to facilitate monitoring and screening of all involved parties to a transaction.

5.1.2. Payable-through Accounts

A payable-through account involves a respondent institution opening a correspondent account with a correspondent institution and then providing its customers with the means of directly transacting on the respondent's account with the correspondent institution. This can take the form, for instance, of a respondent institution's customers being able to write cheques and have access to other financial services on the correspondent account. In this scenario, ML/TF/PF risks are heightened as the respondent institution lacks direct oversight of the transactions being conducted on the account, which can pose even greater risk to the correspondent institution who lacks access to information about the third parties accessing the account. A third party's direct access to the correspondent account differs from downstream or nested relationships where the respondent institution is routing the nested financial institution's transactions to the correspondent institution.

Similar to nested relationships though, for correspondent institutions that allow payable-through accounts, the respondent institution should seek to demonstrate that it conducts adequate Customer Due Diligence/ Know Your Customer ("CDD/KYC") on its customers and that it is able to provide such information upon request to the correspondent institution. Correspondent institutions should perform additional due diligence and monitoring for respondent institutions in higher-risk jurisdictions commensurate to the respondent institution's risk. As a best practice, the correspondent institution should collect information from the respondent institution about the identities of any persons with authorization to direct transactions through a payable-through account, and the sources and the ultimate beneficial owners ("UBOs") of funds in the payable-through account. Given the heightened risks, correspondent institutions should also consider implementing additional controls for payable-through accounts, such as stricter transaction limits, real-time transaction monitoring, and enhanced scrutiny of the purpose and nature of transactions.

5.2. Respondent Institution's Geographic Risk

Also impacting a respondent institution's ML/TF/PF risk is a respondent institution's exposure to jurisdictions with elevated ML/TF/PF risk. For jurisdictions that have unsatisfactory AML/CFT/CPF laws and regulations or weak AML/CFT/CPF regulatory and supervisory regimes, for instance, the ML/TF/PF risk of providing correspondent banking services to financial institutions located or operating through these jurisdictions is heightened. This includes if a respondent institution has exposure to a country that has been found to be deficient in its application of global FCC standards, such as by the FATF.

In addition to assessing the ML/TF/PF risks where the respondent institution is based, correspondent institutions should also assess the risks associated with the respondent institution's presence or operations in countries with the following risk indicators. These risk indicators should be considered for jurisdictions where a respondent institution's ultimate parent is headquartered, and where the respondent institution conducts business, including the location of a respondent institution's branches and subsidiaries:

- Jurisdictions with weak regulatory AML/CFT/CPF frameworks, as determined by the LFI or as notified by local regulatory or supervisory authorities;
- Jurisdictions subject to a call for action or under increased monitoring by FATF;
- Jurisdictions subject to the UNSC or UAE sanctions, or other relevant international sanctions;
- Jurisdictions where there are ongoing conflicts;
- Jurisdictions that are known to produce or transit drugs;
- Jurisdictions that have relatively higher levels of corruption or organized crime, or are known as a financial secrecy or tax haven; and
- Jurisdictions that are known to provide transit corridors to countries rated as high-risk by the UAE National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations

Committee (NAMLCFTC).

In order to understand a particular jurisdiction's ML/TF/PF risk, a correspondent institution should verify whether the jurisdiction of a respondent institution is considered as jurisdictions under increased monitoring or jurisdiction subject to a call for actions by FATF. The correspondent institution may also review other sources of information, including AML/CFT/CPF laws and regulations of the respondent institution's home country, country assessment reports and guidance from regulatory agencies and applicable international bodies, including the World Bank or International Monetary Fund. This will help a correspondent institution to evaluate the degree of risk presented by a specific jurisdiction. The assessment of a respondent institution's exposure to a jurisdiction with heightened ML/TF/PF risk should be considered as part of a correspondent institution's risk assessment of each correspondent banking relationship. LFIs should also implement continuous monitoring of geographic risks associated with correspondent banking relationships, adapting their risk assessments in response to changes in the regulatory environment and emerging risks in high-risk jurisdictions.

5.3. Respondent Institution's Ownership and Management Structures

Certain features of a respondent institution's ownership and management structure may present increased ML/TF/PF risks, making it more conducive for illicit actors to own, control, hold a significant or controlling interest, or hold a management function in a respondent institution. Correspondent institutions should prioritize transparency in ownership and executive management structures, requiring thorough documentation of beneficial ownership and executive management structures to mitigate potential ML/TF risks. The following features should be considered along with other risk factors when deciding to onboard and continue a correspondent banking relationship:

- **Respondent institution's legal form (such as whether the respondent institution is state owned, publicly held, or privately owned)**. Certain factors associated with whether an institution is state owned, publicly held, or privately-owned impact the risk of the correspondent institution's relationship with the respondent institution. Generally speaking, more transparency in a respondent institution's ownership structure is associated with less ML/TF/PF risk, while opaque ownership structures present a greater degree of ML/TF/PF risk. Risks are elevated, for instance, if the respondent institution is privately owned by UBOs and senior management located in high-risk jurisdictions. Alternatively, risks are reduced if an institution is publicly owned with shares traded on a recognized exchange in a jurisdiction with a satisfactory AML/CFT/CPF regulatory regime. However, different exchanges will have different requirements for reporting, and LFIs should ensure that the disclosure and transparency requirements of a regulated stock exchange are at least equivalent to those of the UAE.

- **The location and reputation of shareholders and beneficial owners**. Shareholders and UBOs pose different levels of ML/TF/PF risk. Because shareholders and UBOs could have direct influence over how a respondent institution implements its AML/CFT/CPF program, it is important for a correspondent institution to identify these individuals and obtain relevant information about them, further discussed below, including their background, source of funds, and source of wealth, when the institution is not state-owned or publicly listed.

- **The presence of any PEP(s) in the senior management or ownership structure, particularly in circumstances where the PEP(s) have day-to-day control over the respondent**. Politically exposed persons ("PEPs") are at higher risk of involvement in certain proceeds-generating offenses (e.g., corruption, misuse or theft of public funds, and bribery), and the presence of a PEP in a respondent institution's senior management or ownership structure increases a respondent institution's financial crime risk. PEPs are at greater risk of misdirecting a respondent institution's funds—using their power or influence in a respondent institution to directly enrich themselves, their family members, and their associates, which should be considered as part of a correspondent institution's risk assessment of a correspondent banking relationship.

To assess the risks associated with a respondent institution's ownership and management structure, correspondent institutions should identify and perform negative news, PEP, and sanctions screening on the respondent institution's shareholders, UBOs, senior management, and other officers, as relevant, such as the Chief Executive Officer and the Chief Financial Officer. In certain circumstances, such as if the shareholders and UBOs are associated with financial crime-related negative news, the correspondent institution should evaluate the UBOs' and shareholders' source of wealth and source of funds. The correspondent institution also should gather sufficient information about the ownership and control structure of the respondent institution that also includes verifying that the respondent institution is not a shell bank.

5.4. Respondent Institution's Products and Services

The nature of the products and services offered to a respondent institution, or that a respondent institution offers to its customers, can impact the risk associated with the correspondent banking relationship. LFIs should consider the following factors when evaluating the risks of products and services involving a respondent institution:

- Potential for intermediation: The extent to which the correspondent institution or respondent institution is offering services that carry intermediated risk, such as if the respondent institution will be allowing nested relationships or providing payable-through accounts. In this case, the institution would have limited visibility into the originator or beneficiary of a transaction (payment instructions) that it is processing, increasing the ML/TF/PF risk of the products and services provided.

- Potential for anonymity: Whether the correspondent institution or respondent institution will be offering services to the respondent institution that facilitate anonymity, such as allowing nested relationships, enabling an illicit actor to operate with limited transparency when conducting transactions.

- Cross-border funds flows: Whether the correspondent institution or respondent institution offers services that typically or characteristically involve the cross-border movement of funds (such as cross-border remittances, cross-border bulk cash delivery, international cash letters, trade finance, etc.), as illicit actors often exploit cross-border funds flows to disguise the origins of illicit funds, making them appear legitimate through complex layering and integration schemes involving multiple jurisdictions.

- Settlement times and terms: Whether the correspondent institution or respondent institution offers services that provide for near instantaneous and irrevocable settlement, making financial crime harder to detect and reverse.

To manage these risks, a correspondent institution should collect the purpose of the respondent institution's account and relationship with the correspondent institution. As part of establishing a correspondent banking relationship, a correspondent institution should also understand the anticipated activity for the products and services the respondent institution intends to use with the correspondent, assessing whether this anticipated activity is reasonable for the size and characteristics of the respondent institution's customer base. The correspondent institution should also conduct ongoing transaction monitoring to assess any anomalies between the actual use of the correspondent institution's products and services with the anticipated activity established during onboarding.

5.5. Respondent Institution's Customer Base

A respondent institution's customer base impacts its level of ML/TF/PF risk, and subsequently, the risk it contributes to a correspondent banking relationship. Specifically, a respondent institution that derives a significant portion of its business income from high-risk customers poses greater ML/TF/PF risk to a correspondent institution. Overall, high-risk customer types have elevated ML/TF/PF risk due to the nature of their business and potentially weak AML/CFT/CPF controls (e.g., dealers in precious metals or stones, non-profit organizations, cash-intensive businesses, PEPs, Virtual Assets Services Providers, and FinTech Companies) and due to the jurisdictions where they are located or operate (e.g., jurisdictions that are known as financial secrecy or tax havens).

For example, non-resident accountholders pose greater ML/TF/PF risk to a respondent institution obtaining identification information, understanding source of wealth and source of funds, and performing customer verification is typically more difficult for non-residents than local customers. For a respondent institution with a significant proportion of non-resident accountholders, a correspondent institution should understand why so many customers are non-residents in addition to whether or not the respondent institution's AML/CFT/CPF controls are sufficient to manage the risks of this customer type.

Examples of customer types that should be avoided by correspondent institutions are the following, although this list is not exhaustive and should be evaluated when considering an LFI's risk appetite:

- **Shell banks**: Shell banks have been found to facilitate ML/TF/PF due to their lack of a physical presence and their association with jurisdictions that have weak AML/CFT/CPF supervisory regimes. Correspondent institutions should ensure that they do not knowingly deal with financial institutions that engage shell banks. Under Article 25 of the AML-CFT Decision, LFIs should avoid entering into, or continuing, a correspondent banking relationship with shell banks.

- **Unlicensed and/or unregulated banks or NBFIs**: Unlicensed and/or unregulated banks or non- bank financial institutions ("NBFIs") lack AML/CFT/CPF regulatory oversight and a supervisor that monitors their ongoing compliance and AML/CFT/CPF program effectiveness. Maintaining accounts for a respondent institution that engages unlicensed and/or unregulated banks or NBFIs increases the risk of processing transactions for customers that lack appropriate CDD/KYC, and thus, elevating the chances of abusing the unlicensed and/or unregulated bank or NBFI for illicit purposes.

To manage the risks of a respondent institution's customer base, the correspondent institution should collect sufficient information to understand the major business activities that could explain and provide a business rationale for the respondent institution's high-risk customer types. In determining the risk and control effectiveness of a respondent institution, the correspondent institution should also consider all relevant risk factors, not limited to a respondent institution's customer base (such as by assessing a respondent institution's products and services, countries in which it operates, and target markets) in addition to a respondent institution's AML/CFT/CPF controls designed to mitigate these risks. As part of this evaluation, the correspondent institution should also take into consideration, the number of years the respondent institution has been offering correspondent banking services to its customers.

6. Risk Mitigation

As discussed, correspondent banking relationships are diverse in nature and pose varying levels of risk to an LFI. To mitigate risks associated with correspondent banking relationships, LFIs should design and implement controls to identify, assess, and manage the ML/TF/PF risks of each correspondent banking relationship and embed these assessments within their broader AML/CFT/CPF program. LFIs are also encouraged to explore and consider the adoption of new technologies, such as blockchain or distributed ledger technology, in their correspondent banking operations. These technologies have the potential to enhance transparency and strengthen AML/CFT/CPF controls.

The sections below discuss how LFIs can apply preventive measures associated with their correspondent banking relationships. The risk mitigation measures addressed in this Guidance are not a comprehensive discussion of all AML/CFT/CPF requirements imposed on LFIs. LFIs should therefore consult the UAE legal and regulatory framework currently in force. The controls discussed below should be integrated into each LFI's broader AML/CFT/CPF program and supported by appropriate governance, independent audit, and training. The level and nature of risk of a respondent institution's risk may also change over the course of its relationship with an LFI, and adjustments should be made in the LFI's AML/CFT/CPF controls to reflect these changes.

6.1. Enterprise-wide ML/TF/PF Risk Assessment and Correspondent Banking Risk Assessment

Under Article 4 of the AML-CFT Decision, LFIs are required to identify, assess, and understand the ML/TF/PF risks to which they are exposed in order to determine the nature and extent of AML/CFT/CPF resources necessary to mitigate and manage those risks. For this purpose, LFIs should also perform, document, and regularly update an enterprise-wide risk assessment that includes an assessment of risks related to correspondent banking. The LFIs' policies and procedures should indicate the appropriate frequency for conducting the enterprise-wide ML/TF/PF risk assessment and the circumstances and significant changes requiring an off-cycle risk assessment. LFIs should also ensure that their enterprise-wide ML/TF/PF risk assessments explicitly incorporate and integrate the risks associated with correspondent banking activities across all business units. Conducting a risk assessment is the first step in an LFI's effort to counter illicit finance, including risks stemming from offering correspondent banking services. Specifically, LFIs should evaluate the ML/TF/PF risks associated with respondent institutions. To form a clear understanding of their risk exposure, LFIs may opt to perform a standalone risk assessment of their correspondent banking line of business.

When performing the correspondent banking risk assessment, LFIs should identify and assess risks taking into account different categories of risk factors. The most common categories of risk factors are **customers, geographies, products and services, and delivery channels**. LFIs should assess their ML/TF/PF risk exposure taking into account different categories of risk factors, including customers, geographies, products and services and delivery channels as follows:

- **Customers:** To better understand customer risk, LFIs should assess their exposure to respondent institutions' customers engaged in potentially higher-risk activities, such as customers that operate in high-risk industries (e.g., customers operating in the extraction and management of oil, gas, and other natural resources; customers involved in nuclear power; gambling; production, sales, and distribution of marijuana, gambling; etc.). Customers with complex ownership structures may also pose heightened ML/TF/PF risks. Certain customer behaviour may also indicate higher levels of risk and thus require additional scrutiny, such as customers that handle customer money (such as lawyers, accountants, consultants, and real estate agents). Particularly important in the context of correspondent banking, the LFI should evaluate the ability of third parties to have access to a correspondent account, such as through nested relationships or payable-through accounts.

- **Geographies**: LFIs should also consider the ML/TF/PF risks associated with the countries where respondent institutions are located, where respondent institutions' ultimate parent are headquartered, and where respondent institutions conduct business, including the location of branches and subsidiaries. The adequacy of a respondent institution's AML/CFT/CPF regulatory and supervisory authority and that of the respondent institution's ultimate parent also impacts an LFI's geographic risk. Jurisdictions with weak or inadequate AML/CFT/CPF framework present higher risk.

- **Products and Services**: LFIs should consider their products and services and assess the inherent risk associated with offering such products in the context of correspondent banking. LFIs should take into account product transparency, complexity, potential for intermediation, settlement times and terms, usage of cash, and cross-border funds flows. Specifically, LFIs should evaluate products and services that enable cross-border transactions (such as cross-border bulk cash currency, cross-border funds transfers, international cash letters, trade finance, etc.) and the extent to which these products and services can be abused for illicit activity, such as by masking end-users and disguising payments.

- **Delivery Channels**: Overall, an LFI should assess products and services that are provided to respondent institutions through higher-risk delivery channels, specifically, those that create anonymity and can be used to obscure the source or destination of funds. The primary drivers of risk for delivery channels include whether a particular delivery channel involves non-face-to-face transaction initiation mechanisms, is operated by or through a third party, or offers rapid or near-instantaneous processing and settlement. If a respondent institution operates as a virtual bank, for instance, risks are greater that the institution does not truly understand the identity and activities of the customer. In addition, delivery channels operated by third parties are inherently higher risk because—as with transactions taking place through a non-face-to-face

channel—they make it more difficult for an institution to truly understand the identity and activities of the customer or collect meaningful and sufficient data for ongoing monitoring.

Risk assessments should provide a consolidated assessment of an LFI's ML/TF/PF risks across all business units, including those of branches, subsidiaries, parent entities, or other affiliates located outside the UAE. The identified risks should be consistently reported to senior management, and any internal control deficiencies noted during the risk assessment process should be appropriately tracked and remediated. LFIs should also ensure that their risk assessments are integrated into their overall risk management frameworks, including into an LFI's risk appetite. The risk appetite should set out the different types of parties and transactional activity the LFI prohibits from being processed through its correspondent accounts, which should be approved by the LFI's Board of Directors or senior management. Risk assessments and risk appetite statements should be an ongoing process and should be reviewed regularly to ensure that they remain relevant, effective, and up to date. Furthermore, the LFI should adopt mitigation strategies based on the correspondent banking risk assessment including enhanced due diligence measures, more frequent reviews, limitations etc.

6.2. Standard Customer Due Diligence

Under Article 5 of the AML-CFT Decision, LFIs should conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. An LFI's CDD program should cover, at a minimum:

- Customer identification and verification;
- Beneficial ownership identification and verification;
- Understanding the nature and purpose of the customer account and relationship for the purpose of establishing a risk profile; and
- Ongoing monitoring, including periodic and event-driven updating of customer and beneficial ownership information and the customer risk profile throughout the business relationship.

CDD, and where necessary EDD, are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers.

Accordingly, as a first step to onboarding a potential respondent institution, an LFI is required to identify and verify the identity of the respondent institution, using reliable, independent sources. LFIs should verify the identity of respondent institutions using reliable, independent sources such as corporate registries, beneficial ownership registries, and other licensing authorities.[7] Although the LFI can require information directly from the respondent institution, the LFI should seek to verify this information. For verification purposes, the correspondent institution can rely on corporate registries, beneficial ownership registries, and other registries maintained by licensing authorities. For more information on what constitutes a reliable, independent source, please refer to the *Guidance for LFIs on CDD/KYC and Record-keeping*.

In addition to verifying the respondent institution's identity, an LFI should also identify and take reasonable measures to verify the identity of the respondent institution's UBOs. To perform this verification, the correspondent institution should gather sufficient information about the ownership and control structure of the respondent institution and establish that the respondent institution is not a shell bank. In this capacity, the correspondent institutions can obtain information on a respondent institution's shareholders, senior management, and other officers, as relevant, such as the Chief Executive Officer and the Chief Financial Officer. The LFI should then screen these parties against lists of sanctioned persons, internal watchlists (such as lists of customers previously exited for financial crime reasons), and relevant ML/TF/PF information sources (such as adverse media databases) prior to onboarding a respondent institution and opening the correspondent account.

If the LFI discovers that a PEP is associated with a respondent institution, such as a member of the respondent institution's Board of Directors or senior management, the LFI should ensure it has an understanding of the person, their role and the appropriateness of that role in the respondent institution, their ability to influence the respondent institution, and the risk they may present to the relationship.

Finally, as part of standard CDD, an LFI should determine if a financial institution customer must be subject to specific due diligence for correspondent banking relationships. If the financial institution qualifies as one of the types of financial institutions receiving correspondent banking financial services from the LFI, an LFI should apply the requirements for correspondent banking relationships in Section 6.3 *Specific Due Diligence for Correspondent Banking Relationships*.

---

[7] For more information on what constitutes a reliable source, please refer to the Guidance for LFIs on CDD/KYC and Recordkeeping.

6.3. Specific Due Diligence for Correspondent Banking Relationships

In addition to the CDD conducted on all customers, according to Article 25 of the AML-CFT Decision, LFIs are obliged to fulfil certain due diligence requirements regarding their correspondent banking relationships and other similar relationships they maintain, regardless of whether these relationships involve foreign or domestic financial institutions. Specifically:

- LFIs are required to collect sufficient information about any receiving correspondent institution for the purpose of identifying and achieving a full understanding of the nature of its business, and to determine, through publicly available information, its reputation and level of AML/CFT/CPF controls, including whether it has been subject to a ML/TF/PF investigation or regulatory action;
- LFIs are obliged to evaluate the AML/CFT controls applied by the receiving correspondent institution;
- LFIs are required to obtain approval from senior management before establishing new correspondent relationships; and
- LFIs are obliged to understand the responsibilities of each institution in the field of AML/CFT/CPF.

In performing the following steps on a respondent institution, the LFI should assess whether it is evaluating a correspondent banking relationship or "other similar relationship." As clarified by the FATF, "other similar relationships" includes providing services to MVTS providers when they act as intermediaries for other providers, or where they are accessing banking or similar services through the account of another MVTS customer of the bank. LFIs—including RHPs, exchange houses, and payment service providers—should therefore determine the extent to which they should apply enhanced measures—applying additional scrutiny and collecting additional information—on a respondent institution that poses increased ML/TF/PF risks, as referenced in Section 5, according to a risk-based approach.

A. Understand Respondent Institution's Business and Intended Purpose of the Correspondent Account

When an LFI performs CDD/KYC on a respondent institution, it should gather sufficient information to understand the nature of the respondent institution's business in line with identified risks. Understanding the respondent institution's business profile and intended purpose of the correspondent account requires the LFI to consider all relevant risk factors, such as developing a general overview of the respondent institution's products and services; customer base, including nested relationships; and countries and markets in which it operates.

What this means is that the LFI should seek to understand a respondent institution's major business activities, including the target markets and customer segments that are served by a respondent institution. In addition to

examining the nature of the respondent institution's business—the types of customers they serve and the location of their customers and markets—the LFI should evaluate the respondent institution's intended purpose of the correspondent account. In general terms, the LFI should evaluate the products and services the respondent institution will offer to its customers and how it will provide these services by assessing the following risk factors:

- The purpose of the services provided to the respondent institution (e.g., foreign exchange services for the respondent institution to conduct proprietary trading or payments between a respondent's financial group within the same jurisdiction are potential lower risk scenarios);

- What types of customers the respondent institution intends to serve through its correspondent banking relationship and how it will offer these services, such as:

    - Whether the correspondent account will be used for nested downstream activity, by either the respondent institution's affiliates (branches, subsidiaries, and affiliates of the respondent institution's financial group) or other third parties;

    - Whether the correspondent account will be used to conduct payable-through account activity, by either the respondent institutions affiliates (branches, subsidiaries, and affiliates of the respondent institution's financial group) or other third parties; and

- The expected activity within the correspondent account, including the transaction volume and value and the nature of the planned transactions.

Please note, the above risk factors that an LFI should evaluate for a respondent institution need to be applied equally to their branches, affiliates, and subsidiaries when they are direct customers of the LFI.

B. Assess Respondent Institution's Regulatory Status and AML/CFT/CPF Regime

In addition to understanding a respondent institution's business and purpose of the account, the LFI should verify that the respondent institution is subject to regulatory oversight and is licensed in the jurisdictions where it operates. This can involve obtaining a respondent institution's license or charter, or other documentation evidencing the respondent institution's authorization or certification to operate as a financial institution. Separately, the LFI should evaluate the regulatory AML/CFT/CPF framework where the respondent institution is based. Depending on the risk of the relationship, the LFI may also assess the regulatory AML/CFT/CPF framework where the respondent institution's ultimate parent is headquartered and the location of the respondent institution institution's branches and subsidiaries.

As discussed in Section 5.2 *Geographic Risk*, to determine the adequacy of a specific jurisdiction's AML/CFT/CPF regime, an LFI should review guidance from regulatory agencies and applicable international bodies, including by reviewing a country's Mutual Evaluation Report or other country assessment reports on a country's AML/CFT/CPF regime. This will help the LFI to evaluate the quality and effectiveness of a respondent institution's regulatory framework. Other sources of information include AML/CFT/CPF laws and regulations of the respondent institution's home country, and an LFI may even seek to engage AML/CFT/CPF supervisors and other relevant bodies about the AML/CFT/CPF regime in a respondent institution's home country.

C. Evaluate Respondent Institution's AML/CFT/CPF Control Framework

When assessing the level of risk of a particular correspondent banking relationship, LFIs should also evaluate a respondent institution's AML/CFT/CPF controls to decide whether to onboard or continue a correspondent banking relationship. Determining the adequacy of a respondent institution's AML/CFT/CPF controls is particularly important in the context of correspondent banking, as the LFI has limited visibility into the respondent institution's customer base. To mitigate this risk, the LFI is responsible to ensure that the respondent institution has appropriately conducted CDD/KYC on its customers and is implementing risk-based controls embedded within a broader

AML/CFT/CPF program to manage its risks. A useful tool for assessing a respondent institution's AML/CFT/CPF controls and determining the quality of the respondent's AML/CFT/CPF program is the Wolfsberg Group CBDDQ.

The Wolfsberg Group CBDDQ has been designed to provide LFIs with an in-depth view of a respondent institution's FCC policies and practices. Specifically, the CBDDQ enables LFIs to obtain a greater level of understanding of how a respondent institution mitigates the risk of their products, services, customer base, and jurisdictions. While LFIs may use the CBDDQ as part of their AML/CFT/CPF program's due diligence requirements, the Wolfsberg Group CBDDQ is only one possible source to understand a respondent institution's AML/CFT/CPF controls. LFIs are expected to perform their own internal assessment—going beyond relying on the respondent institution's responses—on whether their respondent institution has adequate AML/CFT/CPF controls, including by undertaking enhanced measures to understand and assess the AML/CFT/CPF controls of any higher-risk respondent institutions, as described in Section 6.4 *Enhanced Due Diligence for High-risk Correspondent Banking Relationships*.

In sum, all correspondent banking relationships should be subject to an appropriate level of due diligence following a risk-based approach. The CDD/KYC process should not be treated as a "paper-gathering exercise," and as such, this requires the LFI to assess the respondent institution's AML/CFT/CPF controls on a risk-sensitive basis (e.g., receiving a description of the respondent institution's AML/CFT/CPF policies, procedures, and process, and checking if the internal audit function or other external third party that regularly reviews the adequacy of the respondent institution's AML/CFT/CPF controls). This information-gathering process that is part of CDD/KYC should be supplemented by discussions with the respondent institution's Money Laundering Reporting Officer ("MLRO") and local management to assess their AML/CFT/CPF awareness and the respondent institution's compliance with international standards.

D. Assess the Respondent Institution's Reputation

Complementing its review of a respondent's institution regulatory status and AML/CFT/CPF regime, the LFI should research the respondent institution's reputation and determine if the respondent institution has been the subject of any investigation or regulatory action related to financial crime. Information to consider includes the specific type of regulatory action issued (civil, administrative, criminal); the timeframe of when the compliance lapses occurred; the severity of the deficiencies; and if applicable, how the respondent institution remediated the identified deficiencies. Public registries, third-party databases, and reputable newspapers can help in examining an LFI's AML/CFT/CPF record and understanding the respondent institution's overall reputation. Upon completing its review, the LFI should determine the extent to which the investigation or regulatory action is relevant to informing its onboarding decision, including whether the LFI should apply EDD measures on the respondent institution given the materiality of the investigation or regulatory action.

E. Senior Management Approval and Correspondent Banking Agreement

In all cases, the LFI should obtain approval from senior management before establishing new correspondent relationships, as required by FATF Recommendation 13 and Article 25 of the AML-CFT Decision. In addition, senior management approval should accompany a formalized, written agreement or contract that includes the following:

- Describes the correspondent and respondent institution's roles, responsibilities, and expectations of the respective parties, including the respondent institution's responsibilities specific to AML/CFT/CPF compliance;
- Covers the products and services to be provided under the correspondent banking relationship;
- Addresses any potential restrictions on the use of the correspondent banking relationship;
- Permitted third-party usage of the correspondent account and applicable internal controls to these situations;
- Any potential restrictions that the correspondent institution may want to place on the use of the correspondent account (e.g. limiting transaction types, volumes, etc.);

- Conditions regarding the requests for information on particular transactions, especially in the case of "payable through accounts" relationships, and

- Causes for termination or limitations of a business relationship.

Correspondent agreements should also include a statement that the respondent institution does not provide financial services directly or indirectly to shell banks or to customer types prohibited under the LFI's AML/CFT/CPF policies. Each agreement may differ based on the nature and risks of the correspondent relationship.

6.4. Enhanced Due Diligence for High-risk Correspondent Banking Relationships

Although all correspondent banking relationships should be subject to specific due diligence measures, an even higher level of scrutiny should be applied to respondent institutions that present greater ML/TF/PF risks when considering the risk indicators referenced in Section 5. Risk Factors. These risk factors include, but are not limited to, the following:

- Correspondent banking relationship arrangements that provide services to nested institutions or allow payable-through account activity;

- Respondent institution with geographic locations, including parent company, branches, and subsidiaries, in high-risk jurisdictions;

- Respondent institution has an ownership or management structure that poses specific ML/TF/PF risks (such as the presence of PEPs in the senior management or ownership structure);

- Respondent institution's is using the correspondent banking relationship to provide products and services that are higher risk for ML/TF/PF; and

- Respondent institution's customer base has a significant proportion of high-risk customer types due to the nature of their business or due to the jurisdictions where they are located or operate.

LFIs should follow a risk-based approach and scale their due diligence efforts based on the risk levels of correspondent banking relationships. Applying a risk-based approach to due diligence or tiered approach to CDD/KYC, ensures that the depth of information collected is commensurate with the associated risk levels of the correspondent banking relationships. For higher risk correspondent banking relationships, the LFI should apply EDD measures on institutions that pose increased ML/TF/PF risks. Conducting a more detailed and in-depth review for higher-risk relationships, may include, but is not limited to, reviewing thoroughly the respondent institution's AML/CFT/CPF controls and internal audit reports, interviewing an MLRO and Compliance Department, obtaining an independent third-party review of the respondent institution's AML/CFT/CPF controls, and potentially scheduling an onsite visit. The onsite visit could be an opportunity for the LFI to speak with representatives of the respondent institution to obtain additional information, review AML/CFT/CPF controls, and corroborate findings.

In addition to such enhanced measures for understanding the respondent institution's risk profile, an LFI may seek to establish additional terms in the LFI's written agreement with the respondent institution, as referenced in Section 6.3. Specific additional measures to establish between the LFI and respondent institution includes potential restrictions and controls the LFI seeks to apply to the correspondent banking relationship as a condition for opening a correspondent account and for reducing the risk posed by the relationship. Examples of risk-based measures an LFI could apply on a higher risk correspondent banking relationship are the following:

- Restricting certain products offered to the respondent institution (e.g., restricting the use of higher-risk products like international cash letters);

- Limiting the volume of activity (e.g., only executing a certain amount of third-party transactions in the span of a month); and

- Conducting real-time monitoring and sample testing of transactions to ensure timely and effective detection of potentially suspicious activity.

Additionally, higher levels of senior management approval may be necessary for higher risk correspondent banking relationships, as well as the performance of transaction monitoring review of all activities to determine consistency with profile, projected account activity and actual volumes.

6.5. Ongoing Monitoring of Correspondent Banking Relationships

Following the decision to onboard a respondent institution, an LFI should review its relationships with respondent institutions on an ongoing basis to assess whether the relationship remains within the LFI's risk appetite. For high-risk correspondent banking relationships, LFIs should conduct ongoing due diligence at least annually or more frequently based on changes in assessed risk levels, customers behaviors, or regulatory updates. This review should include evaluating the ongoing effectiveness of the respondent institution's AML/CFT/CPF program and to ensure that all information relating to a respondent institution's CDD/KYC risk profile are accurate and up to date. CDD/KYC information should be updated regularly in accordance with a risk-based approach, and updates should also occur when there are changes to risks associated with the relationship.

6.5.1. Ongoing Due Diligence

LFIs are required to conduct ongoing due diligence of a correspondent banking relationship (both existing and new relationships), including periodic reviews of the CDD/KYC information on the respondent institution. The frequency of these reviews will depend on the levels of risk associated with the respondent institution, based on risk factors, changes in customer behavior, or regulatory updates. For high-risk relationships, reviews, including periodic reviews of CDD/KYC information, should be conducted more frequently (e.g., quarterly) to ensure that all information is up-to-date and aligns with the risks established at onboarding. In addition to updating a respondent institution's CDD/KYC information, an LFI should conduct a risk-based review to determine the effectiveness of the respondent's AML/CFT/CPF program, and the respondent institution's ability to manage risks of its customers. By conducting a reassessment of its correspondent banking relationship, an LFI ensures information on the respondent institution is up to date and aligns with the risks of the relationship established at onboarding. The frequency with which periodic reviews are undertaken will depend on the level of risk associated with the respondent institution. When a review identifies material changes in the respondent institution, the LFI should reflect on whether it should adjust its risk assessment of the respondent institution and what further information may be needed to support this adjustment.

Particularly important in the context of correspondent banking is an account activity review of the respondent institution's activity on the correspondent account. As part of this account activity review, the LFI should review the respondent's transactional activity, paying close attention to whether transactional activity is inconsistent with due diligence information or expected activity and whether there are any material changes in the volume and/or value of transactions in the correspondent account. To this end, the LFI should utilize all available information, such as the presence of any adverse news on the respondent and its customers and whether any suspicious activity reports ("SARs") or suspicious transaction reports ("STRs") were filed on the respondent and its customers. Furthermore, the correspondent institution should identify whether the services will be used, via nested or downstream correspondent banking relationships, by either the respondent bank's affiliates or other third parties. The correspondent institution should conduct enhanced ongoing monitoring of these activities, and specifically review full transactions to assess the potential misuse of nested relationships by LFIs from higher-risk jurisdictions. Overall, the account activity review should help facilitate a comparison between what the respondent institution declared at

onboarding or during the last periodic review with the respondent institution's actual use of the correspondent account.

Any change identified during the ongoing monitoring should be promptly reflected in the LFI's risk profile as well as in enterprise-wide ML/TF/PF risk assessment. If an LFI finds that after a reassessment of a respondent institution's relationship, the respondent institution's risk profile has changed and/or is using the correspondent account in a manner that is outside of the LFI's risk appetite, the LFI should seek to communicate correspondent account termination decisions to senior management. LFIs should give consideration to account terminations that could restrict access to financial services for an entire group of customers, potential customers, or geographic locations. LFIs should maintain a clear audit trail of the reasons and process for closing the account.

Best Practices: Continual Communication about Correspondent Banking

A correspondent institution should continuously engage a respondent institution to understand and assess the AML/CFT/CPF controls a respondent institution. As per best practice, this can also take the form of regular outreach and ongoing dialogue that also includes messaging a correspondent institution's AML/CFT/CPF requirements and expectations specific to the correspondent banking relationship.

Helping a respondent institution understand a correspondent institution's AML/CFT/CPF policy and risk appetite, for instance, can bridge any gaps in understanding and also promote the adoption of a robust AML/CFT/CPF control framework. In addition, this type of engagement supports with the identification of any new and emerging risks; helps quickly resolve any incidents (such as any requests for information specific to activity detected through a correspondent institution's transaction monitoring program); and overall, enables a coordinated approach to a correspondent institution's risk management program.

LFIs should also document all findings from ongoing monitoring activities, including any actions taken in response to identified risks, to ensure accountability and facilitate the conduct of audits.

6.6. Suspicious Activity and Reporting in Correspondent Banking

6.6.1. Transaction Monitoring

Under Article 16 of the AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may require filing of an STR, SAR, or other report types. Moreover, as required by Article 7 of the AML-CFT Decision, LFIs must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity, and the risks they pose, including, when necessary, the source of funds. Transactions may be suspicious simply by virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries). Alternatively, transactions may be suspicious because, together with other transactions, they form a pattern that diverges from expected or historical transactional activity and may otherwise be indicative of illicit activity.

In the context of correspondent banking, LFIs should continuously monitor transactions to, from, or through the correspondent account for unusual and potentially suspicious activity. Specifically, LFIs should put in place appropriate transaction monitoring policies, procedures, processes, and technology to be able to detect any activity that is inconsistent with the purpose of the services provided to the respondent institution and/or that is not in line with the anticipated activities of the respondent institution. The policies and procedures should require appropriate monitoring of the Respondent's activity, incorporating due diligence results, such as customer risk rating and other factors considered meaningful in the assessment of transaction activity. The results of suspicious activity monitoring should be factored into the periodic review of the customer relationship, particularly when the results of transaction monitoring indicate elevated risk levels. The relationship between due diligence information and transaction monitoring shall be continuous throughout the life of the Respondent relationship and apply to both the

Respondent and any related suspicious activity. These policies and procedures should also include guidance and examples on what the correspondent institution considers to be unusual or suspicious.

While all correspondent banking relationships should be subject to ongoing monitoring, certain respondent institutions may require enhanced monitoring depending on unique risk factors posed by the relationship (e.g., respondent institution is located in high-risk jurisdiction, respondent institution has a history of prior SAR/STR filings, etc.). To this end, as part of transaction monitoring, LFIs should tailor their scenarios, parameters and thresholds used to monitor correspondent banking activities. For example, LFIs can adapt transaction scenarios to identify hidden relationships between accounts and customers, which can be useful to identify common beneficiaries and remitters amongst apparently unconnected parties.

Overall, transaction monitoring programs should be calibrated to the size, nature, and complexity of each institution. Larger LFIs with extensive correspondent banking relationships, as well as high transaction volumes and values, may implement Transaction Monitoring systems that also track the activities of their customers' customers. Transaction monitoring can include manual monitoring processes and the use of automated and intelligence-led monitoring systems, with automated solutions being the preferred option. LFIs with a larger scale of operations are expected to have automated systems capable of handling, in real time, the risks from an increased volume and variance of transactions. LFIs utilizing automated systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. While smaller LFIs may rely on transaction monitoring systems that are less automated, they should still ensure that their systems and controls are appropriately executed to address the risks from their day-to-day transactional activity. With that understanding, smaller LFIs should look to employ automated systems wherever feasible.

6.6.2. Suspicious Transaction/Activity Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, LFIs must file an STR, SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, or are intended to be used in a crime. LFIs should continuously monitor transactions to identify behaviour that is potentially suspicious and may require filing of an STR, SAR, or other report types. Transactions may be suspicious due to individual characteristics (e.g., value, source, destination) or because they form a pattern diverging from expected or historical transactional activity. This applies equally in relation to suspicious transactions involving a respondent institution's activities. LFIs are encouraged to adopt a proactive monitoring strategy that anticipates potential suspicious activities, thereby strengthening their overall AML/CFT framework.

When a transaction monitoring system alerts the LFI to a transaction that could indicate potentially suspicious activity, the LFI should have processes to request information from a respondent institution to investigate the alerted activity. In order to understand the background of a transaction that has been processed through a correspondent account, the correspondent bank may send a request for information. This request for additional information should be targeted on the specific transaction which created an alert in the system, and could include, depending on the risk level of the transaction, a request to access information about the customer of the respondent institution as a means to get a proper understanding of the reasonableness of the transaction. Depending on the risk of the activity, the correspondent institution may request that the respondent institution provide information about their customer. Accordingly, when an LFI is assessing whether to file an STR or SAR, an LFI may seek to request information on a respondent institution's customers, such as:

- Purpose of the customer's account with the respondent institution;
- Duration of customer relationship with the respondent institution and whether the respondent institution classifies the customer as a high-risk customer;
- Customer's source of funds;

- Information regarding the customer's legal and ownership structure (such as information on parent company and the customer's UBOs);
- Nature of the relationship (including any other affiliations/connections) between the customer and counterparty;
- Purpose of the transaction (including goods and services exchanged) between the customer and counterparty;
- Alignment of the transaction with the customer's historical transactional activity;
- Status of the bank account of customer (opened/closed); and
- Any other relevant information about the customer to support with the LFI's investigation.

Responses to requests for information by the respondent bank should be timely and provide responses to inquiries related to transactions in the account with the level of detail requested, If the respondent institution fails to provide sufficient documents and data in response to the LFI's request for information, or the documents and data indicate the presence of illicit activity, an LFI may have grounds to file an STR or SAR. Furthermore, a request for information could be followed by a reassessment of the respondent's business and risk profile where/when necessary. STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. By filing STRs with the UAE Financial Intelligence Unit ("FIU"), LFIs alert law enforcement authorities about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs. LFIs should ensure that all relevant staff receive comprehensive training on identifying suspicious transaction patterns and the appropriate actions to take when such patterns are detected. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.[8]

An STR or SAR also may trigger concerns that the respondent institution is unable to manage its financial crime risks and could lead to a reassessment of the respondent's relationship with the correspondent institution, depending on the severity of the activity. If a correspondent institution collects data and documents that do not necessitate a STR or SAR filing, the information obtained should nonetheless be recorded in the respondent institution's customer profile for future reference.

---

[8] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

6.7. Targeted Financial Sanctions Obligations

The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the UNSC under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, the Cabinet Decision 74 of 2020 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS"), including the UAE Local Terrorist List and the UNSC Consolidated List.

In addition, under Article 15 of the AML-CFT Decision, LFIs are required to have suitable risk management systems and take sufficient measures to identify whether a customer, or the beneficial owner of a customer, has been added to UAE Local Terrorist List or UNSC Consolidated List. In practice, it will generally be appropriate to conduct screening prior to onboarding and ongoing screening on all customers.

LFIs should take appropriate steps to screen customers and transactions. Respondent institutions frequently use SWIFT messages to conduct cross-border remittances, and LFIs with a high volume of SWIFT messages should determine whether their screening efforts are adequate to detect involvement of a sanctions target, particularly in the case of screening backlogs, unusual spikes in screening activity, updates to the relevant sanction lists, and other operational events.

Correspondent banking due diligence and ongoing account monitoring should also consider how well the respondent institution is implementing sanctions screening, including information on the mechanisms for screening transactions with required originator and beneficiary information, risk-based policies and procedures for determining how to handle such transactions, systems for sanctions screening, and procedures and systems for clearing false positives results.

Correspondent institutions should adopt strict sanctions programs and screen all the information available (e.g., payer's information, payee's information, and intermediary's information) against relevant sanctions list to ensure there is no sanctioned person involved in the transaction. The timing of the screening should be in a manner that allows freezing or suspending of assets once such assets are in an LFI's possession. For more information and details on obligations in relation to sanctions obligations, LFIs should consult the Executive Office for Control and Non-Proliferation ("EOCN")'s *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*[9] and the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*" and *Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening.*[10]

---

[9] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.
[10] Available at: https://www.centralbank.ae/en/cbuae-amlcft

6.7.1. Confirmed Name Match Reports

LFIs must implement strict protocols for addressing confirmed matches, including immediate reporting to authorities and potential termination of the relationship, to ensure compliance with sanctions obligations. If an LFI identifies a confirmed name match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List, LFIs are required to take the following actions:

- Implement all necessary measures without delay as outlined in Article (21) of Cabinet Resolution No. (74) of 2020, to include freezing without delay, refraining from offering any funds or other assets and services, and reporting freezing measures to the EOCN and CBUAE; and

- If the confirmed name match is a potential customer, reject the transaction immediately and report the case.[11]

LFIs should promptly apply directives issued by competent authorities of the UAE, if a confirmed match is identified. Per Section (5) of Article 21 of Cabinet Resolution No. (74) of 2020, LFIs are expected to freeze assets without delay (24 hours) and report any freezing measures, prohibition to provide funds or services, and any attempted transactions immediately via the goAML platform within five working days by selecting the Confirmed Name Match Report ("CNMR") option. LFIs should also ensure that all necessary information and documents regarding the confirmed name match are submitted along with the CNMR. Pursuant to Section (1) of Article 22 of Cabinet Resolution No. (74) of 2020, supervisory authorities should receive all information within five working days.

---

[11] See also EOCN, *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*, section 4, available at: https://www.uaeiec.gov.ae/enus/un-page?p=7.

6.7.2. Partial Name Match Report

If an LFI identifies a partial name match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List, LFIs should take the following actions:

- Cross-check the identifiers published on the relevant sanctions list with the LFI's internal customer, beneficial ownership, and other data as well as external sources where appropriate to determine whether the

partial name match is a confirmed match or can be waived as a false positive; and

- If the LFI is unable to determine whether the partial name match is a confirmed name match or a false positive, the LFI must suspend any transaction and report the case to the EOCN and the CBUAE and uphold the suspension measures until a response is received from the EOCN on the status of the partial name match.

LFIs are expected to submit a Partial Name Match Report ("PNMR") through the goAML platform within five working days of implementing the suspension measures. LFIs should ensure that all necessary information and documents regarding the potential match are submitted to the PNMR.

6.8. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT/CPF program that is appropriate to the risks an LFI and respondent institution face, and organized in accordance with the "three lines of defence" model. All three lines of defence must report up to, and have the active support and oversight of, the LFI's senior management, defined broadly to include executives, senior leadership, and the Board of Directors. Specific to managing the unique risks posed by correspondent banking relationships, LFIs should consider creating a formal governance body with oversight of correspondent banking relationships. The governance body can be charged with reviewing and approving certain high-risk correspondent banking relationships and act as a point of escalation for potentially suspicious activity involving correspondent accounts and circumstances warranting termination of a correspondent banking relationship.

LFIs should organize their AML/CFT/CPF programs according to the 'three lines of defence' model: frontline personnel as the first line of defence; AML/CFT compliance function as the second line, and internal or external auditors as the third line. The governance body should include representation from all three lines to ensure effective oversight and risk management.

Under three lines of defence model, an LFI operating correspondent banking services including its business units, sales or relationship managers, and other frontline personnel serve as the **first line of defence** against ML/TF/PF, and other forms of illicit activity. They should scrutinize respondent institutions at onboarding and perform periodic and risk-based account activity reviews to update respondent institution information and the LFI's understanding of the respondent's risks.

The LFI's AML/CFT compliance function, in turn, constitutes the **second line of defence**, supporting the frontline units' risk management activities through its system of internal controls and related monitoring, reporting, and risk assessment responsibilities. The core of an effective risk-based program is an appropriately experienced MLRO, located within the second line of defence, who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. The governance body with oversight of correspondent banking, as described above, should include representation from the first and second lines of defence.

Finally, under Article 20.6 of the AML-CFT Decision, LFIs must be subject to independent testing by internal or external auditors, who represent the **third line of defence** by providing independent assurance to the Board of Directors and senior management on the effectiveness and adequacy of the LFI's governance, risk management, and internal controls. LFIs should conduct independent audits of their AML/CFT/CPF programs regularly following a risk-based approach to assess the compliance with regulatory requirements and the effectiveness of controls of the LFI's AML/CFT/CFP program, with a scope including correspondent banking relationships and associated risks. Auditors should have sufficient expertise and understanding of ML/TF/PF risks and requirements and should be fully independent of the activities and reporting structure of the functions subject to independent testing.

Additionally, as per Article 32 of the AML-CFT Decision, LFIs with overseas branches, subsidiaries, or other affiliates or legal entities must ensure that all entities within the affiliate network are subject to the AML/CFT/CPF policies, procedures, and controls that are at least as stringent as those in place at the LFI located in the UAE. Likewise, all

institutions within the affiliate network should be included in the LFI's enterprise risk assessment and subject to AML/CFT independent testing and consolidated governance and oversight.

6.9. Training

As with all risks to which an LFI is exposed, an LFI's AML/CFT/CPF training program should ensure that employees are aware of the risks of correspondent banking relationships and equipped to apply appropriate risk-based controls to manage these risks. Training should be tailored and customized to an LFI's risk and the nature of its operations and should be clearly documented in its AML/CFT/CPF program, including associated policies, procedures, training plans, and training materials. LFIs should provide training to employees at onboarding, and on an ongoing basis, covering updates in AML/CFT/CPF emerging and evolving risks, including correspondent banking risks.

Specifically, the LFI's AML/CFT/CPF training programs should train employees on how correspondent banking transactions may be used for ML/TF and should also refer employees to the systems, processes, and controls, documented in the LFI's policies and procedures, for managing this risk. This training should be targeted to cover those employees directly involved in correspondent banking transactions and dealing with correspondent banking relationships, such as front-line managers and other personnel associated with an LFI's correspondent banking unit. Tailored training should, among other topics, cover:

- Applicable AML/CFT/CPF laws and recent trends in ML/TF/PF, including the ways in which such laws demonstrate changes to correspondent banking guidance, best practices, and risk mitigation strategies;
- The LFI's own policies, procedures, and processes to combat ML/TF/PF, including how to identify and report suspicious correspondent account activity; and
- ML/TF typologies of abuse of correspondent banking relationships, including transaction monitoring scenarios.

Ensuring that AML/CFT/CPF compliance personnel are aware of and trained on global FCC standards and best practices is critical to proactively ensuring an LFI is meeting current correspondent institution and international AML/CFT/CPF expectations in the context of its correspondent banking relationships. Respondent institutions should proactively engage their correspondent institution if they need assistance in interpreting global FCC standards or require targeted training.

6.10. Record-keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs operating correspondent banking services must maintain detailed records associated with their ML/TF/PF risk assessment and mitigation measures as well as records, documents, data and statistics for all financial transactions, all records obtained through CDD/KYC measures for both the originators and the beneficiaries, account files and business correspondence, copies of personal identification documents, including STRs/SARs and results of any analysis performed. LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs must maintain all records, documents, and data for all transactions, whether local or international, and should make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five years, from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

When an LFI enters into a correspondent banking relationship, for example, it should keep all the due diligence records associated with the respondent institution for at least five years, such as:

- A copy of the respondent institution's license or banking charter;
- A copy of the correspondent banking contractual agreement outlining the respective responsibilities of the correspondent institution and the respondent institution;
- Due diligence conducted on the respondent institution, including the respondent institution's AML/CFT/CPF controls and compliance with AML/CFT/CPF regulations in jurisdictions where the respondent institution operates;
- A Wolfsberg Group CBDDQ completed by the respondent institution;
- A written statement from the respondent institution that it does not have a correspondent banking relationship with a shell bank; and
- Records of site visits and call reports documenting the interviews conducted of the respondent institution, as applicable.
- A copy of records of the ML/TF/PF risk assessment of the correspondent banking relationship and any mitigation measures. This should include CDD/KYC records, account files, business correspondence, copies of personal identification documents, STRs/SARs, and results of any analysis performed.

LFIs should also ensure that all records are stored securely with access controls in place to protect sensitive information, in compliance with data protection regulations.

Annex 1. Global Standards on Correspondent Banking

Given the different risk factors posed by correspondent banking relationships, both global standards-setters and industry groups have issued standards, principles, and guidance governing how correspondent institutions should seek to manage the ML/TF/PF risks associated with their correspondent banking relationships. Particularly, as foreign respondent institutions may not be subject to equivalent laws, regulations, and supervision as domestic LFIs, the FATF and Wolfsberg Group recommend specific measures for correspondent institutions to gain appropriate assurance that respondent institutions are adequately managing the ML/TF/PF risks associated with their customers, about whom the correspondent institution may have limited information.

FATF Standards

As part of the FATF Standards, FATF outlines the due diligence that correspondent institutions should apply to understand the risks of a respondent institution and the respondent institution's customers. Correspondent institutions should apply due diligence to understand the risks of respondent institutions and their customers by gathering sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine the institution's reputation and the quality of its supervision. Specifically, FATF Recommendation 13 sets forth EDD requirements for financial institutions providing financial services to foreign respondent institutions, as these relationships are seen to be inherently higher risk for ML/TF than domestic correspondent relationships. In addition, the FATF requires EDD for financial institutions providing financial services to "similar relationships" as cross-border correspondent banking relationships, which includes providing services to MVTS providers when they act as intermediaries for other providers, or where they are accessing banking or similar services through the account of another MVTS customer of the bank. These requirements supplement the basic CDD requirements that LFIs must meet for all customers under Recommendation 10. FATF Recommendation 13 requires financial institutions to:

- Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine the institution's reputation and the quality of its supervision,

including whether it has been subject to a ML, TF or PF investigation or regulatory action;

- Assess the respondent institution's AML/CFT/CPF controls;
- Obtain approval from senior management before establishing new correspondent relationships;
- Delineate clearly the responsibilities of each institution; and
- Ensure that the respondent institution has conducted CDD on "payable-through accounts" customers with direct access to accounts of the correspondent institution, and that the correspondent institution can provide relevant CDD information upon request.

According to FATF Standards, LFIs also should avoid entering into, or continuing, a correspondent banking relationship with shell banks, defined as banks that have no physical presence in the country in which it is incorporated and licensed. In addition, LFIs should verify that respondent institutions do not permit their accounts to be used by shell banks.

The Wolfsberg Group

The Wolfsberg Group is an industry group of 12 global banks that aims to develop industry standards for the management of financial crime risks, particularly with respect to AML/CFT policies. The Wolfsberg Group has published a number of documents, including principles, guidance, frequently asked questions ("FAQs"), and statements. Of these documents, the 2022 Wolfsberg Financial Crime Principles for Correspondent Banking,[12] known as the Wolfsberg Principles, represents global guidance for financial institutions engaging in foreign correspondent banking relationships.

Wolfsberg Principles and Correspondent Banking Due Diligence Questionnaire

To assist with the due diligence process for cross-border and other higher risk correspondent banking relationships, the Wolfsberg Group issued a Correspondent Banking Due Diligence Questionnaire ("CBDDQ"), most recently revised in February 2023.[13] The CBDDQ is designed to help correspondent institutions collect information that can inform a risk assessment of their respondent institution's business and financial crimes risk management program, with sections addressing the following information about a respondent institution:

- A respondent institution's basic information, ownership structure, and regulatory background;
- Products and services offered by the respondent institution;
- Information aimed at helping a correspondent institution assess the adequacy of the respondent institution's AML/CFT/CPF, sanctions, fraud and anti-bribery and corruption ("ABC") programs; and
- Information on a respondent institution's policies, procedures, and controls covering CDD/KYC, EDD, risk assessment, payment transparency, monitoring and reporting, independent testing, quality assurance/compliance testing, and training.

The use of this questionnaire or similar risk assessment tools has become an industry best practice for foreign financial institutions with global networks that receive correspondent banking services.

Best Practices: Correspondent Banking Due Diligence Questionnaire

- Respondent institutions should integrate Wolfsberg Group's 2023 CBDDQ into their AML/CFT/CPF program, guiding their approach to managing the risk of correspondent banking relationships.

- Respondent institutions should refer to the CBDDQ as the "industry standard" for CDD/KYC requirements and expectations, which can help respondent institutions if located in jurisdictions with less stringent AML/CFT/CPF regulatory regimes.

- Respondent institutions may seek to communicate about their alignment with the CBDDQ requirements, whether as part of a site visit or other correspondence with the correspondent institution, in order to provide assurance to the correspondent institution about the rigor of the respondent institution's AML/CFT/CPF controls applied on its customers.

- Respondent institutions should regularly update the CBDDQ and proactively communicate changes about their AML/CFT/CPF controls to the correspondent institution.

Correspondent institutions should utilize tools like the Wolfsberg Group's Correspondent Banking Due Diligence Questionnaire (CBDDQ) to assess the adequacy of the respondent institution's AML/CFT/CPF controls, sanctions, fraud, and anti-bribery and corruption programs. The CBDDQ should be integrated into their AML/CFT/CPF program to guide their approach to managing the risk of correspondent banking relationships.

---

[12] Wolfsberg Group, "Wolfsberg Financial Crime Principles for Correspondent Banking," 2022, https://db.wolfsberg-group.org/assets/d39a50727fb6-4e31-9a87-9e54021ce71f/Wolfsberg%20Correspondent%20Banking%20Principles%202022.pdf
[13] Wolfsberg Group, "Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ) V1.4," 2023, https://db.wolfsberggroup.org/assets/27bae403-246e-419c-8c37-af52e66b53ad/CBDDQ%20v1.4.pdf

Annex 2. Correspondent Banking Red Flags

Correspondent institutions should identify and address red flags by continuously monitoring transactions for red flags and unusual patterns. The following is a list of red flags[14] associated with correspondent banking relationships. These red flags, when combined with the risk factors identified in this Guidance, present instances that, when identified, warrant additional scrutiny.

- The activity of the correspondent account is inconsistent with the foreign correspondent banking customer's business;

- Transactional activity that appears unusual in the context of the relationship with the correspondent account;

- Many funds transfers are seen in large, round-dollar amounts, where the correspondent account has not previously been used for similar transfers;

- An unusually large number of funds transfers or fluctuations in the volume of funds transfers (e.g., sudden bursts of activity followed by lulls);

- Funds transfer activity to or from a correspondent account that is unexplained, repetitive, or shows unusual patterns;

- The engagement in an unusual volume of the foreign correspondent banking customer's own bank check or dollar draft activity;

- A sudden increase in transaction volume, especially if it involves high-risk jurisdictions;

- Unusually high numbers of returned or rejected items involving a correspondent account;

- Large currency or bearer instrument transactions either into or out of the correspondent account;
- The deposit or withdrawal from a correspondent account of multiple monetary instruments (e.g., traveler's checks, money orders and bank drafts) just below the reporting threshold on or around the same day, particularly if the instruments are sequentially numbered;
- The issuance of large volumes of cashier's checks or bank drafts against the correspondent account, particularly when the face amounts are less than local reporting requirements; and
- High-value deposits or withdrawals, particularly irregular deposits or withdrawals, not commensurate with the type of correspondent account or business of the foreign correspondent banking customer;
- The provision of insufficient or suspicious information during the onboarding process;
- The reluctance to provide complete information about the nature and purpose of its account, anticipated account activity, prior correspondent banking relationships, the names of its officers and directors, or information on its business location;
- Transactions occurring in bursts of activity within a short period of time;
- A request to establish a relationship with, or route a transaction through, a financial institution that is not accustomed to doing business with foreign financial institutions and that has not sought out business of that type;
- The routing of transactions through several jurisdictions or financial institutions prior to, or following entry into, the financial institution without any apparent purpose other than to disguise the nature, source, ownership or control of the funds;
- Frequent or numerous funds transfers originating from or for the benefit of shell banks or high-risk foreign correspondent banking customers;
- Fund transfer activity occurring to or from a correspondent account originating from or going to a financial secrecy haven or a higher-risk geographic location (such as a FATF non-cooperative jurisdiction) without an apparent business purpose, or when the activity is inconsistent with the foreign correspondent banking customer's business or history;
- Beneficiaries of foreign correspondent banking customers maintaining accounts at foreign financial institutions that have been the subject of previous SAR/STR filings due to suspicious wire activity;
- The reappearance of a beneficiary's financial institutions based in offshore locations, the account of at least one of which has been closed by the foreign correspondent banking customer due to overall suspicious activity;
- Large currency or bearer instrument transactions either into or out of the correspondent account; the deposit or withdrawal from a correspondent account of multiple monetary instruments (e.g., traveler's checks, money orders and bank drafts) just below the reporting threshold on or around the same day, particularly if the instruments are sequentially numbered;
- The issuance of large volumes of cashier's checks or bank drafts against the correspondent account, particularly when the face amounts are less than local reporting requirements;

- High-value deposits or withdrawals, particularly irregular deposits or withdrawals, not commensurate with the type of correspondent account or business of the foreign correspondent banking customer;
- Funds transfers to or from the correspondent account originating from or going to accounts of individuals or entities identified by law enforcement agencies as being suspected of engaging in money laundering or terrorist activities;
- The presence of a sanctioned entity as beneficiary; and
- An inquiry by or on behalf of a foreign correspondent banking customer regarding exceptions to the reporting requirements of the UAE or other rules requiring the reporting of suspicious transactions.

---

[14] The Clearing House, "Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking," February 2016, https://media.theclearinghouse.org/-/media/Action-Line/Documents/Volume-VII/20160216-TCH-AML-Correspondent-Banking-GuidingPrinciples.pdf?rev=dc5d809b732b4afd8d29c049a13a277b&hash=62D3B42791D3F39276D1E5B8FC814A94

Annex 3: Transition from SWIFT to the ISO 20022 Payment Standard

As the financial industry continues to grow in complexity and geographical coverage, financial institutions are relying on an ever-growing number of different settlement systems, data exchange formats and standards. For example, financial institutions rely on SWIFT to settle cross-border payments (with SWIFT being a proprietary messaging system), but also use domestic settlement systems such as SEPA (Europe), CHIPS and the Fedwire (US), CHAPS (UK), and others. Separately, for settling securities-related transactions, financial institutions rely on yet another set of systems such as DTCC (US) and Cboe Clear (Europe). In the UAE, the Central Bank of the UAE owns, operates and manages the following payment systems, categorized into Large-Value Payment Systems such as the UAE Funds Transfer System and Retail Payment Systems such as the Image Cheque Clearing System, the UAE Wages Protection System, the UAE Switching System, the UAE Direct Debit System, the UAE Payment Gateway System. Therefore, a financial institution often needs to deploy multiple systems and tools that are able to generate, process, and store messages in the various formats used by different settlement providers.

Lack of a uniform, global standard causes delays in payments, securities settlements, and other financial services; interrupts straight-through processing ("STP") and requires manual intervention; necessitates the deployment of multiple internal systems; and may also lead to lack of transparency or failure of certain automated compliance controls. To address these issues, the International Organization for Standardization ("ISO") developed ISO 20022, a new financial standard that is envisioned to become a global standard on payments. SWIFT is a major participant and contributor in developing this new standard, promoting its adoption worldwide.

ISO 20022 is based on the core principle that all financial industry market participants—from financial institutions to end-users—should be able to rely on a single global standard that is based on methodology and glossary available to all in open source. The ISO 20022 standard has also been designed with the aim of being able to cover all types of business processes of the industry, ranging from accounting, payments, to securities settlements and asset allocation. Instead of designing a new message type for a particular subset of financial transactions, the ISO 20022 standard aims to create a library of all business processes that exist in the financial industry (with an opportunity to document new processes in future, if needed) and then write automated messages based on certain "blocks" that are elements of each documented business process. All these processes and building blocks are available in the open-source Data Dictionary published by ISO. To further promote uniformity, ISO 20022 uses XML (eXtensible Markup Language), which is a widespread international language model to represent structured information.

While for certain financial processes the adoption of ISO 20022 is voluntary, in 2018, the SWIFT community decided to adopt ISO 20022 for all cross-border payments. The adoption period started in March 2023 and is scheduled to

be completed by November 2025. During this period ISO 20022 and SWIFT MT messages co-exist. However, starting in November 2025, SWIFT will retire SWIFT MT 1xx, 2xx, and 9xx message series (other MT messages are not currently impacted). The adoption of the global ISO 20022 cross-border payment standard will lead to further improved STP rates, offer higher quality data exchange, and further transparency.

The transition from SWIFT to ISO 20022 will require correspondent institutions to adapt their systems for processing cross-border payments. This transition should be managed proactively to ensure that all necessary infrastructure is in place, including training staff on the new standard and testing systems for compliance with ISO 20022 requirements. Financial institutions should prepare for the transition to ISO 20022 by assessing their current systems for compatibility, investing in necessary upgrades, and providing comprehensive training for staff to ensure a smooth transition, During the transition from SWIFT to ISO 20022, LFIs should also ensure that internal systems are updated to handle both message formats concurrently to avoid disruptions in payment processing.

Annex 4: SWIFT and Non-Customer RMA Relationships

As discussed above, the SWIFT network is a messaging infrastructure, and not a settlement system. In the context of correspondent banking, financial institutions use the SWIFT RMA messaging capability to exchange secure messages with non-customer financial institutions or other third parties for the purpose of facilitating non-transactional and transactional messages. This type of engagement between financial institutions supports the exchange of information necessary for international finance and global banking— whether or not the message exchanged contains payment instructions. As a result, LFIs should also understand the requirements and their obligations surrounding SWIFT RMA relationships.

Within the category of non-customer RMA relationships, "reporting-only" relationships are those noncustomer RMA relationships in which exchanged messages do not lead to the initiation of any transactions; "transactional" relationships, on the other hand, are all other non-customer RMA relationships that do lead to the initiation of transactions.

Examples of non-customer RMA relationships may include:

- The receipt of balance and transaction information on a corporate customer's account at another financial institution, so that the corporate customer can view activity through its financial institution's reporting tool.
- The relaying of payment instructions from a corporate customer to their third-party financial institution.
- The provision of information from a sub-custodian financial institution to the global custodian at the request of the customer.
- The exchange of messages with financial institutions that do not otherwise have direct payment relationships, such as in the context of trade finance.

As advised by the Wolfsberg Group,[15] for transactional non-customer RMA relationships, financial institutions should perform the following minimum due diligence prior to the exchange of SWIFT keys and on a periodic basis thereafter:

- Collect the name and address of the non-customer financial institution or other third party;
- Conduct name screening against relevant watchlists, such as internal, PEP, and sanctions lists in accordance with applicable internal policies and procedures.
- Assess the risks associated with the RMA relationship on the basis of the above information and applicable "red flags" to determine whether further review is required based on the financial institution's risk appetite.[16]

Separately, a more granular version of RMA, known as RMA Plus, allows institutions to specify which message type(s) they want to send to and receive from each of their counterparties. The use of RMA Plus to restrict the range of

message types that can be exchanged may enable financial institution personnel to review a correspondingly restricted list of red flags for the purpose of assessing the risk associated with the RMA relationship.

For non-customer RMA relationships that are reporting-only, there are no minimum due diligence requirements; however, sanctions obligations should always be considered as it relates to the information that is available to the financial institution. The Wolfsberg Group also indicates that financial institutions should periodically review non-customer RMA relationships to identify those that should be canceled due to lack of usage.

Finally, financial institutions should establish clear communication protocols and maintain comprehensive documentation for all non-customer RMA relationships to ensure compliance and facilitate risk management.

---

[15] Wolfsberg Group, "Guidance on SWIFT RMA Due Diligence," 2024, https://db.wolfsberg-group.org/assets/ed52141f-81ce-4cdf-9815ceff95cb941c/Swift%20RMA%20Guidance.pdf

[16] Applicable "red flags" may be similar to the correspondent banking red flags listed in Annex 2. Correspondent Banking Red Flags. These may include, but are not limited to: unexplained or unusual transactions such as frequent transfers of large sums of money to and from high-risk jurisdictions, without clear or legitimate business reasons; layering or routing funds to third parties without any clear commercial justification; involvement of high-risk or sanctioned jurisdictions; reluctance to provide information or documentation etc.

Annex 5: Synopsis of the Guidance

introduction	Purpose and Scope of the Guidance	The purpose of the Guidance on Correspondent Banking and Expectations for Managing Correspondent Banking Relationships is to assist licensed financial institutions (LFIs) in the understanding and effective performance of their statutory obligations under the legal and regulatory framework in force in the UAE related to correspondent banking, focusing notably on the operationalization of the statutory obligations.
	Applicability	This Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers; and other covered financial institutions not specified above, or any other entities that are licensed or registered by the CBUAE and are engaged in financial activities that fall under AML/CFT/CPF regulations.
	Legal Basis	▪ Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments; ▪ Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organizations and its amendments; ▪ Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution and its amendments; ▪ CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

	Acronyms and Definitions	▪ Several frequently used terms and phrase are defined, and a list of acronyms used in the Guidance is provided.
Correspondent Banking Risk Factors	Respondent Institution's Third-Party Transaction Risk	▪ This section discusses third-party transaction risks and provides further details on nested relationships and payable-through-accounts. ▪ The section also includes best practices to manage third-party risks.
	Respondent Institution's Geographic Risk	▪ This section notes the impact of respondent institution's exposure to jurisdictions with elevated ML/TF/PF risk. ▪ It provides criteria to assess respondent institutions' jurisdictional risks.
	Respondent Institution's Ownership and Management Structures	▪ This section discusses the features of a respondent institution's ownership and management structure that may present increased ML/TF/PF risks. ▪ The section details further criteria related to the respondent institution's legal form, location and reputation of shareholders and beneficial owners, and the presence of Politically Exposed Persons in the senior management or ownership structure.
	Respondent Institution's Products and Services	▪ This section discusses the respondent institution's products and services that may present increased ML/TF/PF risks, because of the potential for intermediation, anonymity, cross-border fund flows, settlement times and terms. ▪ The section also includes information to collect on the purpose of the respondent institution's account and relationship with the correspondent institution.
	Respondent Institution's Customer Base	▪ This section discusses how a respondent institution's customer base impacts its level of ML/TF/PF risk and provides examples of high-risk customers. ▪ This section also includes examples of types of customers to avoid such as shell banks, unlicensed or unregulated banks or non-bank financial institutions.
Risk Mitigation	Enterprise-Wide ML/TF/PF Risk Assessment and Correspondent Banking Risk Assessment	▪ This section discusses how LFIs are required to identify, assess and understand their ML/TF/PF risk exposure to appropriately manage them. ▪ The section also underscores the need for correspondent banks to assess the risk factors of their respondents through a review of their customers, geographies, products and services, and delivery channels risks.
	Standard Customer Due Diligence (CDD), Specific Due Diligence for Correspondent Banking Relationships	▪ This section covers the standard due diligence and CDD measures LFIs should apply before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship, including identification and verification requirements. ▪ The section also discusses specific due diligence required for correspondent banking relationships and other similar relationships, including but information to understand fully the nature of a respondent institution's business, regulatory status and reputation, and an assessment of the respondent institution's AML/CFT controls. ▪ The section also discusses the requirements correspondent banks should have in place when offering correspondent banking services, such as senior management approval and correspondent banking agreement.

	Enhanced Due Diligence for High-Risk Correspondent Banking Relationships	▪ This section details the enhanced due diligence measures applicable to correspondent banking relationships subject to a higher level of scrutiny. ▪ The section provides a list of risk factors for correspondent banking relationships, as well as detailed guidance on potential enhanced due diligence measures.
	Ongoing Monitoring of Correspondent Banking Relationships	▪ The section provides information on how to conduct ongoing due diligence of a correspondent banking relationship to ensure the information is up-to-date and the risks of the relationship aligns with the risks established at onboarding. ▪ The section offers details on the frequency of the review, the account activity review, and best practices related to ongoing communication with the respondent institution.
	Suspicious Activity and Reporting in Correspondent Banking	▪ This section discusses how LFIs should continuously monitor all transactions and customers activities, including those of respondent institutions, to identify suspicious behaviors that may necessitate the filing of a Suspicious Transaction Report (STR), Suspicious Activity Report (SAR), or other report types. ▪ The sections detail the requirements related to transaction monitoring, and suspicious transaction and activity reporting.
	Targeted Financial Sanctions Obligations	▪ This section covers the requirements related to the implementation of Targeted Financial Sanctions obligations by LFIs. ▪ The section includes information about the appropriate steps to screen customers and transactions both for correspondent and respondent institutions.
	Governance and Independent Audit	▪ This section details the governance structure and three lines of defence model to manage the risks posed by correspondent banking relationships. ▪ This section also provides information about the requirements of independent testing and audit to provide assurance to the Board of Directors and senior management of the effectiveness and adequacy of the LFI's governance, risk management, and internal controls.
	Training, Recordkeeping	▪ The training section provides guidance to LFIs on the importance of covering correspondent banking risks as part of the AML/CFT/CPF training program, to ensure that employees are aware of the risks of correspondent banking relationships and equipped to apply appropriate risk-based controls to manage these risks. ▪ The recordkeeping section details the need LFIs for operating correspondent banking services to maintain detailed records associated with the correspondent banking relationships, including the ML/TF/PF risk assessment of the relationship and related mitigation measures.
Annexes	Annex 1	▪ This Annex covers the Global Standards on Correspondent Banking.
	Annex 2	▪ This Annex covers the Correspondent Banking Red Flags.
	Annex 3	▪ This Annex covers the Transition from SWIFT to the ISO 20022 Payment Standard.
	Annex 4	▪ This Annex covers SWIFT and Non-Customer RMA Relationships.

Guidance for Licensed Financial Institutions on Customer Due Diligence/Know Your Customer and Record-Keeping

1. Introduction

Conducting customer due diligence ("CDD") and implementing know your customer ("KYC") and recordkeeping controls are foundational parts of compliance with anti-money laundering, combating the financing of terrorism, and counter proliferation financing ("AML/CFT/CPF"), sanctions, counter-fraud, and antibribery and corruption laws. Specifically, adequate CDD/KYC is the cornerstone for licensed financial institutions ("LFI") when establishing an understanding of customers, including a customer's occupation / profession, business practices, source of income or source of wealth ("SoW"), source of funds ("SoF"), and expected activity for which to detect suspicious activity in the future. According to both the United Arab Emirates ("UAE")'s laws and regulations in addition to financial crimes compliance ("FCC") global standards, all LFIs should have a written CDD/KYC program reasonably designed to mitigate financial crime risks specific to their institution.

It is critical for LFIs to have robust record-keeping requirements and controls to enable an LFI to comply swiftly with information requests from Competent Authorities. These records should be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) and the identification of the persons involved so as to provide information to a requesting authority, conduct lookbacks to identify and remediate compliance gaps, among other measures as necessary. Complete records of customers and transactions should be secure, yet easily accessible, to enable an LFI to work with authorities, regulators and outside consultants in cases where the LFI or its regulator has identified areas needed improvement or remediation.

As such, LFIs should understand the importance of CDD/KYC and the elements that comprise a robust CDD/KYC and record-keeping framework, which should be tailored to the size, complexity, and risk profile of the LFI and the specific characteristics of the LFI's customer base.

1.1. Purpose

Article 44.13 of the *Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") LFIs and registered hawala providers ("RHPs") of their statutory obligations under the legal and regulatory framework in force in the UAE, as detailed in section 1.3 below. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021) (hereinafter CBUAE's *AML/CFT Guidelines for Financial Institutions)* and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, circulars, and notices, and outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF") [2] and industry best practices. LFIs are reminded that this Guidance is intended to supplement CDD/KYC requirements and record keeping requirements set forth in various UAE laws and regulations. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs and RHPs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs and RHPs expected to demonstrate compliance with its requirements within one month from its coming into effect.

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft
[2] For example, please see: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets- 2021.html

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are licensed and/or registered by the CBUAE, in the following categories[3]:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, payment token service providers, registered hawala providers; and
- Insurance companies, agencies, and brokers.

[3] This is a non-exhaustive list; this Guidance applies to any natural or legal person that is a licensed financial institution by the CBUAE.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

- Federal Decree-Law No. (14) of 2018, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments ("CBUAE Law").
- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");
- Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments;
- Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence;
- Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58");
- Cabinet Resolution No. (109) of 2023; and
- CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

This Guidance is designed to complement and clarify the legal obligations laid out in the aforementioned laws, providing LFIs with practical steps to ensure compliance with both the letter and spirit of the law.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
EDD	Enhanced due diligence
EOCN	Executive Office for Control and Non-Proliferation
FATF	Financial Action Task Force
FCC	Financial Crimes Compliance
FIU	Financial Intelligence Unit
KYC	Know your customer
LFI	Licensed financial institution
ML	Money laundering
PEP	Politically exposed person
PF	Proliferation financing
RHP	Registered hawala providers
SAR	Suspicious activity report
SDD	Simplified due diligence
SoF	Source of funds
SoW	Source of wealth
STR	Suspicious transaction report
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSC	United Nations Security Council
UNSCR	UN Security Council Resolution

2. The Role and Significance of CDD/KYC and Recordkeeping

2.1. The Significance of CDD and KYC

The financial sector continues to grow in complexity. The traditional model of a local customer physically opening an account and utilizing products and services at a local LFI is increasingly being replaced by global customer base engaging in large volumes of cross-border transactions. The growing use of online banking allows customers to establish a relationship without ever coming in direct face-to-face contact with an LFI's employees, posing challenges to an LFI's effort to verify the identity of a customer. Adding to these transparency challenges, customers are able to utilize the services of different non-bank and third-party payment processors, potentially in jurisdictions where the customer does not physically reside, as internet- and smartphone-based payment applications are involved in a growing percentage of payment transactions across the globe. In addition, the interconnected elements of the international financial system and global nature of trade, with numerous participants, serve as a justification for a high volume of cross-border payments, often originated electronically and processed straight through without an LFI's intervention or oversight.

Overall, the significance of CDD/KYC is highlighted by the following factors:

- **Sophisticated financial crimes threats:** Criminals are using more sophisticated means to engage in money laundering ("ML"), terrorist financing ("TF"), proliferation financing ("PF") and other financial crimes, while remaining undetected, by hiding behind complex corporate structures or creating false identities through

fake documentation, whether by stealing a real person's identity or by combining real and fake information to create a new identity. Such practices are disruptive and result in significant financial losses for countries, LFIs, and other market participants. Appropriately identifying and verifying customers, *inter alia*, understanding the nature of a customer's business, occupation or profession, source of income or SoW, SoF, expected activity helps LFIs protect their institution against financial crimes.

- Non-compliance risks[4]: Regulatory, reputational, and financial consequences of non-compliance are all serious repercussions resulting from ineffective CDD/KYC controls. Without appropriate CDD/KYC to mitigate against financial crime, LFIs' ML, TF, PF risks and other financial crimes incidents that put an LFI's reputation on the line and can cause financial harm to LFIs in a number of ways. The occurrence of such incidents also associates the LFI in the minds of the public with financial crime. This hurts an LFI through a loss of confidence in the LFI's ability to uphold its commitment to financial integrity. For example, the penalties for non-compliance with regards to maintaining accurate records can range from AED 50,000 to AED 5,000,000.

- Interconnected financial system: The UAE's financial system is increasingly interconnected, and the harm done by illicit actors engaging in financial crime is global, impacting the financial integrity and stability of the international financial system as a whole. Appropriate CDD/KYC controls not only ensures the financial integrity of the UAE's financial system overall, but it also helps LFIs build and maintain trusting relationships with correspondent banks. In the context of correspondent banking specifically, LFIs are expected to conduct sufficient CDD/KYC on customers having direct and indirect access to the account of a correspondent bank.

All of this requires an LFI to remain vigilant when designing, deploying, revising or updating, reviewing, and testing their risk-based CDD/KYC program to ensure that the LFI has an adequate understanding of their customers' identities and expected transactions.

Both "CDD" and "KYC" terms are used interchangeably in this Guidance to refer to an LFI's overall process of verifying the identity of its customers and assessing the risk of engaging these customers, both prior to onboarding and throughout the customer relationship. CDD/KYC is an ongoing, risk-based process to collect, record, and assess relevant information about customers and the customer's related parties, business profile, and transactions to appropriately assign and monitor the ML/TF/PF and other financial crimes risks of the customer. CDD/KYC often happens before a new customer is onboarded, and then at regular intervals throughout a customer's relationship with the LFI. Specifically, LFIs should perform CDD/KYC in the following scenarios:

- When establishing a business relationship: Ahead of establishing a new customer-business relationship and conducting any transactions on a customer's behalf, LFIs should perform due diligence to verify the identity of the customer and its related parties, evaluate the customer's risk profile, understand the customer's business and expected transactions, and ensure the customer is not using a fake identity to access the LFI's products and services.

- To analyse occasional transactions: Certain transactions might require further CDD/KYC measures. For example, transactions over a material monetary amount will require an LFI to review and potentially update a customer's CDD/KYC information.

- When there is suspicious activity: LFIs should implement additional CDD/KYC checks if the customer engages in unusual or potentially suspicious activity that requires further investigation, either due to the presence of a red flag or because the customer is engaging in activity that is inconsistent with their historical profile established at onboarding, or if the customer has been classified as a Related Party to a party of concern identified through transactional review, ownership and control, or public domain. Ultimately if the LFI has reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime, the LFI is required to file a Suspicious Transaction Report ("STR") or Suspicious Activity

Report ("SAR") with the UAE's Financial Intelligence Unit ("FIU").

- **Unreliable identification:** If information a customer has provided is inaccurate, incomplete, or does not meet an LFI's internal requirements for CDD/KYC, LFIs should implement additional CDD/KYC measures to ensure that they can properly establish the identity of the customer and the nature and purpose of the customer's relationship with the LFI.

- **Periodic and trigger-event reviews:** LFIs should implement periodic CDD/KYC reviews for all existing customers with the review frequency corresponding to the risk profile of a customer, as well as one-off reviews due to a particular trigger event occurring related to the customer.

There are four core elements of a CDD/KYC program, each addressed in a further detail below in section 3 *Customer Due Diligence*:

- Identifying a customer and verifying the customer's identity;

- Identifying beneficial owner(s) and key senior personnel of a legal entity customer and verifying their identity using a reliable and independent source;

- Understanding the nature, purpose, and transactional behaviour of a customer relationship to develop a customer risk profile; and

- Ongoing monitoring of customer activity for reporting suspicious transactions and updating customer information and risk profile, as necessary.

---

[4] Recent CBUAE enforcement actions related to AML/CFT/CPF non-compliance can be found at https://www.centralbank.ae/en/ouroperations/enforcement/

2.2. The Importance of Record-keeping

Record-keeping is an essential element of designing and implementing an LFI's internal control framework, and a robust record-keeping program involves the entire LFI. From front-line employees to senior management, all employees should be aware of their LFI's record-keeping policies and understand the importance of storing data in a safe and reliable manner to support any internal processes, as well as regulatory requests and law enforcement inquiries.

Specifically, accurate and up-to-date records enable an LFI's internal stakeholders, regulators, and law enforcement to reconstruct and analyse information and patterns of activity, including the amounts and types of currency involved, if any, as part of any money laundering or terrorist financing investigations.

While there is no definitive set of record-keeping requirements for every customer type, there should be enough documentation that underpins an LFI's onboarding, periodic, and event-driven CDD/KYC review process to demonstrate:

- Why a specific customer was onboarded, with more granular rationales for higher-risk customers;

- How the customer was risk rated, and

- What steps the LFI took to monitor the customer's activity to ensure it corresponded to the customer's risk profile throughout the business relationship with the LFI.

In addition, should a customer's activity rise to a level of a reportable suspicious activity or transaction, LFIs are expected to be able to produce detailed, well-organized supporting documentation if law enforcement has any follow-up inquiries about the customer and activity in question. Poor record-keeping can lead to significant delays during audits and investigations, potentially resulting in missed deadlines for compliance reporting and increased scrutiny from regulators.

As such, adequate record-keeping ensures that all information, including documents and records provided by customers, is preserved in a manner that will allow easy access, when needed, available at all times for inspection as authorized by UAE laws and regulations. Additional detail regarding record-keeping can be found in section 4.

3. Customer Due Diligence

3.1. General Principles

A customer can be anyone who performs a one-off or occasional financial activity or transaction or anyone who establishes an ongoing commercial or financial relationship with the LFI. LFIs should develop and implement appropriate, risk-based, and sufficiently detailed procedures for collecting identifying information and conducting CDD/KYC both at onboarding and on a periodic basis thereafter. These procedures should address, at a minimum:

- Obtaining, analysing, and storing pre-defined types of information about a customer, whether a natural or legal person, its beneficial owners and related parties, the nature of their business, source of wealth, and other data points for purposes of developing a customer risk profile;
- Verifying collected information via documentary or non-documentary means or a combination of both, on a risk-sensitive basis;
- Assigning a risk profile to the customer and adjusting it over time;
- Conducting enhanced due diligence ("EDD") on customers that have been deemed higher risk;
- Refreshing customer information periodically or due to certain incident triggers that are formally documented and defined by the LFI; and
- Conducting ongoing transactions monitoring to verify that a customer's activity is in line with their stated or historic activity and customer profile overall, to update customer information when necessary, and to be able to identify and report suspicious transactions.

In addition to conducting CDD/KYC before or during onboarding and periodically thereafter, LFIs should undertake CDD measures in the following cases:

- Carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked (i.e., a customer initiates several transactions to the same beneficiary or group of the same beneficiaries, which appear to be one transaction broken up into several smaller transactions);
- Carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding AED 3,500;
- Where there is a suspicion of crime; or
- Where there are doubts about the veracity or adequacy of previously obtained customer identification data.

Best Practices to Ensure Consistent Application of CDD/KYC

It is advisable that LFIs with a presence and operations in multiple countries develop standardized, global CDD/KYC procedures to ensure uniform collection, verification, and record-keeping of customer data across all offices, branches, and majority-owned subsidiaries. A global approach to CDD/KYC enables an LFI to have a comprehensive view of its customer base, standardize its risk ratings, and apply uniform controls and analytic tools across different products and jurisdictions.

In the case of where the AML/CFT laws and regulations of an LFI's host country (outside of the UAE) are less stringent than those of UAE, LFIs should ensure that foreign branches and majority-owned subsidiaries in these countries implement the CDD/KYC requirements of the UAE, to the extent permitted under a host country's AML/CFT laws and regulations. This is important as deficient CDD/KYC measures undertaken by an LFI's subsidiary in another country may limit the overall effectiveness of the LFI's AML/CFT controls at the group level.

In addition, it is further recommended that LFIs develop detailed, standardized customer onboarding forms, with the information gathered ultimately forming part of a customer's CDD record. Such forms can be tailored to specific customer types (for example, individuals; trusts; operating companies; publicly listed companies; correspondent banks; investment companies). The selection of these customer types also may be due to the customer's risk, such as if the customer type is known to be higher risk from an FCC perspective and requires specific documents to be collected as part of the LFI's EDD process, or if the customer is lower-risk and requires Simplified Due Diligence ("SDD") as discussed in section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*. LFIs may also seek to streamline their onboarding process and tailor their onboarding forms to those customer types that are most prevalent to their institution (for example, the LFI onboards a high number of insurance companies which represents a significant portion of the LFI's customer base).

LFIs can also choose to develop two types of on-boarding forms, (i) a customer facing form, and (ii) an internal on-boarding form, with the latter being used for additional data gathering, data verification, and analysis performed by the LFI's staff.

It is important to remind staff that CDD/KYC should not be treated as a "check-the-box" exercise. Staff should critically assess information provided by a customer, seek additional information or clarifications, if necessary, raise any identified issues internally to the compliance officer of the LFI. Thereafter, the compliance officer will further investigate and, if necessary, report to the UAE FIU. Typically, it is the first line of defence and front-line (i.e., customer facing) employees who are the most equipped to identify red flags when it comes to CDD/KYC - including by assessing a customer's behaviour at onboarding, reviewing customer documentation for authenticity, and determining whether there are any challenges associated with obtaining a customer's CDD/KYC information. Whenever possible, LFIs should incorporate a "foureye" principle into their CDD/KYC procedures with regard to the verification of customer identification documentation and other CDD/KYC information, including inputting the relevant data into their information technology systems.

Since CDD/KYC is a risk-driven process, as part of CDD/KYC procedures, LFIs should also prescribe situations where a customer should undergo either EDD or SDD. EDD is warranted in situations where a customer typically presents higher financial crime risk, such as relationships with foreign and/or domestic PEPs, relationships with high-net-worth individuals, relationships with persons from high-risk countries, and correspondent banking and other similar relationships. LFI's CDD/KYC procedures should prescribe what additional information the LFI should collect as part of EDD. For further detail on EDD, please refer to section 3.6 *Enhanced Due Diligence for Higher-Risk Scenarios*. SDD can be applied in customer relationships that do not raise red flags and that involve UAE government entities, publicly listed companies, or customers rated as low risk under the LFI's documented customer risk assessment methodology. For further detail on SDD, please refer to section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*.

LFIs should not establish or maintain relationships with customers who are unable or unwilling to provide required CDD/KYC information, whether at onboarding or as a part of ongoing monitoring, periodic review, or event-driven review processes. Where required CDD/KYC processes cannot be completed, including where the customer refuses

to provide CDD/KYC information; the customer provides apparently false or misleading information or documentation; the customer is suspected of engaging in identity theft; or the customer provides information that differs from information obtained during the verification process or subsequent ongoing monitoring; the matter should be escalated through an LFI's appropriate channels to be considered for suspicious activity and transaction reporting. Where discrepancies cannot be resolved, the account should be rejected or restricted and closed in a commercially reasonable manner, taking into consideration the legal requirements applicable to the LFI maintaining the customer relationship.[5]

If an LFI is unable to undertake the CDD/KYC measures on the new or existing customer as outlined in section 3 of the Guidance, the LFI:

- Shall not open the account, commence business relations or perform the transaction; and
- Shall file a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) (whichever is more appropriate) with the UAE FIU.

In case, the LFI has already commenced the business relationship, it shall terminate the business relationship and submit a Suspicious Transaction Report.

---

[5] For example, positive balances on the account(s) or long-term loans and other types of relationships may also present challenges if an LFI decided to offboard a customer for compliance considerations. In such instances, the LFI may consider imposing sufficient restrictions on customer's account(s) to ensure the customer does not commit financial crimes and work towards reducing the balance to zero.

3.2. Customer and Beneficial Owner Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify and verify the identities of all customers, regardless of whether they are establishing a permanent relationship or require a one-off service (such as exchanging currencies or transferring funds to a walk-in customer). The identification and verification requirements also apply equally to natural and legal persons or legal arrangements. Verification of a customer's identity should be performed using documents, data, or information from a reliable and independent source. Examples of reliable and independent sources include official government-issued documents (e.g., passport, license, national ID such as Emirates ID), documents that are certified by a third party (e.g., a notary), and documents issued from a reputable third party or public authority (e.g., utility bills, stock exchange disclosure reports, credit reporting agencies, etc.).

Customer identification and verification allows an LFI to form a reasonable belief that it knows the true identity of the customer. An LFI can use documentary or non-documentary methods of identification and verification, or a combination of both, which is further discussed in section 3.2.4 *Documentary and Non-Documentary Means of Customer Identification and Verification*. The LFI's CDD/KYC procedures should describe these methods in an easy-to-understand manner, including explaining the types of documents an LFI finds acceptable for CDD/KYC. Customers should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, as per Article 4.3 of the AMLCFT Decision, where there is no ML/TF/PF suspicion and a customer's ML/TF/PF risks are assessed to be low, an LFI may complete the verification of the customer's identity after establishing a business relationship, as set forth in section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*. Additional detail regarding customer identification and verification can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.1.[6]

---

[6] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

3.2.1. Natural Persons

Under Article 8.1 of the AML-CFT Decision for natural persons, LFIs should verify an individual's identity using original documents, data or information from a reliable and independent source, as follows:

- Person's name (as identified on an identification card or travel document, and taking a copy of and attaching the copy of the original and valid identification card or travel document);
- Nationality;
- Address (i.e., the permanent residential address);
- Date of birth;
- Place of birth (obtained on the basis of customer risk);
- Name and address of employer;
- For minors (those under the age of 18), documentation to verify the identity and relationship status of parent and/or legal guardian;
- The intended purpose and nature of the business relationship (obtaining, when necessary, information related to this purpose); and
- PEP status, determining whether the customer or beneficial owner is a PEP.[7]

[7] LFIs should obtain approval from senior management if the customer or beneficial owner is a foreign PEP or there are high-risk markers associated with the domestic PEP or head of international organization.

3.2.2. Legal Persons and Arrangements

Under Article 8.1 of the AML-CFT Decision, for legal persons or legal arrangements, LFIs should verify the legal person or arrangement using original documents, data or information from a reliable and independent source, as follows:

- The name, legal form, and memorandum of association;
- Headquarters office address or the principal place of business. (If the legal person or arrangement is a foreigner, it should mention the name and address of its legal representative in the UAE and submit the necessary documents as proof. If the legal person or arrangement is a foreigner without presence in the UAE and does not have a legal representative in the UAE, LFIs should verify the entity using other supporting documents, such as certified incorporation documents, proof of principal place of business, or notarized identification of the entity's controlling individuals.);
- Articles of incorporation (if appropriate, given entity type), bylaws or any similar documents, attested by the competent authority within the UAE;
- Key countries of operations, if any outside of the UAE;
- Names of relevant key controllers or persons holding senior management positions with the legal person or legal arrangement (i.e., a Chief Executive Officer, a Chief Financial Officer, a Chief Operating Officer, a General Partner, a Treasurer, a President or persons with similar authority), and all account signatories or persons otherwise authorized to give instructions on the account(s);

- Information on the ownership and structure of the legal entity, up to an individual level of ownership in accordance with section 3.2.5 *Beneficial Ownership Identification and Verification*;

- The intended purpose and nature of the business relationship (obtaining, when necessary, information related to the purpose of the customer's business relationship with the LFI); and

- The nature of the customer's business.

Depending on its risk assessment, an LFI may develop and implement additional methods of customer identification and verification tied to certain types of customers or financial products. For example, for an individual customer that is onboarding via an online application, an LFI may consider collecting additional information such as a phone number, email address, and/or tax identification number; for a corporate customer that meets a certain risk threshold, an LFI may choose to conduct a site visit. This information may confirm the location of a customer and also serve as an additional verification method should a customer later claim loss of access to the account.

For all relevant individuals associated with (e.g., ultimate beneficial owners ("UBOs") a legal person and persons acting on behalf of the customer), the LFI should verify their identity using the same markers as when verifying individual customer's identity in accordance with section 3.2.1 *Natural Persons*.

3.2.3. Natural Persons Acting on Behalf of the Customer

LFIs are required to verify that any person purporting to act on behalf of the customer is authorized, and LFIs should verify the identity of that person as described above. Persons acting on behalf of customers can range from, for example, lawyers collecting or disbursing funds through their customer's trust accounts to a broker authorized to execute trading orders on a customer's securities account. In these instances, LFIs should seek to obtain documentation establishing the individual's authority to act on behalf of the customer.

Examples of acceptable evidence to establish the individual's authority to act on behalf of the customer include copies of board resolutions, articles of incorporation, other constitutional documents or extracts from company registries, a Letter of Authority, or Power of Attorney. A representative's authority may be implicit if the individual is a director or equivalent officer for a legal person customer, provided the LFI's first line employee has no cause to believe the director is a nominee shareholder acting on behalf of another individual.

3.2.4. Documentary and Non-Documentary Means of Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify each customer and verify the customer's identity using documents, data, or any other identification information from **a reliable and independent source**. This requirement is technology neutral (i.e., LFIs may choose the most appropriate technology adequate to their needs and requirements) and expressly permits LFIs to use documentary as well as non-documentary sources (i.e., information or data) when performing identification and verification. An LFI's CDD/KYC procedures should describe the process and authorized means of verifying a customer's identity, including scenarios, if any, where more than one verification method should be used.

Documentary sources mean that an LFI can use pre-defined types of documents to verify a customer's identity, such as an unexpired government-issued registrations, documentation, or certifications, or documentation issued by other respectable third parties, such as another LFI or public authority.

In the case of verifying an individual, the following are examples of documentary methods (all documents should be valid, unaltered, and unexpired):

- To confirm an individual's identity, an LFI can use an official government-issued identification document, such as a passport, national identification card, so long as the document bears a photograph of the

individual. The use of these documents extends to confirming an individual's nationality and national ID number;

- To confirm the date and place of birth, an LFI can use a birth certificate, a passport, or a national identification card; and

- To confirm residency address, an LFI can ask for a recent (e.g., such as within the last three months) utility bill, correspondence from a UAE government office, tenancy contract, tax statement, a deed for purchase of a residence, or a mortgage statement.

In the case of verifying a legal entity, the following are examples of documentary methods:

- Certificate of incorporation bearing an official government agency seal;

- An official extract from a government-maintained corporate registry; or

- An official government-issued corporate ID;

Considering a wide use of counterfeit and fraudulent documents, an LFI may consider in certain cases, such as onboarding of a non-resident customer, to review more than a single document to ensure it can form a reasonable belief that it knows the true identity of the customer. In addition, LFIs should take reasonable steps to understand those types of identification documents that are legally valid in the relevant jurisdictions of a non-resident customer. If an LFI is unfamiliar with the type of document issued by a foreign government authority, it can ask the customer to provide a notarized or apostilled copy of the document or a copy certified by an embassy official. For non-resident companies with complex ownership structures, the ownership documents of the first layer of the non-resident company should be notarized; the other layers of non-resident companies should have complete incorporation documents, including UBO's information.

Non-documentary sources refer to a range of verification methods other than a government-issued document. For example, for both individual and legal entity customers, it may include:

- Scheduling a face-to-face meeting with a customer;

- Contacting a customer via phone, video conference, mail, or email to confirm they are still valid;

- Checking references with other financial institutions;

- Independently verifying the customer's identity or registration, beneficial ownership, and confirming current active status via public or private databases, corporate registries, or a credit bureau; or

- Visiting the legal person customer's place of business, if practical.

An LFI should consider utilizing non-documentary sources as part of the enhanced due diligence measures undertaken for high-risk scenarios such as: the LFI being unfamiliar with a document presented, the LFI opening the account remotely or via mobile/online application without the customer or its authorized representatives physically present at the LFI, or if an LFI's front-line employees identify red flags during the customer onboarding process.

3.2.4.1. Digital Identification and Verification

Separately from using documentary and non-documentary methods to verify a customer's identity, financial institutions around the world and in the UAE are increasingly relying on digital methods for customer identification and verification. With the rapid development of digital systems and solutions, more and more financial institutions offer customers the ability to be onboarded remotely, without ever visiting a financial institution's office or branches.

Some financial institutions also operate on a fully online basis, without establishing physical locations. Even further, many government authorities, including in the UAE, are moving towards adopting full or partial digital system solutions for issuing, verifying, recording, and securely maintaining individual IDs or corporate registries or certificates.

Thus, it is important for LFIs to develop procedures that are responsive to these new technological advances, but at the same time, consider unique risks that they may represent and ensure that digital identification and verification processes are adequate and appropriate. In order to mitigate common risks associated with implementing digital identification and verification, LFIs should consider adopting measures such as multi-factor authentication and enhanced monitoring for customers whose identities are verified digitally.

Recognizing these developments, Article 8 of the AML-CFT Decision does not impose any restrictions on the form—physical or digital—that identity evidence should take, nor does it impose limitations as to the use of digital identification systems for the purpose of linking a customer's verified identity to a unique, real-life individual, provided this is done using a "reliable" and "independent" source. Digital identification systems use electronic (as opposed to physical) means to assert and prove a person's identity, including through the use of:

- Electronic databases to obtain, confirm, store, and/or manage identity evidence;
- Digital credentials to authenticate identity for accessing mobile, online, and offline applications;
- Biometrics to help identify and/or authenticate individuals; and
- Digital application program interfaces, platforms, and protocols that facilitate online identification and the verification and authentication of identity.

As such, LFIs are permitted to utilize digital identification systems as well as physical forms to perform customer identification and verification, consistent with the expectations set forth in this Guidance and the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*.[8] Thus, although digital means of identification are separate and distinct from the documentary or non-documentary means, the governing principle remains the same – an LFI should not establish a customer relationship or offer services to a person unless the LFI forms a reasonable belief that it knows the true identity of the customer.

In the digital identification context, the requirement that digital source documents, data, or information should be "reliable" and "independent" means that the digital identification system used to conduct CDD/KYC relies upon technology, adequate governance, processes, and procedures that provide an appropriate level of confidence that the system produces accurate results. Reliability and independence in this sense depends specifically on the effective application of mitigating measures to prevent and manage risks related to **identity proofing and enrollment**, such as the risks of an applicant using falsified identity evidence or another individual's identity, as well as risks related to **authentication and identity lifecycle management**, including various risks that bad actors will illicitly obtain an individual's legitimate identity credentials and use them to open an account or obtain unauthorized access to products, services, and data.

See the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, section 4 for additional information regarding the risks and corresponding mitigating measures related to the use of digital identification systems for specified CDD/KYC purposes.

Overall, LFIs should be aware of and utilize the following national-level identification systems and processes that exist or are under development in the UAE:

- **Emirates ID**, the mandatory identity card for all UAE citizens and residents issued by the Federal Authority for Identity, Citizenship, Customs and Ports Security ("ICP"). While issued as a physical card, the Emirates ID uses public key infrastructure to attach individual identities to digital certificates that be used to sign and encrypt data, as well as fingerprint biometrics. LFIs should use the online Validation Gateway maintained by the ICP[9] when verifying an Emirates ID card and should keep a copy of the card and evidence of its digital

verification in accordance with its recordkeeping policies.

- **UAE Pass**,[10] the UAE's first national digital identity and signature solution that enables users – citizens, residents, and visitors in the UAE – to identify themselves to government service providers in all emirates through a smartphone-based authentication protocol and to sign documents digitally with a high level of security. The UAE Pass app uses biometric facial recognition software to verify and register users without requiring an in-person visit to a government services centre.

- **Emirates Facial Recognition**, an initiative launched by the UAE Ministry of Interior and ICP, together with private sector partners. The facial recognition initiative includes a "face fingerprint" system for digital verification of digital transactions and remote identities.

---

[8] Available at https://www.centralbank.ae/media/nphlwxs5/guidance-for-lfis-on-digital-identification-for-customer-due-diligence.pdf
[9] Available at https://icp.gov.ae/en/icp-validation-gateway/
[10] For more information, see https://uaepass.ae/

3.2.5. Beneficial Ownership Identification and Verification

The AML-CFT Law defines a beneficial owner as a "natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement, whether directly or through a chain of ownership, control or other indirect means."

Accordingly, under Article 9 of the AML-CFT Decision, LFIs are required to identify the UBOs of the customer and take measures to verify the identity of such persons using information, data, or statistics acquired from a reliable source, as follows:

- For any **legal person customer:**
    - The identities of all beneficial owners of such customer are defined as all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25 percent or more.
    - Where no individual meets this description (for example, in case of publicly listed entities; non-profit organizations and religious organizations; where no natural person is a UBO by virtue shareholding not exceeding 25%), the LFI is required to identify and verify the identity of the individual(s) exercising control over the organization. This option should be used only as a last resort, however, and when the LFI is confident that no one individual, or small group of individuals, exercises control over the customer.
- For any **legal arrangement customer**:
    - The identity of the settlor, the trustee(s), or anyone holding a similar position, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement.
    - LFIs should also obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment or at the time he/she intends to exercise his/her legally acquired rights.

The UBO of a legal person or arrangement should be an individual. With one exception listed below, another legal person cannot be classified as the UBO of a customer, no matter what percentage it owns. LFIs should continue tracing ownership all the way up the ownership chain until it identifies all individuals who own or control at least 25

percent of the LFI's customer. If the LFI has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the UBOs. The most common method of doing so for a legal person is to identify additional UBOs below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of UBOs at the 10 percent or even *de minimis* percentage thresholds, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD/KYC—in order to conduct sanctions screening or negative news checks.

In case of companies listed on a regulated stock exchange and their majority-owned subsidiaries, it is not necessary for LFIs to identify and verify the identity of a shareholder or UBO, if such information is obtainable from reliable sources, such as exchange-mandated periodic disclosure. However, an LFI may choose to prescribe in its procedures high-risk scenarios where such identification and verification should take place using either documentary or non-documentary means (for example, in case of companies listed on exchanges in jurisdictions subject to economic or financial sanctions or where negative news screening indicate recent changes in the status or ownership of the legal person customer).

UBOs should generally be identified and verified prior to establishing a business relationship, conforming to the same requirements and expectations that apply to the identification and verification of natural person customers, as set forth in section 3.2.1 above. Consistent with those requirements and expectations, including Article 4.3 of the AML-CFT Decision, in exceptional circumstances, where there is no ML/TF/PF suspicion and ML/TF/PF risks are assessed to be low, an LFI may complete verification after establishing a business relationship, as set forth in section 3.5 below. Further information can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.3.1 and 6.3.3,[11] and *Guidance for LFIs Providing Services to Legal Persons and Arrangements*.[12]

---

[11] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf
[12] Available at https://www.centralbank.ae/media/0yljawmh/outreach-presentation-cbuae-amlcft-guidances-for-lfis-prov-serv_-to-lp-laand-real-estate-and-pms-sectors-4-august-2021.pdf

3.3. Establishing a Risk Profile

LFIs should have an understanding of the ML/TF/PF and other financial crimes risks of its customers, also known as a **risk profile** of a customer, and should reflect this risk through assigning a customer risk rating. There is no universal customer risk rating model that can be used across the financial sector, as the assessment of customer risk is LFI-specific and should be based on an analysis of all relevant customer information. LFIs should consider the ongoing publication of information by the CBUAE and other UAE competent authorities to identify, assess, and understand the risks associated with their customers.

At the same time, an LFI's customer risk rating model should be sufficiently detailed to distinguish between variations in ML/TF/PF and other financial crimes of its customers. If such a model is improperly designed or implemented, it can have a significant detrimental impact on the LFI's ability to implement other internal controls and result in an overall weak AML/CFT compliance program. LFIs are reminded, that each customer's ML/TF/PF risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behavior, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, LFIs should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/TF/PF risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/TF/PF risk category. This means that the CDD measures are not to be taken as a static formula but that depending on the risk of a customer the intensity and depth of the CDD measures should vary.

The factors used to create a customer risk profile are substantially similar to the risk categories an LFI uses when assessing its overall risk profile. Thus, an LFI should consider the following risk categories of a customer relationship:

- Products and services;
- Geographic locations; and
- Customer's type of business, customers, and counterparties.

To allow it to establish a proper customer risk profile, and as required under Article 8 of the AML-CFT Decision, LFIs should understand the nature of the customer's business and the nature and purpose of the LFI's relationship with the customer, including the expected uses to which the customer will put the LFI's products or services. One element is the collection and assessment of the customer's ownership structure and UBOs, described in section 3.2.5. In addition, an LFI should collect and document the following types of information for all types of customers as part of the customer onboarding process:

- Nature of customer contact and stated purpose of the account;
- Source of funds and source of wealth;
- Customer occupation (for individual customers) or legal entity type and industry (for legal entity customers);
- Anticipated channels for maintaining the relationship (in-person, telephone, online banking, acting via an authorized representative);
- Anticipated products and services to be used throughout the relationship;
- Anticipated geography of customer's expected activity; and
- Anticipated types and volumes of transactions.

The level and type of other customer information an LFI considers collecting for the purpose of establishing a customer risk rating should correspond with its preliminary assessment of the customer's risk profile. In other words, an LFI's efforts to understand its customer should both reflect and influence the customer risk rating. If an LFI anticipates that a customer has a higher-risk profile, then it should obtain more customer information while, on the contrary, an LFI may determine that less information is required for customers with a lower-risk profile.

For example, inherently, an individual-citizen of the UAE who wishes to open a checking account to collect their salary and make ordinary day-to-day payments will typically represent a lower-risk profile than a branch of a multinational corporation wishing to open an operational account for multiple cross-border payments. Thus, for lower-risk customers, where the LFI may have an inherent understanding of the nature and purpose of the customer risk profile based on the documentation obtained at account opening, there may be no need to collect any further information. The LFI should, however, implement ongoing monitoring even for low-risk customers to ensure that their actual activity corresponds with their expected activity, stated purpose of the account, and nature of the relationship. LFIs should also incorporate ongoing monitoring results into a customer's risk profile. If appropriate for the size and complexity of the LFI, ongoing monitoring may be used to trigger enhanced due diligence reviews or adjust a customer's risk score, in real time.

On the other hand, the higher the anticipated customer risk profile is, the further the LFI should consider collecting additional detailed information about:

- Source of funds ("SoF") and SoW;
- Detailed description of a customer's business operations;
- Anticipated size and/or turnover of a customer's account balances;

- Known or anticipated countries in which the customer will be transacting;
- Known or expected counterparties with whom the customer conducts transactions; and
- Anticipated timing or seasonal adjustments to a customer's transactional activity.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship—together with the ongoing analysis of actual customer behaviour and the behaviour of relevant peer groups—allows the LFI to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. This element of CDD/KYC also informs the LFI's risk-based ongoing monitoring of the customer (see section 3.4) and determining whether SDD or EDD measures may be warranted (see sections 3.5 and 3.6, respectively).

3.3.1. Customer Segmentation

Customer segmentation involves obtaining sufficient information to assign a customer to a customer segment and to calculate an initial risk rating using the LFI's customer risk rating model. The customer segmentation process enables LFIs to appropriately divide customers into categories of risk for defining and calibrating subsequent internal FCC monitoring controls, such as determining whether the customer is subject to EDD, setting up transaction monitoring thresholds, and identifying the customer's periodic review schedule. Customer segmentation also enables an LFI to detect unusual or potentially suspicious activity if the customer engages in a transaction that deviates from what is expected for that particular customer type.

LFIs are encouraged to utilize a wide range of data elements collected as a part of baseline CDD/KYC when developing a customer risk rating and segmentation methodology. A customer's assignment to a given customer segment may automatically result in an elevated customer risk rating and thus trigger EDD and/or specific additional EDD based on the customer's industry or customer type.

3.3.2. Source of Funds and Source of Wealth

If an LFI determines that a particular customer represents a higher-risk relationship and warrants EDD, the LFI should use reasonable means to collect information regarding the customer's SoF or SoW.

- Identifying the SoF means to identify the direct source of the funds that are used to initially fund a customer's account, and any funds that are transacted through the account during the course of the business relationship (such as the customer's salary or the sale of a real estate property).
- Identifying the SoW means to identify the sources that have generated or significantly contributed to the customer's total net worth (such as a customer's inheritance). Where the size of balances in the account is inconsistent with a customer's stated SoW and/or where the initial source of capital for an account is unclear, LFIs should take additional steps to corroborate SoW.
- LFIs should verify the SoF/SoW by obtaining evidence from the customer, with verification requirements increasing relative to customer risk (e.g., customer statements as to employment and income sufficing for lower risk customers and bank or brokerage account statements, housing deeds, or signed court rulings indicating a customer is due compensation for those deemed higher risk).
- Depending on an LFIs risk tolerance and risk management framework, an LFI can also develop policies and procedures that require low and medium risk customers to provide evidence of SoF/SoW.

LFIs should take a critical approach towards assessing and verifying SoF or SoW of a customer, particularly in highest-risk customer relationships. Examples of red flags that an LFI should be aware of include:

- Generic description of SoF or SoW as “inheritance,” “salary,” “income,” “investment,” “self-funding” where customer is unable to provide supporting documentation;
- Apparent inconsistencies in the stated SoF or SoW with the customer profile, such as a newly formed legal entity customer with little or no business history is funding an account with significant funds, or an unemployed customer is frequently depositing large sums;
- SoF or SoW supporting documentation has an opaque ownership structure with multiple ownership layers that lacks a clear rationale;
- Customer identified as a PEP deposits significant funds greatly exceeding their stated salary;
- Customer states that the account will be funded from a third party with no apparent links to the customer;
- Customer indicates that they will transfer the funds from another LFI to close their account;
- Customer wishes to use multiple bank accounts to fund the newly opened account with no apparent business purpose; or
- Funds will be deposited from high-risk countries or countries subject to United Nations and/or UAE sanctions.

3.3.3. Expected Activity

Collecting information regarding a customer’s expected account activity and assessing self-reported expected activity is required for LFIs in order to determine the reasonableness of certain transactions. This can be completed, for example, by comparing activity against a customer’s stated purpose of the account and the transactional activity profile of the customer’s customer type or relevant peer group.

Where a customer’s self-reported expected activity appears to be inconsistent with the stated purpose of the account, or where there is a material discrepancy between the self-reported expected activity and the typical activity of the customer’s peers, LFIs should conduct an additional transaction analysis and collect sufficient information, such as a written explanation from the customer, supporting business documentation, or past financial statements, to understand and corroborate the self-reported activity.

3.3.4. Geographic Information and Assessment of Risks

A geographic component represents an important part of the overall customer risk rating and assessment and should be used when developing a customer risk rating methodology. LFIs should collect and assess the following types of information:

- Jurisdictions where a customer resides, is registered in (either directly or exercises control over a subsidiary), or doing business in or with,
- Jurisdiction(s) of customer’s counterparties; and
- Jurisdictions with which the customer expects to transact.

It is important to assess this information for any high-risk indicators such as follows:

- Presence in or operations with countries with weak regulatory AML/CFT frameworks, as determined by the LFI or as notified by local regulatory or supervisory authorities;

- Presence in or operations with jurisdictions subject to a call for action or under increased monitoring by FATF;
- Jurisdictions subject to United Nations, UAE, or other international sanctions;
- Other indicators of risk in a jurisdiction, such as whether the customer operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, PF, or is known as a financial secrecy or tax haven; and
- Any discrepancies between the location where a customer seeks to open an account and its business activities (e.g., a customer is seeking to open a UAE-based account while not conducting any business activities or residing in the UAE).

LFIs may leverage resources such as FATF's High-Risk Jurisdictions List or any other list provide valuable data for evaluating geographic risk.

3.3.5. Prohibited Customers

It is important for LFIs to clearly document their risk appetite, also referred to as a customer acceptance policy, that formalizes the LFI's posture toward both prospective and current customers. This customer acceptance policy typically identifies the types of customers an LFI will not accept as a matter of policy due to unacceptable legal, regulatory, or reputational risks they pose to the LFI. Thus, LFIs should develop procedures that enable employees to appropriately identify such types of customers and prevent them from onboarding or continuing an existing customer relationship with the LFI. Several examples of such potentially prohibited customers may include the following customer types (although the list is not exhaustive):

- Persons wishing to operate an anonymous account;
- Persons refusing to provide requested CDD/KYC documentation or assist in a CDD/KYC process;
- Persons subject to TFS;
- Shell banks;
- Customer where the LFI is unable to identify the UBO(s);
- Companies issuing bearer shares or owned, in whole or in part, by nominee shareholders;
- Entities the LFI determined are operating in a jurisdiction without an appropriate license or registration; or
- Persons who are the subject of material negative news (such suspected of conducting cyberattacks and associated extortion, or suspected of illegal trafficking (human trafficking, narcotics, illegal wildlife trafficking)).

3.4. Ongoing Monitoring

Under Article 7 of the AML-CFT Decision, all customers should be subject to ongoing monitoring throughout the business relationship, as an element of both continuous CDD/KYC and suspicious activity reporting. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD/KYC during onboarding, and that transactions are normal, reasonable, and legitimate. Depending on the nature, size and complexity of the business, LFIs can use automated, manual or a combination of

both, monitoring systems and processes to conduct ongoing monitoring. However, bigger LFIs are recommended to use automated transaction monitoring systems.

3.4.1. Risk-Based Periodic and Event-Driven Reviews

As a part of the ongoing monitoring process, LFIs should develop standards and procedures outlining the frequency and process of periodic customer reviews, driven by the assigned customer risk rating. For example, an LFI with three customer risk categories of high, medium, and low may establish periodic reviews at the following risk-based intervals: (1) annually for customers rated as high risk; (2) every two years for customers rated as medium risk; and (3) every three years for customers rated as low risk. LFIs should ensure they have procedures and systems in place to track and monitor the progression of periodic customer profile review that are in-process. These customer risk categories and the associated periodic review schedule are not mandatory, and instead, an LFI should develop appropriate parameters for both depending on its overall ML/TF/PF risk assessment.

In addition, LFIs should perform event-driven periodic reviews upon the occurrence of a material change to the customer's profile or other "trigger" event related to the customer, including but not limited to:

- A change in a customer's domicile;
- A change in a customer's legal name through mergers and acquisitions;
- A regulatory filing (e.g., a STR) or inquiry involving a customer;
- Customer transactions are found to have been frequently rejected or blocked by correspondent banks;
- A customer requests to use higher-risk products and services or products or services that are inconsistent with the customer's business;
- Significant and unexplained changes in account activity;
- Changes in employment (considered on the basis of customer risk) or business operation;
- Changes in ownership of a business entity;
- LFI employees become aware that the customer information is outdated or incorrect; or
- Customer produces a true hit against an applicable sanctions, PEP, or negative news screening list.

An LFI may prescribe in its procedures whether an event-driven review re-sets the anniversary date from when the next scheduled periodic review is to be conducted, or whether this "off cycle" event-driven review does not affect the previously scheduled periodic review date.

Both scheduled and event-driven periodic reviews consist of a refresh and assessment of customer data, documents, and risk ratings, including EDD, if applicable. As part of scheduled and event-driven periodic reviews, if a customer's CDD/KYC information has changed, information should be re-validated as correct and up-to-date and signed-off by a designated representative, as necessary.

LFIs should prescribe the processes for conducting a refresh of a customer's CDD/KYC information to address the following:

- Requesting, reviewing, and updating identification information for the customer, UBO(s), and natural person(s) acting on behalf of the customer;

- Conducting an activity review to ensure that the stated/expected activity continues to align with the actual account activity;
- Collection, verification, and review of any EDD, as required;
- Appropriate levels of manager sign-offs in case of a revised customer risk rating following the refresh; and
- Re-screening the name of the customer, UBO(s), natural person(s) acting on behalf of the customer, and other related parties as identified in section 3.8 *Name Screening*.

As outlined in the general principles of CDD/KYC, LFI should not maintain relationships with customers who are unable or unwilling to provide required CDD/KYC or EDD information during periodic review processes. If a periodic review identifies any red flags—such as apparently false information or documentation; discrepancies between the information obtained by the customer and information obtained during the verification process; lack of business justification for a complex ownership structure; or inexplicable volume/value of funds transfers—the LFI should prescribe appropriate escalation channels to investigate the activity and determine whether there are sufficient grounds for filing an STR or SAR. Where discrepancies or red flags cannot be resolved, the account should be rejected or restricted and closed in a commercially reasonable manner.

3.4.2. Incorporation of the Customer Risk Profile into Transaction Monitoring

Both CDD/KYC and transaction monitoring work together and help an LFI form an understanding of their customers. CDD/KYC establishes a customer's risk profile and expected activity against which an LFI can review a customer's actual activity to assess potential variances. Transaction monitoring helps LFIs validate and continue to assess a customer's risk profile on a customer-by-customer and institution-wide basis. Transaction monitoring also feeds an LFI's suspicious activity reporting program and wider AML/CFT compliance program with information by flagging high-risk and potentially suspicious transactions and typologies.

As a basis for an LFI's transaction monitoring program and in accordance with a risk-based approach, LFIs should use a customer's risk profile to inform the degree and nature of transaction monitoring that the LFI applies to its customers. For customers identified as high risk, LFIs may choose to conduct enhanced transaction monitoring. The specific form of enhanced monitoring applied to a high-risk customer will depend on the particular circumstances of the customer relationship. For example, an LFI may set lower alert thresholds for customers who are new to the LFI.

Additionally, an LFI may apply enhanced monitoring on customers who were previously the subject of a STR or SAR filing and suspected of or investigated for potentially suspicious activity. In the case of customers that are identified as low risk, LFIs may consider monitoring and reviewing transactions at a reduced frequency and/or setting lower alert thresholds within their automated transaction monitoring program.

3.4.3. Use of Digital Identification Systems for Ongoing Monitoring

As discussed in section 2 of the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, authentication using a digital identification system establishes confidence that the person asserting identity today is the same person who previously opened the account or other financial service and is, in fact, the same individual who underwent reliable, independent identification and verification at onboarding. In other words, ongoing digital authentication of the customer's identity links that individual with their financial activity. LFIs that use digital identification systems to authenticate the identity of their existing customers as part of account authorization should leverage the data both generated by authentication and other related information (such as geolocation or IP addresses) to support ongoing due diligence and transaction monitoring. For example, an LFI can use a customer's

IP address to identify cases in which a customer may be transacting from a sanctioned, otherwise prohibited, or high-risk jurisdiction. Information generated from an LFI's digital identification systems therefore can be used as part of ongoing monitoring to assess whether a customer's actual activity conforms to the LFI's expectations of normal or typical activity for that customer. LFIs that leverage digital identification systems, as discussed in section 2, are should establish minimum security standards to reduce the likelihood of customer data being lost or compromised.

3.5. Simplified Due Diligence for Lower-Risk Scenarios

As per Article 4.3 of the AML-CFT Decision, an LFI may perform SDD measures in relation to a customer, a beneficial owner of a customer, a natural person appointed to act on behalf of a customer, or a beneficiary or other payee if it is satisfied that the risks of ML/TF/PF are low. The assessment of low risks should be supported by an adequate analysis of risks by the LFI, and the selection of simplified measures should be commensurate with the type and level of risk identified through such risk analysis. In all cases, the LFI should document the details of its risk analysis and the nature of the SDD measures employed.

Where no other countervailing risk factors are present, examples of potentially lower-risk scenarios may include those in which:

- The customer is a UAE government entity, including UAE state-owned enterprises;
- The customer is an entity listed on a stock exchange and subject to regulatory disclosure requirements that identify a customer's UBOs; and
- The customer is rated as low risk under the LFI's documented customer risk rating methodology. The LFI's customer risk rating methodology should meet the minimum requirements as provided for in section 6.1.1 (Assessing Customer and Business Relationship Risk) of the CB Notice No. 3599 of 2023 Regarding Updated Guidelines on Anti-Money Laundering & Combating the Financing of Terrorism & Illegal Organizations for Financial Institutions.

Where an LFI is satisfied that the ML/TF/PF risks are low, the LFI may perform one or more of the following SDD measures, as warranted by the risk analysis:

- Verifying the identity of the customer and any UBO(s) after establishing the business relationship, provided verification is nonetheless completed in a timely fashion (to be documented in the LFI's internal procedures) and appropriate controls are in place to manage the ML/TF/PF risks associated with the customer and the relationship prior to verification;[13]
    - Note that, even where identity verification may be postponed until after the establishment of a business relationship, LFIs should nonetheless obtain basic identifying information (on both natural person and legal entity customers) prior to the establishment of any business relationship.
- Reducing the frequency of updates to CDD/KYC information;
- Reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
- Developing an understanding of the intended nature and purpose of the customer relationship on the basis of the relationship type and the customer's historical transaction activity, rather than by collecting information regarding the intended nature and purpose of the relationship during onboarding or at a periodic or event-driven CDD/KYC refresh.

An LFI should not perform SDD measures where:

- A customer or any UBO of the customer is from or in a country or jurisdiction identified as noncooperative by the FATF;

- A customer or any UBO of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the LFI, or as notified by local regulatory or supervisory authorities; or

- The LFI suspects that ML, TF, or other criminal activity is involved.

---

[13] Such measures may include holding funds in suspense or escrow until verification of identity has been completed or making completion of identity verification a precondition of closing any transaction with or on behalf of the customer.

3.6. Enhanced Due Diligence for Higher-Risk Scenarios

The AML-CFT Law and the AML-CFT Decision impose specific and EDD obligations on LFIs with respect to three classes of customers or transactions:

- Customers that are foreign or domestic PEPs with high-risk factors, which include the direct family members or associates known to be close to the PEPs (Article 15 of the AML-CFT Decision). Ruling family members classified as domestic PEPs should not have a SoW/SoF verification requirement, if the information can be verified through publicly available and reliable sources; and

- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries (Article 15 of the AML-CFT Decision).

The AML-CFT Law and the AML-CFT Decision give special attention to customers in these groups because they are likely to expose LFIs to a heightened risk of money laundering, terrorist financing, and other financial crimes.

In addition to these classes of customers and transactions, for which EDD is mandatory, LFIs are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for ML, TF or PF using appropriate customer risk rating methods, and thus whether the customer warrants EDD. Examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The customer belongs to a higher-risk industry or sector (such as financial services) identified in topical risk assessments, or to an industry or sector identified by the LFI as higher-risk for ML, TF or PF;

- The ownership structure of a legal entity customer appears unusual or excessively complex given the nature of the legal entity's business;

- The legal entity customer is a personal asset-holding vehicle;

- The business relationship is conducted under unusual circumstances, such as significant unexplained geographic distance between the LFI and the customer;

- The legal entity customer has nominee shareholders or shares in bearer form;

- The customer is a cash-intensive business or conducts cash-intensive operations;

- The customer performs complex operations that do not have clear economic objective;

- The customer has a presence in or operations with countries with weak regulatory AML/CFT frameworks, as determined by the LFI or as notified by local regulatory or supervisory authorities;

- The customer operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, or is known as a financial secrecy or tax haven;

- The relationship involves or could involve cash or anonymous transactions;

- The relationship involves or could involve frequent payments received from unknown or unassociated third parties.

As per Article 4.2(b) of the AML-CFT Decision, where the LFI identifies a customer or relationship as presenting higher ML/TF/PF risks, it should apply EDD measures commensurate with those risks. Examples of EDD measures include but are not limited to:

- Obtaining approval from the LFI's senior management to establish or continue a business relationship with the customer;

- Establishing the SoF and SoW of the customer and any UBO of the customer;

- Conducting enhanced monitoring during the course of the business relationship with the customer, including by increasing the degree and nature of transaction monitoring and CDD/KYC updating;

- Requiring the first payment to be carried out through an account in the customer's name with an LFI subject to similar or equivalent CDD/KYC standards;

- Using public or private sources of information (e.g., websites, proprietary databases) to gain a better understanding of the reputation of the customer or any UBO of the customer;

- Commissioning external intelligence reports where it is not possible for the LFI to easily obtain information through public sources or where there are doubts about the reliability of public information; and

- For high net-worth individuals, particularly those utilizing higher-risk products or services or characterized by other markers of heightened ML/TF/PF risk:

    - Independently corroborating information obtained on the SoF and SoW of customers and UBOs against documentary evidence or public information sources;

    - Screening operating companies and individual benefactors contributing to the customer's and UBOs' SoF and SoW; and

    - Scrutinizing transactions relating to customers that have multiple accounts with the LFI or to customers having a common beneficial owner.

In addition, as noted in section 3.2 *Customer and Beneficial Owner Identification and Verification*, if the LFI has followed its standard beneficial ownership identification and verification procedures and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the UBOs. The most common method of doing so is to identify additional UBOs below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of UBOs at the 10 percent or even *de minimis* percentage thresholds, as the customer's risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

Additional examples of EDD measures are provided in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.4.[14]

[14] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

3.7. Non-Face-to-Face Relationships

LFIs should develop policies and procedures to address any specific risks associated with non-face-to-face customer relationships and transactions undertaken in the course of such relationships. Such policies and procedures should be applied when establishing a new customer relationship and when conducting ongoing monitoring and should be at least as stringent as those that would be required to be performed if there was face-to-face contact. Note that relationships in which personal contact between a representative of the LFI and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships for the purpose of this Guidance.

Heightened ML/TF/PF risks may arise from establishing business relationships or undertaking transactions according to instructions conveyed by customers over the internet (absent personal contact via video teleconference), digital application, post, fax, or telephone. An LFI should note that online applications and transactions may pose greater risks than other non-face-to-face business due to the following factors, which taken together may compound the associated ML/TF/PF risks:

- The ease of unauthorized access to the application or online banking platform, across time zones and locations, in situations where third persons received or have stolen customer's log-in credentials;
- The ease of making multiple fictitious applications or requests without incurring additional cost or the risk of detection;
- The ease of concealing a customer's residence in a country subject to United Nations and/or UAE sanctions;
- Individuals being used as a "front" for an unknown third party;
- The absence of physical documents; and
- The speed and often irreversible nature of electronic transactions.

The measures taken by an LFI for verifying the identity of customers and UBOs in the context of non-face-to-face relationships will depend on the nature and characteristics of the product or service provided and the customer's risk profile. Where verification of identity is performed without face-to-face contact (e.g., electronically), an LFI should apply additional checks to manage the risk of impersonation or fraud. The additional checks may consist of robust anti-fraud checks that the LFI routinely undertakes as part of its existing procedures, which may include as appropriate and feasible:

- Telephone contact with the customer at a residential or business number that can be verified independently;
- Confirmation of the customer's address through an exchange of correspondence or other appropriate method;
- Subject to the customer's consent, telephone confirmation of the customer's employment status with his or her employer's human resource department at a listed business number of the employer;
- Confirmation of the customer's salary details by requiring the presentation of recent bank or payment statements where applicable;

- Provision of certified identification documents by lawyers or public notaries;
- Requiring the customer to make an initial payment using a check drawn on the customer's personal account with a bank in the UAE;
- Using biometric data methods such as facial recognition using reliable and independent digital ID systems;
- Requiring customers to use multi-mode authentication factors for access to online banking or digital applications; and
- Conducting a video call with the customer.

When engaging in non-face-to-face relationships, LFIs should continue to explore digital identification systems that can enable remote customer identification and verification, support remote financial transactions, and otherwise facilitate non-face-to-face business relationships and transactions, please see section 3.2.4.1 *Digital Identification and Verification*. Given the evolution of digital identification technology and the emergence of consensus-based open-source digital ID technical standards, non-face-to-face interactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place may present a standard level of risk, and may even present a lower level of risk where higher assurance levels are implemented and/or appropriate control measures are present.

See the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, section 4 for specific risk mitigation measures and strategies that can help ensure that a digital identification system is suitably "reliable" and "independent" in this sense.

3.8. Name Screening

An LFI should screen the following parties against relevant ML/TF/PF information sources (such as negative media databases), databases of known PEPs, and internal watchlists (such as lists of customers previously exited or denied onboarding for financial crime reasons) prior to a customer's onboarding and keep records of true matches as part of the KYC documentation:

- All customers, regardless of risk rating or risk profile;
- UBOs of legal entity customers;
- Natural persons appointed to act on behalf of the customer (see section 3.2.3);
- Names of relevant persons holding senior management positions with the legal person (such as directors, partners, authorized signatories, and senior executives); and
- Natural persons having executive authority over customers that are legal arrangements.

All LFIs are required to fully comply with the obligation to implement all necessary measures without delay as described in the Cabinet Decision No. (74) of 2020, Executive Office for Control & Non-Proliferation ("EOCN")'s *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*[15] and the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*, and *Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanctions Screening.*[16]

This means that all LFIs should maintain awareness of sanctions promulgated by the UNSC as well as the UAE sanctions list(s) published on the EOCN's website. In addition, LFIs should register on the EOCN's website to receive automated email updates about changes to the UAE sanctions list.

With respect to these sanctions lists, the parties listed above should be screened prior to a customer's onboarding and on an ongoing basis thereafter. The results of screening and assessment by the LFI should be documented. When there is a confirmed match against an existing customer, an LFI should freeze without delay (within 24 hours) all funds and other assets. When a partial name match is identified, the LFI should use reasonable information (e.g., open-source information, media articles, commercial data bases) to cross verify customer data to rule out false positive" results. An LFI should report all confirmed or potential matches, for existing and potential customers, in addition to the actions the LFI has taken to suspend or freeze the relevant funds or transactions, as required, utilizing the UAE FIU's online reporting platform, goAML, within five business days of the required action taken.

---

[15] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.
[16] Available at: https://www.centralbank.ae/en/cbuae-amlcft

3.9. Customer Rejection and Exit

Under Article 14.2 of the AML-CFT Decision, LFIs should not deal with any person on an anonymous basis or any person using a fictitious name and using pseudonyms, fictitious names, or numbered accounts without the account holder's name. In addition, as outlined in section 3.3.5 *Prohibited Customers*, an LFI may decide that certain types of customers are outside of its risk appetite and should not be onboarded or that ongoing relationships with such customers should be terminated.

Prior to establishing a business relationship, if an LFI has any reasonable grounds to suspect that the assets or funds of a customer are the proceeds of crime or related to the financing of terrorism, the LFI should reject the business relationship and, per Article 17 of the AML-CFT Decision, file an STR or SAR with the UAE FIU.

As per Article 13.1 of the AML-CFT Decision and Article 15 of Cabinet Decision 74, if an LFI is unable to undertake the CDD/KYC measures described in this Guidance, or identifies a confirmed match to a party included on applicable sanctions lists, the LFI should:

- Not onboard the customer;
- In case of a confirmed match, freeze without delay and without giving a notice to the customer, funds owned or controlled, wholly or jointly, directly or indirectly, by a sanctioned person or by a person or organization acting on behalf of or at the direction of a sanctioned person;
- Exit the relationship if one has been established;
- For insurance operators, not make any payment to a payee or beneficiary under the customer's policy or other insurance relationship; and
- Maintain all related records (see section 4 *Record-keeping* below).

As per Article 15 of Cabinet Decision 74, in case of a confirmed match, the LFI should freeze without delay and without giving a notice to the customer, funds owned or controlled, wholly or jointly, directly or indirectly, by a sanctioned person or by a person or organization acting on behalf of or at the direction of a sanctioned person and notify EOCN within five business days.

In addition, the LFI may decide to add the customer, its UBOs, directors, and managers to the LFI's internal watchlists to ensure the individual is prevented from being onboarded with the LFI in the future. The LFI should also determine whether the circumstances warrant the filing of an STR or SAR. The LFI is required to document the customer rejection or exit rationale(s) as well as the exit policy and procedures.

3.10. Third-Party Reliance

Third-party reliance enables an LFI to rely on the CDD measures carried out by another vendor. However, it is important to remind LFIs that the Compliance Officer of the LFI bears the ultimate responsibility to verify and validate CDD information provided by the third-party. LFIs are required to submit a non-objection certificate/letter of the third-party to the Central Bank for approval for such services. Third-party reliance does not apply for outsourcing, service providers, vendors or agency relationships of the LFI.

LFIs are permitted to rely on certain third parties – financial institutions or designated non-financial businesses and professions ("DNFBPs") – to perform the following elements of CDD measures:

a) Identifying a customer and verifying a customer's identity using reliable, independent source documents, data, or information.

b) Identifying a beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that an LFI is satisfied that it knows the identity of the beneficial owner.

c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

When entering into a third-party reliance arrangement, LFIs should ensure the third party has appropriate measures in place to comply with the UAE's AML/CFT regulatory requirements. LFIs should ensure that the following criteria are met:

a) An LFI relying upon a third party should immediately obtain the necessary information concerning elements (a) to (c) as outlined above, as well as all other identification data and necessary information collected during the CDD.

b) LFIs should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

c) LFIs should satisfy itself that the third party is regulated, supervised or monitored for ML/TF/PF compliance, and adheres to the CDD and record-keeping requirements outlined in the AML-CFT Decision.

d) When determining in which countries the third party that meets the conditions can be based, LFI should have regard to information available on the level of country risk.

The third-party reliance does not apply in the context of outsourcing, service provider, or agency relationship. The third-party reliance is only acceptable in the case of reliance on other financial institutions or DNFBPs conducting CDD, which typically means that the third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying financial institution. In contrast, in the scenario in which the outsourced entity applies the CDD measures *on behalf of* the delegating financial institution, in accordance with its procedures, the delegating LFI should ensure control of the effective implementation of its CDD procedures by the entity/agent.

Article 19 of the AML-CFT Decision states that even in situations where reliance on third parties is permitted, the ultimate responsibility for CDD measures remains with the LFI relying on the third party. Therefore, third-party reliance in no way relieves the relying LFI of performing other CDD measures, including understanding a customer's expected activity, determining whether customers are high-risk, and assessing whether a customer's transactions constitute suspicious activity. LFIs should understand that use of third-party reliance is likely to be a focal point of any supervisory engagement with an LFI.

LFIs that decide to utilize reliance on third parties should develop clear policies and procedures outlining when it is acceptable to do so and what steps an LFI's staff should follow to satisfy themselves that the requirements in sections (a)-(d) above are met.

Whichever methods are utilized, LFIs bear the ultimate responsibility of ensuring that the third parties adhere to the statutory CDD and record-keeping requirements of the UAE, and that the CDD documentation provided are complete, adequate, valid, authentic, and meets the UAE AML/CFT/CPF requirements.

An LFI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the third-party upon demand and without undue delay.

Whenever an LFI has doubts as to the reliability of the third-party, it should take reasonable steps to review the third-party's ability to perform its CDD duties. If the LFI intends to terminate its relationship with the third-party, it should immediately obtain all CDD information from the third-party. If the LFI has any doubts regarding the CDD measures carried out by the third-party previously, the LFI should perform the required CDD as soon as reasonably practicable.

Best Practices for Third-Party Reliance

- The relying LFI and the third party should have an agreement in place (such as a service-level agreement) that acknowledges the existence of reliance and outlines its major principles and considerations, including the roles and responsibilities of the LFI and the third party and the nature of the CDD and record-keeping requirements to be fulfilled by the third party.
- Third-party reliance arrangements should be approved and overseen by an appropriate senior managing official within the LFI.
- The LFI's policies and policies should document the third-party reliance arrangement and should establish review procedures for evaluating the relationship on an ongoing basis, including the adequacy of the third party's CDD and record-keeping measures.
- LFIs should conduct a periodic review of the third party to ensure that it continues to conduct CDD and record-keeping in a manner as comprehensive as the LFI and is consistent with the UAE's AML/CFT regulatory requirements.
- The LFI should assess negative news and any enforcement action regarding AML/CFT deficiencies or violations involving the third party to determine whether it should engage or continue to engage in a third-party reliance arrangement with the entity.
- The LFI's risk assessment should identify reliance on third parties and evaluate the risk exposure posed by the LFI's third-party reliance arrangements.
- LFIs should consider terminating reliance with a third party that fails to apply adequate CDD on their customers or otherwise does not meet the LFI's AML/CFT requirements.

4. Record-keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs should maintain detailed records associated with their ML/TF/PF risk assessment and mitigation measures as well as records, documents, data, and statistics for all financial transactions, all records obtained through CDD/KYC measures, ongoing monitoring, sanctions screening, account files and business correspondence, copies of personal identification documents, and STR or SAR files and results of any analysis performed. LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions in order to provide, if necessary, evidence for prosecution of criminal activity. LFIs are also required to make records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five years from the latest date of the following trigger circumstances: from the date of completion of the transaction; termination of the business relationship with the customer; completion of the inspection by the CBUAE; issuance of a final judgment of the competent judicial authorities; or liquidation, dissolution, or other form of termination of a legal person or arrangement. Although the statutory retention period mandates that LFIs maintain records for at least five years, LFIs may retain records for a longer period of time at their own discretion. An LFI may also consider conducting a formal annual review of its recordkeeping policies to ensure ongoing compliance with applicable laws and regulations, as well as allowing an LFI to stay up to date with record keeping best practices, technology, and data security standards.

Accordingly, an LFI should maintain the following types of records as part of a well-documented AML/CFT compliance program:

- Policies, procedures, and controls: LFIs should maintain its AML, CFT, CPF, sanctions, fraud, and other applicable policies, procedures, and controls, standard operating manuals, internal guidance, and logs documenting any changes made to these documents over time.

- Customer information: LFIs are generally required to verify a customer and related parties' identity before doing business with the customer and keep records of the verification process performed. As such, LFIs should maintain records related to identifying and verifying individual or legal entity customer and related parties' information, such as a customer's name, address, date of birth, and the date of a customer's incorporation.

- Customer screening: LFIs should maintain any records generated during screening a customer and related parties against lists of Politically Exposed Persons ("PEPs"), adverse news, and UNSC and UAE local sanctions, as well as results of any investigations or alert resolution (e.g., in case of confirmed true hits or false positives).

- Other customer due diligence records: LFIs should maintain records related to the CDD/KYC process, such as documents pertaining to a customer's source of wealth ("SoW"), results of internal enhanced due diligence ("EDD"), regulatory requests, and decisions/approval to onboard or offboard a customer by senior management/Board of Directors.

- Documentation on third-party reliance: LFIs should maintain policies, procedures, and service-level agreements describing an LFI's reliance on a third party to conduct CDD/KYC on the LFI's behalf, including the roles and responsibilities of the third party and the LFI's process to determine the adequacy of the third party's CDD/KYC controls.

- Transactions: LFIs should keep records of all transactions with their customers, including the type and amount of the transaction, the date, the parties involved, and any underlying documentation the LFI may have requested from a customer. These transactions include those executed or processed by the LFI, whether domestic or international in nature, and irrespective of the type of customer and whether a business relationship is maintained with the LFI.

- External and internal compliance reports: LFIs should prepare and maintain periodic internal compliance reports and metrics, such as results of monitoring activities, independent audit reports, risk assessments, documents related to employee background investigations (i.e., documentation of the Know Your Employee ("KYE") process), incidents or violations reports, trends in customer risk ratings, and other analysis. This extends to SAR and STR reports submitted to the FIU and supporting documentation specific to the filing, including any follow-up requests from the FIU. LFIs should also keep detailed records of any root cause analyses and remediation actions taken to address identified shortcomings in the LFI's AML/CFT compliance program.

- **Investigation records**: LFIs should keep records of all internal investigations regarding their customers, their activities, or any red flags, including any evidence collected and the ultimate resolution.

- **Information that is not processed**: LFIs should keep records of any information they receive that is not processed or that may raise a red flag, such as customer requests for omitting or altering information to avoid scrutiny and attempted transactions.

- **Regulatory requests and remediation:** If a regulatory authority requests information from an LFI or issues an assessment report indicating deficiencies in the LFI's policies and controls, the LFI should keep records of the information provided and any actions taken as a result of the regulatory engagement.

- **Training Monitoring**: LFIs should keep records of employee training (for example, the date the training took place, a list of the participants who received the training, and the topics that were covered as part of the training). LFIs should also keep records related to the effectiveness of their training programs, such as employee test scores and feedback, to improve future training efforts.

LFIs should document in their internal procedures how they store these records and whether this takes place in a physical or digital form and whether the records stored are originals or scanned/electronic copies. For further details, see the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 9.[17]

---

[17] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

Annex 1. CDD/KYC Red Flags

LFIs should establish a list of ML/TF/PF red flags associated with collecting and updating CDD/KYC information on a customer. The following is a list of representative ML/TF/PF red flags that, when identified, may warrant additional scrutiny. LFIs should tailor these ML/TF/PF red flags to their specific institution and to specific products and services that the LFI offers.

Red flags related to a customer's CDD/KYC information

- A customer provides misleading, inaccurate, or incomplete information.

- A customer's identity cannot be verified, or the customer is unable or refuses to provide all of the information and documents required by the LFI.

- There are inconsistencies in the identification documents provided by the customer, such as a customer provides onboarding documents that contain variations in the customer's name.

- A customer produces documents that appear to be counterfeited or altered.

- A customer's home or business telephone is disconnected.

- The information that is provided by a customer is inconsistent with other (publicly available) information.

- There are apparent inconsistencies in the stated SoF or SoW with a customer profile, such as a newly formed legal entity customer with little or no business history is funding an account with significant funds.

- A customer, related parties, and/or beneficial owners are associated with material negative news.

- A customer has no record of past or present employment experience.

- A customer is a trust or shell company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- A business (legal entity)'s shareholder composition is overly complex.
- A customer indicates they intend to engage or are currently engaging in high-risk products or services (such as high-volume and high-value cross-border funds transfers) without a reasonable explanation.
- A customer wishes to use multiple accounts to fund the newly opened account with no apparent business purpose.
- A customer's account will be funded from a third party with no apparent links to the customer.

Red flags related to a customer's behavior

- A customer demonstrates a defensive stance to the LFI's CDD/KYC questions.
- A business (legal entity) is reluctant to provide information about the nature of its business, anticipated account activity, prior banking relationships, the names of its related parties and UBOs, or other information as required by the LFI.
- A customer provides an insufficient explanation on their SoF and/or SoW (as "inheritance," "salary," "income," "investment," "self-funding"), or is uncomfortable providing SoF and/or SoW information to the LFI.
- Examples of high-risk SoF/SoW scenarios include declaring proceeds from a cash-intensive business without documentation, claiming large inheritances without proof, and using virtual assets not linked to a declared identity.
- A customer provides information that is misleading, inaccurate, or incomplete on its UBOs.
- A customer indicates that they intend to engage with jurisdictions that the LFI knows to be at a higher risk for ML/TF/PF or non-cooperative by the FATF.
- A customer asks to be exempted from the LFI's reporting or recordkeeping requirements.
- A customer makes inquiries about the LFI's AML/CFT and Sanctions Policy.

Red flags related to a customer's transactions

- A customer's transactions (volume or value) exceed the expected activity established at onboarding.
- There is a sudden change in the customer's pattern of activity or transactions. For example, a customer engages in large and/or rapid movement of funds and/or rounded transactions that is inconsistent with the customer's historical profile.
- A customer uses products or services that are unusual for that customer type. For example, the customer is a small convenience store engaging in custodial and brokerage services.
- A customer engages in transactions between parties that are not usually connected (e.g., a textile producer transacting with a luxury car dealer) and who were not disclosed to the LFI at onboarding.
- A customer engages in transactions inconsistent with what is expected from the customer's expected declared business revenue or customer's income/employment information. For example, a customer makes

high-value transactions, but the LFI's CDD/KYC information indicates the customer is unemployed.

- A customer begins to send or receive transactions to or from a financial secrecy or tax haven, or to or from a higher-risk geography which is inconsistent with the customer's business and information provided at onboarding.

- A customer is not responding to an LFIs' request for information related to a transaction within the timeline stipulated in the request.

- A customer transacts outside an area near their home address, employment address, or business address which is inconsistent with the customer's information provided at onboarding.

Annexure 2: Synopsis of the Best Practice

introduction	Purpose and Scope of the Guidance	The purpose of this Guidance is to assist LFIs overall process of verifying the identity of its customers and assessing the risk of engaging these customers, both prior to onboarding and throughout the customer relationship, as well as implementing a record-keeping controls framework.
	Applicability	▪ This Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, virtual asset service providers, registered hawala providers; and insurance and re-insurance companies, agencies, and brokers.
	Legal Basis	▪ Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments; ▪ Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organizations and its amendments; ▪ Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution and its amendments; ▪ Cabinet Resolution No (109) of 2023 ▪ Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58").
	Definitions and Acronyms	▪ Several frequently used terms and phrase are defined, and a list of acronyms used in the Guidance is provided.
The Role and Significance of CDD/KYC and Record-keeping	The Significance of CDD and KYC	▪ Overview on the sophisticated financial crime threats and noncompliance risks that are mitigated by well-designed CDD/KYC programs. ▪ Scenarios when LFIs should conduct CDD/KYC measures. ▪ Core elements of a CDD/KYC program.

	The Importance of Record-keeping	▪ Overview of which data is kept in a customer record and that the data should be maintained to allow for ready and easy access, when necessary, by competent authorities.
Customer Due Diligence	General Principles	▪ An overview of the procedures and guidance an LFI should implement to collect identifying information and conduct CDD/KYC both at onboarding and on a periodic basis.
	Customer and Beneficial Owner Identification and Verification	▪ An overview on identifying and verifying natural persons, legal persons and arrangements, natural persons acting on behalf of the customer, and beneficial ownership identification and verification. ▪ The section includes examples of national-level identification systems that exist in the UAE.
	Establishing a Risk Profile	▪ An overview of how LFIs may undertake customer segmentation to underpin the risk profile. ▪ The importance of obtaining, on the basis of risk, customer source of funds and source of wealth, expected activity levels, and geographic information. ▪ The necessity of an LFI to clearly document its risk appetite.
	Ongoing Monitoring	▪ An overview of risk-based periodic and event-driven customer profile reviews. ▪ Guidance regarding incorporation of the customer risk profile into transaction monitoring.
	Simplified Due Diligence for Lower-Risk Scenarios	▪ The section includes examples of lower-risk customers and related CDD/KYC measures that an LFI may perform in those cases.
	Enhanced Due Diligence for Higher-Risk Scenarios	▪ The section includes examples of higher-risk customers / scenarios and related CDD/KYC measures that an LFI may perform in those cases.
	Non-Face-to-Face Relationships	▪ Discussion of the risks that arise from establishing business relationships or undertaking transactions according instructions conveyed by customers in a non-face-to-face capacity and measures an LFI can take to mitigate the associated risks.
	Name Screening and Customer Rejection and Exit	▪ An overview of customer data that an LFI should include in screening prior to onboarding and on an ongoing basis. ▪ A discussion of common circumstances under which an LFI should reject a customer seeking to open an account or exit an existing customer relationship.
	Third-Party Reliance	▪ An overview of when LFIs may rely on third-parties to perform CDD measures and guidance on how LFI should manage the relationship between it and the third party.
Record-keeping	Record-keeping	▪ This section discusses how an LFI should maintain detailed records associated with their ML/TF/PF risk assessment and mitigation measures as well as records, documents, data, and statistics for all financial transactions, all records obtained through CDD/KYC measures, ongoing monitoring, sanctions screening, account files and business correspondence, copies of personal identification documents, and STR or SAR files and results of any analysis performed. ▪ This section includes examples of types of records an LFI should maintain as part of a well-documented AML/CFT/CPF compliance program
Annex 1	CDD/KYC Red Flags	▪ The annex provides several examples of red flags related to a customer's CDD/KYC information, behavior, and transactions.

The United Arab Emirates' Virtual Assets Travel Rule

Application

Status: In-Force

The following provisions shall apply with respect to Virtual Asset Service Providers within the territorial scope of the UAE Federal and Emirate Laws, any Free Zone and any Financial Free Zone.

Risk Based Approach (Section on Risk Assessment, Enhanced Due Diligence measures)

Article no. (1)

1. This Article applies in relation to any Virtual Asset Transfer which is:

    a. Executed by a Virtual Asset Service Provider acting on behalf of the Originator and in which a Virtual Asset is transferred to a Virtual Asset Service Provider acting on behalf of the Beneficiary; or

    b. Received by a Virtual Asset Service Provider acting on behalf of the Beneficiary and in which a Virtual Asset is Received from a Virtual Asset Service Provider acting on behalf of the Originator.

    Transaction fees (also known as 'gas fees') are excluded from the scope of this Article.

2. Subject to paragraphs 6 to 8 and 11 of this Article, a Virtual Asset Service Provider must not Execute a Virtual Asset Transfer unless it collects, verifies and provides the following data immediately and securely to accompany the Virtual Asset Transfer:

    Information accompanying all qualifying Virtual Asset Transfers should always contain:

    a. the full name of the Originator and the Beneficiary;

    b. the Wallet or Account number of the Originator and the Beneficiary, and in the absence of such Wallet or Account number for either the Originator or the Beneficiary the Virtual Asset Transfer must include a unique reference number that allows the traceability of the transaction from the Originator to the Beneficiary;

    c. the Originator's address, national identity number or travel document number, customer identification number, date and place of birth.

3. Where several Virtual Asset Transfers are Executed on behalf of a single Originator for receipt by one or more Beneficiaries, and are batched into a single transfer before being sent to the Virtual Asset Service Provider of the Beneficiaries, the transfer must include the information set out in paragraph 2 above for each Virtual Asset Transfer.

4. The Originator's Virtual Asset Service Provider must, before executing a Virtual Asset Transfer to another Virtual Asset Service Provider, ensure that the Virtual Asset Service Provider is appropriately regulated in accordance with applicable law in the jurisdiction in which it is incorporated and located, and must not Execute a Virtual Asset Transfer to a Virtual Asset Service Provider which is not appropriately regulated either in the UAE or outside the UAE.

5. A Virtual Asset Service Provider which Executes a Virtual Asset Transfer to another Virtual Asset Service Provider must ensure that the information referred to in paragraph 2 of this Article which accompanies the

Virtual Asset Transfer has been verified by the Originator's Virtual Asset Service Provider.

6. In the case of domestic Virtual Asset Transfers and where the verified data referred to in paragraph 5, is available to the Beneficiary's Virtual Asset Service Provider by other means:

   a. the Originator's Virtual Asset Service Provider is only required to include the Wallet or Account number or the unique reference number of the Virtual Asset Transfer, provided that this number allows the tracing of transactions to the Originator and the Beneficiary; and

   b. for such a Virtual Asset Transfer, the Beneficiary's Virtual Asset Service Provider or Supervisory Authority may request the full set of data in paragraph 2(a), (b) and (c), in which case the Originator's Virtual Asset Service Provider must provide such data within three (3) working days of receiving the request from the Beneficiary's Virtual Asset Service Provider or the concerned Supervisory Authority.

7. The Originator's Virtual Asset Service Provider (VASP A) must have risk-based policies and procedures to identify circumstances where the Beneficiary's Virtual Asset Service Provider (VASP B) is unable to receive any of the information listed in paragraph 2 sent by VASP A.

8. Where VASP A identifies circumstances where VASP B is unable to receive any information as set out in paragraph 7, VASP A must use best efforts to establish, as soon as reasonably practicable, alternative communication with VASP B which enables VASP B to receive the information listed in paragraph 2. If VASP A is unable to establish such communication, then VASP A must consider whether to decline the execution of any further Virtual Asset Transfer to VASP B, having regard to:

   a. if it is subject to the Decision, the risk assessments carried out by VASP A which must be appropriate and proportionate to the level of risks posed from the relevant relationship and transaction, as stipulated under Article 4 of the Decision; and

   b. its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the Virtual Asset Transfer.

   In assessing the level of risk, VASP A must take account of factors including:

   a. the purpose and nature of the relationship with the customer;

   b. the value of the Virtual Asset Transfer and any other Virtual Asset Transfer which appears to be linked;

   c. the frequency of Virtual Asset Transfers initiated or Received by the customer; and
   d. the reputation and regulated status of VASP B, and the adequacy of the financial crime laws applicable in the jurisdiction from which VASP B operates.

   VASP A must take into account its communications, if any, with VASP B when conducting and reviewing its risk assessment of VASP B pursuant to Article 4 of the Decision.

9. Virtual Asset Service Providers which Receive a Virtual Asset Transfer on behalf of a Beneficiary must take reasonable measures to identify Virtual Asset Transfers that lack the required Originator information or required Beneficiary information, which may include real-time monitoring where feasible or post-event monitoring.

10. For Virtual Asset Transfers of daily aggregated amounts of AED 3,500 or more for both occasional transactions or customers, and for customers with whom a Virtual Asset Service Provider has an ongoing business

relationship, a Virtual Asset Service Provider which Receives a Virtual Asset Transfer on behalf of a Beneficiary must verify the identity of the Beneficiary in accordance with Section 3 of the Decision, if the identity has not been previously verified.

11. If a Virtual Asset Transfer is for a value of less than the daily aggregated amounts of AED 3,500 for both occasional transactions or customers, and for customers with whom a Virtual Asset Service Provider has an ongoing business relationship, Virtual Asset Service Providers must comply with paragraph 2 of this Article but without the need to verify the validity of the referred data, unless the Virtual Asset Service Providers has suspicions concerning the commission of a crime.

12. Virtual Asset Service Providers which Receive Virtual Asset Transfers on behalf of Beneficiaries must, to address the possibility of receiving a Virtual Asset Transfer which lacks the required Originator or Beneficiary information, have risk-based policies and procedures determining when to:

    a. reject (if technically possible) the Virtual Asset Transfer;

    b. permit Execution of the Virtual Asset Transfer;

    c. delay Execution of onward transfer of the Virtual Asset;

    d. return the Virtual Asset to the Virtual Asset Service Provider from which it was Received;

    e. as appropriate report to a Supervisory Authority;

    f. as appropriate take follow-up action (including following the Supervisory Authority's response to any report made by the Virtual Asset Service Provider).

13. Where the Virtual Asset Service Provider of a Beneficiary becomes aware that any required Originator or Beneficiary information is missing, the Virtual Asset Service Provider must:

    a. request that the Virtual Asset Service Provider from which it Received the Virtual Asset Transfer provide the missing information; and

    b. consider whether:

        i. to delay making the Virtual Asset available to the Beneficiary until the information is received; and

        ii. if the information is not received within a reasonable time, to return the Virtual Asset to the Virtual Asset Service Provider from which the Virtual Asset was Received.

14. In deciding what action to take for the purposes of paragraphs 12 and 13, the Virtual Asset Service Provider must have regard to:

    a. if it is subject to the Decision, the risk assessments carried out by the Virtual Asset Service Provider under Article 4 of the Decision; and

    b. its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the Virtual Asset Transfer.

    In assessing the level of risk, the Virtual Asset Service Provider must take account of factors including:

a. the purpose and nature of the business relationship with the Beneficiary; and

b. the value and frequency of the Virtual Asset Transfer and any other Virtual Asset Transfer which appears to be linked.

15. The Virtual Asset Service Provider of the Beneficiary must report to its Supervisory Authority any systemic failure by a Virtual Asset Service Provider of the Originator to provide any required Originator information as well as any steps the Virtual Asset Service Provider of the Beneficiary has taken in respect of such failures.

16. Virtual Asset Service Providers must keep all the collected information about the Originator and the Beneficiary, in accordance with the provisions of Article No. (24) of the Decision.

Article no. (2)

1. This Article applies in relation to any Virtual Asset Transfer in which a Virtual Asset is Received or transferred by an Intermediary Provider. Transaction fees (also known as 'gas fees') are excluded from the scope of this Article.

2. An Intermediary Provider must confirm and verify the regulatory status of both the Originator's and Beneficiary's VASPs before facilitating a transfer, and must maintain a log of all Virtual Asset Transfers, including attempts that were rejected due to non-compliance.

3. An Intermediary Provider must ensure that all Originator and Beneficiary information that accompanies a Virtual Asset Transfer is retained by it in accordance with the provisions of Article No. (24) of the Decision.

4. An Intermediary Provider must transfer all Originator and Beneficiary information received by it from the Originator's Virtual Asset Service Provider (whether or not regulated as a Virtual Asset Service Provider in the UAE) to the Beneficiary's Virtual Asset Service Provider (whether or not regulated as a Virtual Asset Service Provider in the UAE) or to another Intermediary Provider.

5. Where technical limitations prevent the required Originator or Beneficiary information accompanying a Virtual Asset Transfer Received by an Intermediary Provider from remaining with a corresponding Virtual Asset Transfer Executed by that Intermediary Provider, the Intermediary Provider must keep a record of all the information received from the Originator's Virtual Asset Service Provider or another Intermediary Provider, in accordance with the provisions of Article (24) of the Decision.

6. Intermediary Providers must take reasonable measures, which are consistent with straight-through processing1 , to identify Virtual Asset Transfers that lack required Originator information or required Beneficiary information. Where an Intermediary Provider becomes aware that any required Originator or Beneficiary information is missing, the Intermediary Provider must:

   a. request that the Virtual Asset Service Provider or Intermediary Provider from which it Received the Virtual Asset Transfer provide the missing information; and

   b. consider whether:

      i. to delay the onward transfer of the Virtual Asset until the information is received; and

      ii. if the information is not received within a reasonable time, to return the Virtual Asset to the Virtual Asset Service Provider or Intermediary Provider from which the Virtual Asset was Received.

7. An Intermediary Provider must have regard to:

    a. if it is subject to the Decision, the risk assessments carried out by the Intermediary Provider under Article 4 of the Decision; and

    b. its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the Virtual Asset Transfer.

    In assessing the level of risk, the Intermediary Provider must take account of factors including:

    a. the purpose and nature of the business relationship with the Originator's Virtual Asset Service Provider, if any; and

    b. the value of the Virtual Asset Transfer and any other Virtual Asset Transfer which appears to be linked.

8. An Intermediary Provider must report to its Supervisory Authority any systemic failure by a Virtual Asset Service Provider (whether or not regulated as a Virtual Asset Service Provider in the UAE) or by another Intermediary Provider to provide any required Originator or Beneficiary information as well as any steps the Intermediary Provider has taken in respect of such failures.

Article no. (3)

1. This Article applies to any Virtual Asset Transfer which is:

    a. Executed by a Virtual Asset Service Provider acting on behalf of the Originator and in which a Virtual Asset is transferred to an Unhosted Wallet; or

    b. Received by a Virtual Asset Service Provider acting on behalf of the Beneficiary and in which a Virtual Asset is transferred from an Unhosted Wallet.

Transaction fees (also known as 'gas fees') are excluded from the scope of this Article.

2. A Virtual Asset Service Provider must perform enhanced due diligence on a customer before sending or receiving a Virtual Asset Transfer to or from an Unhosted Wallet on behalf of that customer, including by requesting additional identification documentation and source of funds verification from that customer.

3. Virtual Asset Service Providers which Receive Virtual Asset Transfers on behalf of Beneficiaries from an Unhosted Wallet must, to address the possibility of receiving a Virtual Asset Transfer which lacks the required Originator or Beneficiary information, have risk-based policies and procedures determining when to:

    a. reject (if technically possible) the Virtual Asset Transfer;

    b. permit execution of the Virtual Asset Transfer;

    c. delay (if technically possible) execution of onward transfer of the Virtual Asset;

    d. return the Virtual Asset to the Unhosted Wallet from which it was Received;

    e. as appropriate report to its Supervisory Authority;

f. as appropriate take follow-up action (including following the Supervisory Authority's response to any report made by the Virtual Asset Service Provider).

4. Where the Virtual Asset Service Provider of a Beneficiary Receives a Virtual Asset Transfer on behalf of a Beneficiary from an Unhosted Wallet and becomes aware that any required Originator or Beneficiary information is missing, the Virtual Asset Service Provider must:

   a. take reasonable steps to obtain the missing information from the Beneficiary; and

   b. consider whether:

      i. to delay (if technically possible) the execution of the Virtual Asset until the information is received; or

      ii. to return the Virtual Asset to the Unhosted Wallet from which the Virtual Asset was Received.

5. If a Virtual Asset Service Provider is instructed by the Originator to Execute a Virtual Asset Transfer to an Unhosted Wallet, the Virtual Asset Service Provider must:

   a. request from the Originator such information specified in Article 1(2) as it does not already hold; and

   b. in the event that the Virtual Asset Service Provider does not receive the information requested it must decline to Execute the Virtual Asset Transfer.

6. In deciding what action to take for the purposes of paragraphs (3) – (5), the Virtual Asset Service Provider must have regard to:

   a. if it is subject to the Decision, the risk assessments carried out by the Virtual Asset Service Provider which must be appropriate and proportionate to the level of risks posed from the relevant business relationship and transaction, as stipulated under Article 4 of the Decision; and

   b. its assessment of the level of risk of money laundering, terrorist financing and proliferation financing arising from the Virtual Asset Transfer.

In assessing the level of risk, the Virtual Asset Service Provider must take account of factors including:

   a. the purpose and nature of the business relationship with the customer, if any;

   b. the value of the Virtual Asset Transfer and any other Virtual Asset Transfer which appears to be linked; and

   c. the frequency of Virtual Asset Transfers initiated or Received by the customer.

7. The Virtual Asset Service Provider must hold any information collected pursuant to paragraphs (2) and (6) above in accordance with Article 1(16).

Article no. (4)

1. The Virtual Asset Service Provider must:
   a. Take into account all information from both the Originator and Beneficiary sides of the Virtual Asset Transfer in order to determine whether a suspicious activity or suspicious transaction report is to be filed

in accordance with the Decision; and

b. If it is decided, in accordance with the Decision, to file a suspicious activity or suspicious transaction report regarding the Virtual Asset Transfer, the STR/SAR must be sent to the UAE Financial Intelligence Unit, attaching all relevant transaction information.

Article no. (5)

No UAE Virtual Asset Service Provider shall Execute a Virtual Asset Transfer of a Privacy Token due to their potential use in obscuring transaction details, thereby increasing the risk of money laundering, terrorist financing and proliferation financing. For the avoidance of doubt, this prohibition shall not prevent a Person from performing Virtual Asset activities for which it is licensed or regulated by a Supervisory Authority.

Article no. (6)

The Supervisory Authorities may provide joint guidance on interpretation of this Document.

Definitions

Account: means a proprietary record maintained by a Virtual Asset Service Provider of an entitlement or interest that a customer has to or in a Virtual Asset.

Beneficiary: means a Person who is the intended recipient of a Virtual Asset Transfer.

Decision: means Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, as amended by Cabinet Resolution No. (24) of 2022 Amending some provisions of Cabinet Resolution No. (10) of 2019 On the Executive Regulations of Federal Decree-Law No. (20) of 2018 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations, and as may be further amended from time to time in due course.

Distributed Ledger Technology: means a class of technologies that supports the distributed recording of encrypted data across a network and which is a type of decentralized database of which there are multiple identical copies distributed among multiple participants and accessible across different sites and locations, and which are updated in a synchronized manner by consensus of the participants, without involving a central authority or intermediary using a system other than the network or another distributed ledger.

Execute a Virtual Asset Transfer: means to effect or make available, or materially contribute to effecting or making available, a Virtual Asset Transfer. Execution has a corresponding meaning.

Financial Free Zone: means any free zone subject to the provisions of Federal Law No (8) of 2004, regarding Financial Free Zones, as may be amended or substituted from time to time.

Intermediary Provider: means a Virtual Asset Service Provider which Receives and Executes Virtual Asset Transfers on behalf of one or more Virtual Asset Service Providers.

Originator: means a Person who performs a Virtual Asset Transfer of a Virtual Asset for which it is the holder, or instructs a Virtual Asset Service Provider to perform such Virtual Asset Transfer on its behalf (by

having the Virtual Asset Service Provider initiate, facilitate, effect or direct such transfer).

Person: means any natural or juridical person.

Privacy Token: means a Virtual Asset which, by design, disguises or otherwise obfuscates, or purports to hide or obfuscate, details of its Token holder or transaction history which would otherwise be visible to third parties through the Distributed Ledger Technology on which the Virtual Asset is hosted.

Receive a Virtual Asset: means to receive the Virtual Asset (or an interest in it) for the benefit of a customer (i) as recorded to an Account or (ii) to a Wallet operated, held, maintained or controlled by the Virtual Asset Service Provider for the purposes of a service it provides to the customer.

STR: means a suspicious transaction report, as defined in the Decision.

Unhosted Wallet: means a Wallet or address, including a 'smart contract' or similar decentralised technology[2] , which is operated, held, maintained or engaged with by a Originator or Beneficiary without the provision of any service to the Originator or Beneficiary by another third party, except the provision of the technology (including provision of updates to the technology, and support to address any technical issues with the technology) to a Originator or Beneficiary which enables them to safeguard or safeguard and administer their own Virtual Assets or the cryptographic keys for such Virtual Assets or the Wallet in which they are held, or to transfer such Virtual Assets on their own behalf.

Virtual Asset: means a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. "Virtual Asset" does not include:

- any digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the UAE's legislative framework; or
- virtual assets which (a) is unique and not fungible with any other Virtual Assets (b) relate to an identified physical or digital asset; and (c) are used to prove the ownership of, entitlement to or provenance of such asset.

Virtual Asset Service Provider: means any natural or legal person who as a business conducts one or more of the following activities or operations for or on behalf of another Person (each, a **Virtual Asset Service**):

- exchanges between a Virtual Asset and a fiat currency;
- exchanges of one Virtual Asset for another;
- participation in and provision of financial services related to an issuer's offer and/or sale of a Virtual Asset;
- safekeeping and/or administration of Virtual Asset or instruments enabling control over virtual assets; and
- Virtual Asset Transfers.

Virtual Asset Transfer: means an act initiated by the Originator or Beneficiary or on either of their behalves of transferring a Virtual Asset(s) or an interest in a Virtual Asset(s), whether or not such transfer is performed using Distributed Ledger Technology and irrespective of any underlying obligations between the Originator and the Beneficiary.

Wallet: means a Distributed Ledger Technology address or account to which a Virtual Asset is attributed from time to time and in relation to which a Virtual Asset Transfer is performed.

Guidance for Licensed Financial Institutions on Risks Related to Proliferation Finance

Effective from 7/11/2025 **Status:** In-Force

1. Introduction

The proliferation of weapons of mass destruction ("WMD") poses a significant threat to global security and stability, as it is regarded not only as a matter of national security for individual countries, but also as a threat to international peace and prosperity. Over the last years, the global community has taken significant steps to prevent the spread of WMD, including through the adoption of a range of international treaties, resolutions, and initiatives. However, the financing of WMD proliferation remains a significant challenge on the world stage, and financial institutions ("FIs") play a critical role in detecting and disrupting illicit financing for proliferation activities.

FIs are key players in the countering the financing of proliferation ("CPF") regime, as they are uniquely positioned to identify, prevent, and disrupt illicit financing for proliferation activities, including by detecting and preventing the collection, storage, movement, and use of funds that may support the development or acquisition of WMD or their delivery systems. It is, therefore, paramount for FIs in the UAE to identify, understand, assess, and mitigate the risks stemming from proliferation financing activities as part of an effective anti-money laundering, counter the financing of terrorism, and countering the financing of proliferation ("AML/CFT/CPF") regime in the UAE.

1.1. Purpose

Article 44.13 of the *Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") and registered hawala providers ("RHPs") of their statutory obligations under the legal and regulatory framework in force in the UAE, as detailed in section 1.3 below. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019), *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021) as amended,[1] and Executive Office for Control & Non-Proliferation ("EOCN") *Guidance on Counter Proliferation Financing for Financial Institutions ("FIs"), Designated Non-Financial Businesses and Professions ("DNFBPs"), and Virtual Asset Service Providers ("VASPs")*, published in November 2022.[2] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, circulars, and notices, and outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF")[3], other competent authorities and international best practices. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and

regulatory framework currently in force. As such, LFIs and RHPs should perform their own assessments of the manner in which they should meet their statutory obligations consistent with their risk exposure.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft
[2] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=1852fefa-f0a7-4629-9515-78c13fd7354e
[3] For example, please see: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, payment token service providers, registered hawala providers; and
- Insurance companies, agents, and brokers.

CBUAE reaffirms its unwavering commitment to combating Proliferation Financing ("PF"), violations and any instances of non-compliance associated with this Guidance document with respect to PF and other related laws and regulations in the UAE pertaining to counter-illicit finance-related efforts may be subject to the measures outlined in Articles 13 and 14 of the AML-CFT Law.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");

(ii) Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;

(iii) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments;

(iv) Cabinet Resolution No. (50) of 2020, concerning the control list annexed to Federal Law No. 13 for 2007 relating to commodities subject to import and export control; and

(v) Federal Decree Law No. (43) of 2021 on the commodities subject to non-proliferation; and

(vi) Notice No.: CBUAE/BIS/2023/5960, which mandates all LFIs to take steps to identify, assess, understand, and mitigate PF risks on an institutional level.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the UAE
CDD	Customer due diligence
CFP	Countering proliferation financing
CFT	Countering the financing of terrorism
CFZ	Commercial Free Zone
DNFBP	Designated Non-Financial Business Profession
DPMS	Dealers in precious metals and stones
DPRK	Democratic People's Republic of Korea (North Korea)
EDD	Enhanced due diligence
EOCN	Executive Office for Control and Non-Proliferation
FATF	Financial Action Task Force
FANR	Federal Authority for Nuclear Regulation
FCA	Federal Customs Authority
FDI	Foreign direct investment
FI	Financial institution
FFI	Foreign financial institution
FFR	Funds freeze report
FIU	Financial Intelligence Unit
FTZ	Free trade zone
GCC	Gulf Cooperation Council
HIO	Heads of international organizations
ICP	Federal Authority of Identity, Citizenship, Customs and Port Security
KYC	Know Your Customer
LFI	Licensed financial institution
ML	Money laundering
MOCD	Ministry of Community and Development
MOD	Ministry of Defence
MVTS	Money Value Transfer Services
NPO	Nonprofit organizations
PEP	Politically exposed person
PF	Proliferation financing
PNMR	Partial name match report
RBA	Risk-Based Approach
RFR	Reasons for reporting
RHP	Registered hawala providers
SAR	Suspicious activity report
SIRA	Security Industry Regulatory Agency
STR	Suspicious transaction report
TBML	Trade-based money laundering
TCSP	Trust and company services providers
TF	Terrorism financing
TFS	Targeted financial sanctions
UHP	Unlicensed Hawala Providers
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution

VA	Virtual assets
VASP	Virtual Asset Services Providers
WMD	Weapons of Mass Destruction

2. Understanding Proliferation Financing

PF is providing financial services for the transfer and export of nuclear, chemical, radiological, or biological weapons and their means of delivery. It involves, in particular, the financing of trade in proliferation sensitive goods, but could also include other financial support to individuals or entities engaged in proliferation.

For the purposes of this Guidance, it is also important to understand the difference between proliferation financing ("PF"), money laundering ("ML"), and terrorist financing ("TF"), as each of these forms of illicit finance have distinct objectives and methods.

PF, as defined by the FATF, refers to the "risk of raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes)." PF-related funding might occur at several stages and by various means, including through raising, moving, and using funds.

ML, on the other hand, is the process of disguising the proceeds of illicit activity as legitimate funds, which is further defined in Article 2 of the AML-CFT Law, and takes place across three stages—placement, layering, and integration. ML has a number of characteristics in common with PF, as the methods used to conceal funds, such as the use of shell and front companies and complex ownership structures, may be similar to the methods used in ML. In addition, the proceeds of crime might also be used to finance proliferation activities.

Finally, TF is the act of providing funds or financial services to support terrorist activities, which consists of any of the acts mentioned in Articles 29 and 30 of Federal Law No. (7) of 2014 on Combating Terrorism Offences, as amended. Similar to PF, TF-related funding occurs across the stages of raising, moving, and using funds.

3. Understanding Risks Related to Proliferation Finance

The FATF's *Guidance on Proliferation Financing Risk Assessment and Mitigation*[4] defines PF risk as a function of three factors: threat, vulnerability, and consequence. In the context of proliferation financing, these concepts can be understood as follows:

- **Threat** refers to a person or group of people, object, or activity with the potential to cause harm to, for example, the state, society, the economy, or the international order, including persons or entities designated under PF-related targeted financial sanctions ("TFS") ("PF-TFS"), their facilitators, their funds, as well as past, present, or future PF activities.

- **Vulnerability** refers to something that can be exploited by a threat or that may support or facilitate the breach, non-implementation, or evasion of PF-TFS. For a country, vulnerabilities may include weaknesses in the laws or regulations that comprise a country's national CPF regime, or contextual features of a country that may provide opportunities for designated persons and entities to raise or move funds or other assets. For private sector firms, vulnerabilities may include features of a particular sector or a financial product or type of service that make them attractive to a person or entity engaged or seeking to engage in the breach, non-implementation, or evasion of PF-TFS.

- **Consequence** refers to the impact or harm that PF may cause, including the effect of the underlying proliferation activity on financial systems and institutions as well as the economy and society more generally. Specific consequences may include outcomes where funds or assets are made available to designated persons and entities, which could ultimately allow them to obtain materials or systems for

developing and maintaining illicit nuclear, chemical, radiological, or biological weapons (or their means of delivery), or where the frozen assets of designated persons or entities are used without authorization for proliferation financing. The breach, non-implementation, or evasion of PF-TFS may also cause reputational damages to the country, relevant sector(s), or private sector firms, and may lead to sanction designations by the UN and/or national authorities.

To be in a position to effectively understand and mitigate PF risks, LFIs should, first, identify the extent to which state and non-state actors attempt to abuse their institutions to procure or raise funds for the procurement or development of WMD and the corresponding systems of delivery. Second, LFIs should assess the policies, procedures, and controls in place to counteract those threats and undertake remedial actions where they identify gaps or weaknesses in the design or operating effectiveness of their CPF program. Finally, LFIs should continually monitor for emerging risks associated with PF, identifying trends, new methods used, and actors involved in potential PF activity, and should monitor for changes in applicable regulations and typologies so as to update and adjust their CPF programs accordingly.

Please note, Annex 2 presents a detailed list of PF typologies identified by the FATF; Annex 3 presents PF-related risk indicators concerning customer risk, transactional risk, and risks specific to the maritime sector and trade finance activity identified by the EOCN; Annex 4 presents potential indicators of sanctions evasion activity identified by the FATF, and Annex 5 presents PF sanctions evasion red flags and typologies issued by the EOCN.

The following sections expand on a variety of specific threats and vulnerabilities associated with PF.

---

[4] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.pdf

3.1. Threats Related to Proliferation Finance

PF threats and related sources of funding mainly derive from three categories, i.e., financial products directly related to trade in PF-sensitive goods; revenue-raising activities; and the use of financial and corporate structures to support movement of funds and cash.

- Regarding financial products directly related to trade in PF-sensitive goods, the main threats derive from trade finance-related financing, the use or misuse of financial products and services, and trades related to persons or entities subject to United Nations Security Council ("UNSC") Resolutions ("UNSCRs").

- Second, revenue-raising activities may include the use of UAE-based front companies to raise revenue for sale of oil and petroleum-based products, cross-border smuggling of cash, gold or other high value goods to support state PF activities, real estate industry and/or related trades owned or operated by or on behalf of persons or entities subject to UNSCRs, cybercrime, restaurants or small to medium businesses which are largely cash-based businesses, wildlife trafficking, and drug trafficking.

- Finally, financial and corporate structures to support movement of finances and cash may also be sources of PF, including the use of cryptocurrencies, use of local branches of banks and financial institutions based in countries of PF concern, use of hawala or bartering systems of value transfer, ease of use of front companies and shell corporations, use of Money Services Businesses for cash transfers for procurement of goods, and use of professional intermediaries and firms to mask end users.

PF threats can be posed by state and non-state actors attempting to obtain WMD and their delivery systems or raising, moving, or using funds to procure such items. Under the FATF Standards, PF threats and CPF requirements are provided under the following UNSCRs:

- UNSCR 1540 (2004), regarding **non-state actors**;

- UNCSRs 1718 (2006), 2087 (2013), 2094 (2013). and 2270 (2016), regarding **the Democratic People's Republic of North Korea ("DPRK" or "North Korea")**; and

- UNCSR 2231 (2015), regarding the **Islamic Republic of Iran ("Iran")**.[5]

For the purpose of identifying, understanding, and assessing PF risks facing their own institutions, LFIs can include other applicable threats distinct from designated person and entities, such as key sectors, products, and services that are prone to abused for PF purposes.

Annex 1 presents a detailed list of potential threats related to products and services that LFIs might offer, or that otherwise can be used for PF purposes.

---

[5] On 18 October 2023, the FATF communicated to all member countries that UNSCR 2231 (2015) related to Iran has ceased to apply, which means FATF Rec. 7 no longer requires countries to apply TFS to individuals and entities designated under said Resolution, and FATF Rec. 1 no longer requires countries to assess and mitigate risks related to individuals and entities subject to said Resolution as they related to the breach, non-implementation and evasion of PF-TFS.

3.2. Vulnerabilities Related to Proliferation Finance

3.2.1. Trade Finance

Trade-based money laundering ("TBML") and other forms of trade-based illicit finance involve the manipulation of trade transactions to disguise the true nature of the underlying financial activity and/or the identities of trade participants. In the context of PF, TBML may be used to facilitate the purchase or transfer of goods and services that are relevant to the development or acquisition of WMDs. This may involve the use of false invoices, undervalued or overvalued goods, or misrepresentations of the nature or purpose of the transaction. Notably, PF is often difficult to detect because illicit procurement looks like international trade, and the relevant networks must interact with the legitimate financial system.

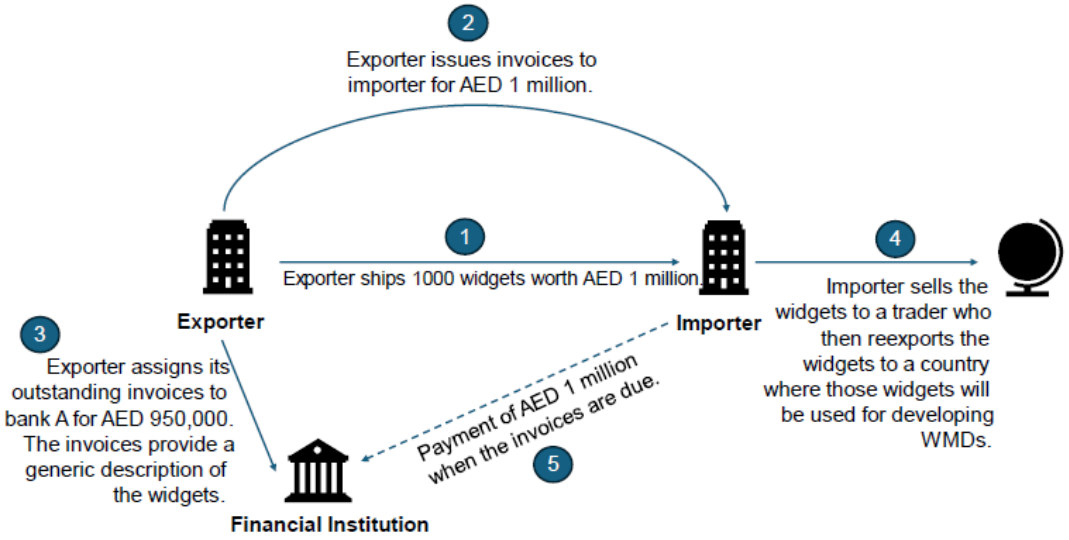


Figure 1 – This figure illustrates factoring a trade finance product utilized in a trade transaction. In this example, the exporter assigns the invoices issued to the importer to a financial institution that pays the exporter and will get paid by the importer when the invoices are due. In this case, the financial institution lacks visibility of the trade transaction between the importer and the third-party trader.

LFIs involved in trade-finance activities may be at a heightened risk for PF activity, given the magnitude of funds involved in international transactions, the volume of international trade (especially that associated with prominent port facilities), and the ability of illicit actors to hide dual-use or restricted goods within shipments or to deliberately mis-identify them in accompanying trade documentation. As such, techniques involved in the exploitation of trade finance transactions for PF may resemble other types of illicit finance such as TBML, including over and under-invoicing and, perhaps most importantly in the PF context, the substitution of controlled or restricted goods for similar non-controlled or restricted goods.

3.2.2. Correspondent Banking

Correspondent banking relationships involve the provision of financial services by one FI, the correspondent institution, to another, the respondent institution. In this capacity, the correspondent institution may provide an array of services including cash management, international wires, check clearing, and letters of credit. Correspondent banking services may present heightened risk insofar as it can involve the rapid and repeated transfers of large quantities of funds on behalf of parties that are not the direct customers of the correspondent institution.

In the PF context, risks associated with facilitating international wires, check clearing, or providing trade facilities for dual-use, sensitive, or restricted goods underscore the importance of customer due diligence ("CDD")/know-your-customer ("KYC") measures, including the application of CDD/KYC as well as specific and enhanced due diligence ("EDD") measures, as appropriate, to respondent institutions.

Correspondent relationships can introduce additional illicit financing risk when one or more of the conditions below are present:

- **Foreign jurisdictions, including high-risk jurisdictions.** Correspondent relationships involving provision of financial services to foreign financial institutions ("FFIs") present heightened risks, as FFIs may not be subject to the same or equivalent laws, regulations, and supervisory expectations as domestic FIs, specifically for FFIs located in high-risk jurisdictions, as determined by the LFI. Accordingly, such FFIs may not have adequate CDD/KYC controls in place to detect PF. These risks can be heightened when involving foreign non-bank FIs, where compliance, transaction monitoring functions, and screening systems may be less robust. As such, it is important to know and understand the CDD/KYC controls of FFIs and foreign non-bank FIs in order to appropriately assess the risk posed by these correspondent relationships.

- **Foreign transfers.** Correspondent banking relationships enable foreign transfers or the cross-border movement of funds between FIs across different jurisdictions. In this case, proliferators can exploit correspondent banking relationships to engage in complex layering schemes, involving multiple intermediary banks across different jurisdictions or conducting circuitous transactions across different jurisdictions, thereby making it difficult to trace the source and end use of these funds.

- **Third-party transactions**. Correspondent relationships involving the execution of payments or the provision of other services for the respondent institutions' customers may allow a respondent FI's customers access to the international financial system without first obtaining—or ensuring that the respondent FI has obtained—an adequate understanding of the customer's identity and risk profile or ensuring the application of appropriate controls to manage such risks. As such, it is important to know and understand the location of those respondent institution customers, along with their business lines, and the underlying business relationship to determine whether such transactions are at a heightened risk for PF.

- **Nested relationships.** A correspondent FI may not be aware that the respondent FI is permitting other FIs to transact through the primary respondent FI's correspondent account or relationship. These "downstream" or "nested" relationships place additional layers of intermediation between the correspondent FI and the underlying customer. This further increases the risk of a respondent FI allowing a customer access to the financial system without a proper understanding of the customer and/or adequate controls in place to

manage that customer's risk.

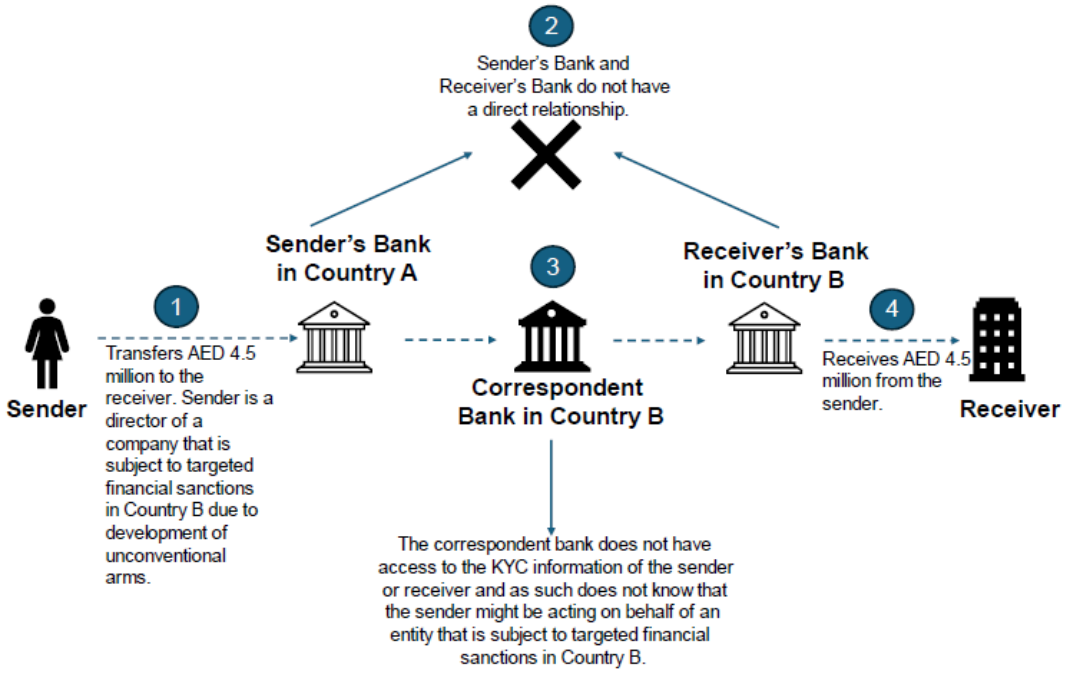


Figure 2 – This figure illustrates a correspondent banking payment flow. In this transaction, the sender's bank does not maintain a relationship with the receiver's bank. Therefore, to transfer the funds, the sender's bank uses a correspondent bank to transfer the funds to the receiver's bank.

3.2.3. Hawala and Other Alternatives to Traditional Banking Products and Services

The FATF defines hawala providers (and other similar service providers) as money transmitters, particularly those with ties to specific geographic regions or ethnic communities, that arrange for the transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. While hawala providers —also known as hawaladars—may often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other methods, including trade, cash, and other methods that do not include the actual transfer of funds.

3.2.3.1. Registered Hawala Providers

CBUAE permits legitimate hawala activity as an important element in its support of financial inclusion, and hawala activity is regulated by the Registered Hawala Providers Regulation issued by CBUAE (Circular No. 24/2019).[6] Under the Regulation, it is not permitted to carry out hawala activity without being registered with the CBUAE.

While registration requirements mandate that such entities maintain compliance with all UAE-related AML/CFT laws and regulations, RHPs may service jurisdictions or customer segments (or "end-users") that may present heighted PF risks. Moreover, similar to money value transfer services ("MVTS") and exchange houses, RHP are considered high-risk despite the relatively small size of the sub-sector and should therefore be subject to enhanced procedures and controls as laid out in this Guidance and in the CBUAE's *Guidance for Registered Hawala Providers and Licensed Financial Institutions Providing Services to Registered Hawala Providers*.[7]

[6] Available at: https://www.centralbank.ae/media/qv1loqzu/registered-hawala-providers-regulation_0.pdf
[7] Available at: https://centralbank.ae/media/b50eai4u/amlcft-guidance-for-registered-hawala-providers-and-lfis-providing-services-to-registered-hawala-providers.pdf

3.2.3.2. Unlicensed or Unregistered Hawala Providers

Unlicensed hawala providers ("UHP") are not permitted to operate in the UAE as they may service customer populations or jurisdictions without maintaining controls or compliance functions/reporting requirements, putting their transactional activity outside the purview of competent authorities such as supervisors and law enforcement. To the extent that actors involved in PF may seek to obscure the origins, destinations, and characteristics and details surrounding their transactions, UHP may provide an attractive vehicle for the transfer of illicit funds to high-risk PF jurisdictions, or for the purchase and payment of dual-use, sensitive, or restricted goods.

LFIs should therefore have in place policies, procedures, and controls to detect and prevent relationships or transactions with or for UHP and, where appropriate, file a suspicious transaction report ("STR") or suspicious activity report ("SAR") with the UAE FIU.

3.2.3.3. Other Alternative Remittance Systems and New Technologies

Other alternatives to banking products and services—such as those facilitated by online MVTSs, money services businesses, exchange houses, and VASPs—can be used by individuals and entities that seek to abuse the financial system to further WMD goals. Illicit actors typically aim to exploit institutions that are perceived as having little or no AML/CFT/CPF controls for the purposes of transferring value to proliferation actors, and certain payment channels, discussed below, are vulnerable to abuse by PF actors, largely due to their rapid money transmission services across international borders.

- Money Services Businesses and Exchange Houses: As part of proliferation networks, illicit actors may exploit money services businesses and exchange houses to transfer, domestically or cross-border, cash to individuals or entities owned or controlled by proliferation actors. Illicit actors also exchange currency to procure or assist in procuring dual-use, controlled, or prohibited goods and services on behalf of proliferation networks. This can also involve structured payments to organised crime networks involved in revenue-raising activities.

- Virtual Asset Service Providers:[8] Illicit actors are also increasingly exploiting VASPs and using VAs to transfer value and hide the identity of proliferation actors. Illicit actors can exploit VASPs based in jurisdictions with little or no regulatory oversight to provide products to designated persons and entities. Illicit actors use falsified or fake documents and identifiers to move and access funds, or employ obfuscating techniques, including using mixers, tumbler services, and anonymity-enhanced VAs.

- New Technologies: PF remains a global threat, with actors constantly adapting their methods to evade sanctions and export controls. New technologies like VAs and online fundraising platforms pose unique challenges due to their anonymity, ease of cross-border transactions, and difficulty in monitoring suspicious activity. Proliferators can exploit these platforms to raise funds and move them across jurisdictions, bypassing AML/CFT controls of regulated LFIs.

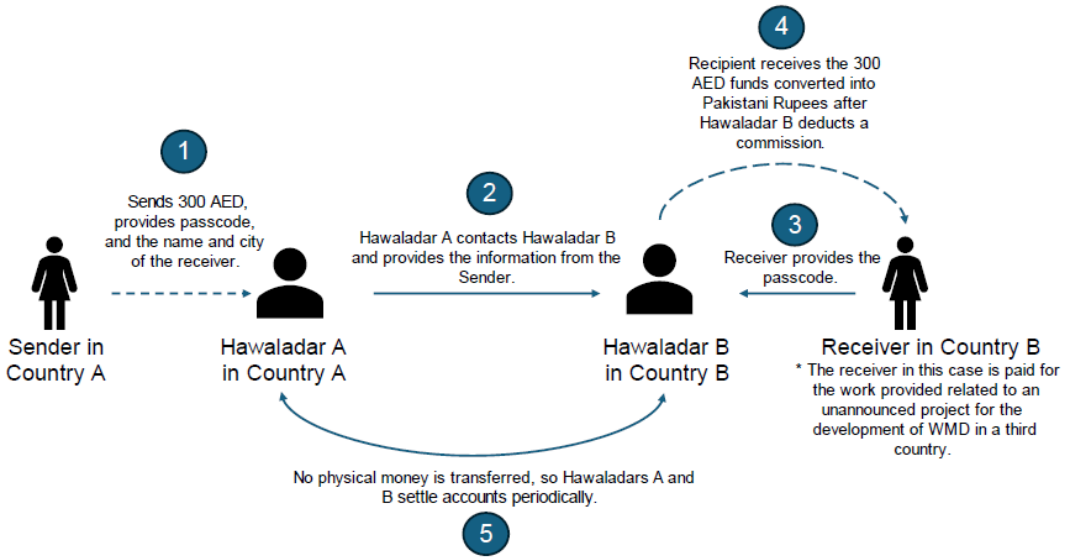


Figure 3 – This figure illustrates a transaction involving an RHP. Sender in Country A sends value to the receiver in Country B through an RHP related to an unannounced project for the development of WMD in a third country.

[8] For more information on the risks related to VAs/VASPs, see the relevant CBUAE Guidance at: https://www.centralbank.ae/media/avwlktgy/cbuae-guidance-for-lfis-on-risks-related-to-virtual-assets-and-virtual-assets-providers_final-clean-version1.pdf

3.2.4. Offshore Accounts

Offshore accounts can be attractive for various financial activities, including legitimate business operations and wealth management. These features also make offshore accounts susceptible to abuse by leveraging the opacity and complexity of cross-jurisdictional regulations and the use of multiple FIs, accounts and corporate vehicles to obscure the trail of funds. Moreover, offshore financial centers may have regulatory frameworks that are not fully aligned with international standards to combat PF, in addition to anonymity and secrecy often offered by some offshore jurisdictions. Proliferators and their networks may engage in cross-jurisdictional arbitrage and exploit regulatory gaps and AML/CFT/CPF deficiencies within specific financial sectors to transfer funds under the guise of legitimate businesses to procure WMDs or fund the procurement of WMDs.

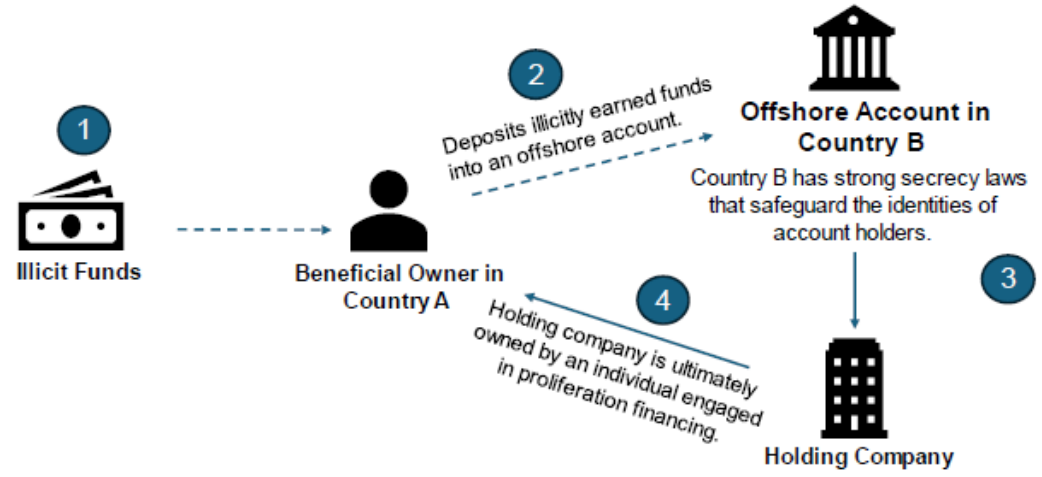


Figure 4 – This figure illustrates the way in which offshore accounts may be abused for PF purposes, including through using complex corporate structures to obscure a beneficial owner's identity. In this scenario, the beneficial

owner takes advantage of Country B with strong bank secrecy laws. The beneficial owner resides in Country A and sends funds to an offshore account in Country B where the corporate vehicle is registered.

3.2.5. Free Trade Zones

Free trade zones ("FTZs") are designated areas within countries in which incentives are offered to support the development of exports, foreign direct investment ("FDI"), and local employment. Incentives include exemptions from certain taxes, simplified administrative procedures, and the duty-free importation of raw materials, machinery, parts, and equipment. These conditions and the following factors internationally may also make such areas attractive to potential illicit actors:

- Inadequate AML/CFT/CPF safeguards;
- Relaxed oversight by competent domestic authorities;
- Weak procedures to inspect goods and register legal entities, including inadequate record-keeping and information technology systems; and
- Lack of adequate coordination and cooperation between a FTZ and customs authorities.[9]

Commercial Free Zones ("CFZs") may present opportunities for regulatory arbitrage whereby illicit actors seek to register in those jurisdictions where controls are perceived to be weak. Port facilities located within these jurisdictions may make certain zones potentially even more attractive to potential PF actors, especially if these facilities are less well-staffed with customs inspectors and related personnel when compared to mainland facilities or port facilities in larger CFZs.

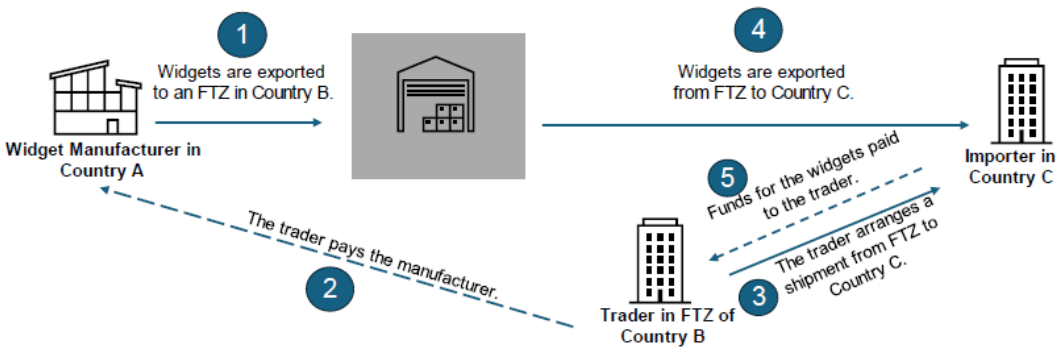


Figure 5 – This figure is an example of how FTZs could be used as a point of transshipment. In this case, the manufacturer in Country A exported widgets to the FTZ in Country B. A trader located in Country B keeps the widgets in the FTZ and reexports them to Country C. The importer in Country C pays the trader in Country B who then pays the manufacturer in Country A. In this case, the manufacturer does not know its widgets are sent to Country C.

[9] FATF Report, Money Laundering vulnerabilities for Free Trade Zones, March 2010. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingvulnerabilitiesoffreetradezones.html

3.2.6. Shell Companies, Front Companies, and Complex Ownership Structures

Shell and front companies are ideal vehicles for nefarious actors to conduct illicit activities and conceal their true identities. Per FATF's *Concealment of Beneficial Ownership* report published in 2018,[10] shell and front companies

are defined as follows:

- **Shell companies** are incorporated entities with no independent operations, significant assets, ongoing business activities, or employees. LFIs should be aware that many offshore accounts are held by shell companies.

- **Front companies** are fully functioning companies with the characteristics of a legitimate business, serving to disguise and obscure illicit financial activity.

In addition to shell and front companies, proliferators exploit complex ownership structures in order to disguise their proliferation activities. Specifically, the FATF[11] has indicated that designated persons and entities, including those persons and entities acting on their behalf, hide their beneficial ownership through opaque legal entities or arrangements and the use of nominee shareholders.[12] Proliferators have been found to engage in schemes through a combination of complex ownership structures, front companies, and shell companies located across different jurisdictions to eventually transfer funds to designated persons and entities for the purposes of obtaining funding or financing for WMD program activities or dual-use or proliferation sensitive goods.

As in the AML/CFT context, conducting CDD/KYC and risk-based EDD measures from a CPF perspective is critical to identify, manage, and mitigate risk associated with PF. Specifically, LFIs should identify and verify the identity of beneficial owners of legal entity customers on a risk-sensitive basis (e.g., legal persons with complex ownership structures or from high-risk jurisdictions), including by lowering ownership percentage thresholds in line with a customer's perceived risks and application of the risk-based approach ("RBA"). LFIs should also consider requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks. Further information regarding beneficial ownership identification and verification can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.3.1 and 6.3.3, and *Guidance for LFIs Providing Services to Legal Persons and Arrangements*.[13]

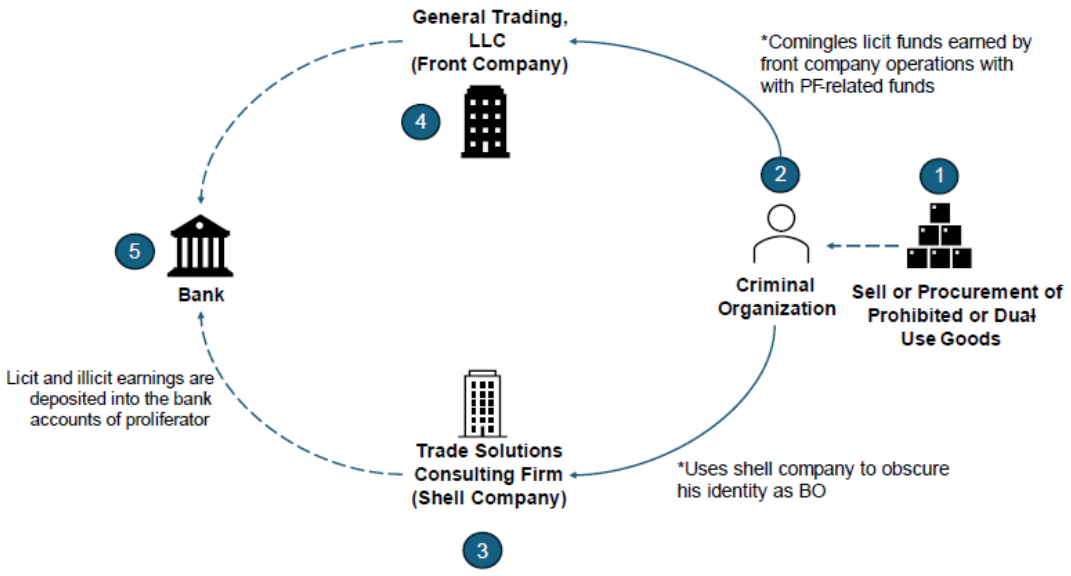


Figure 6 – This figure shows how a criminal organization may use a front or shell company to conceal the illicit activity from an LFI by mixing licit and illicit earnings and depositing these proceeds into the LFI's account.

---

[10] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership-Executive-summary.pdf

[11] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-

Assessment-Mitigation.pdf.coredownload.pdf

[12] Nominee shareholders are individuals who hold shares on behalf of the true beneficial owner.

[13] Available at: https://www.centralbank.ae/en/cbuae-amlcft

3.2.7. Insurance and Reinsurance

In the context of PF, insurance and reinsurance may be susceptible to abuse by illicit actors insofar as they are seeking to move goods and funds, insure illicit activities and goods, or manipulate insurance claims to obtain funds for PF purposes. Various methods of abusing the insurance sector exist, including by acquiring insurance or reinsurance policies for fictitious vessels, providing coverage for shipments involving high-risk goods, such as dual-use items, obscuring the true contents of an insured vessel, or falsifying information related to goods, shipments, or their intended use.

Insurance and reinsurance companies, insurance agents and brokers, should be aware of the vulnerabilities of these products and implement effective measures to prevent illicit actors from abusing them to conduct PF activities. To mitigate the PF risks related to insurance and reinsurance products, including sanctions evasion risk, LFIs should consider:

- Implementing EDD measures as appropriate for higher risk customers;
- Conducting periodic refreshes on customers posing elevated levels of PF and sanctions evasion risk; and
- Tailoring transaction monitoring and name screening scenarios to PF risks related to the insurance and reinsurance of goods.

Specifically, insurers and reinsurers should review CDD and transactional information for the following red flag indicators:[14]

- Vessels that are registered under different "flags of convenience" while operating in the vicinity of high-risk PF jurisdictions;
- Complex corporate structures, as well as the lack of due diligence into the third parties chartering vessels; and
- Vessels with links to other vessels identified as involved in sanctions violations or sanctions evasion schemes.

For further information on how to mitigate the PF risks related to the insurance sector, LFIs should consult the CBUAE's *Guidance on AML/CFT for the Insurance Sector*,[15] and the EOCN's Targeted Financial Sanctions Guidance for the Insurance Sector.[16]

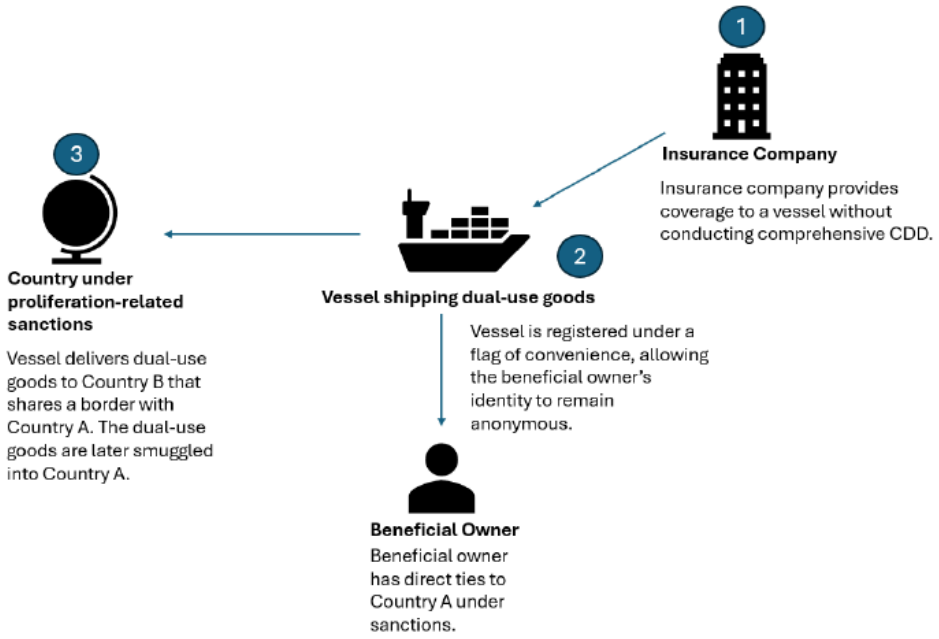


Figure 7 – This figure illustrates the role of insurance companies in a trade transaction. Specifically, an insurance company may insure a vessel registered under a flag of convenience, where the beneficial owner's identity is not disclosed to the insurance company. In this case, the beneficial owner may be a nefarious actor with ties to a sanctioned country (Country A) and who is seeking to use the goods transported on the vessel for PF activities.

---

[14] See RUSI, *Sanctions Evasion, Proliferation Finance, and the Insurance Industry* (July 2018), available at: https://static.rusi.org/20180710_underwriting_proliferation_web.pdf
[15] Available at: https://centralbank.ae/media/eyeeyagu/cbuae-aml_cft-guidance-for-the-insurance-sector.pdf
[16] Available at: https://www.uaeiec.gov.ae/en-us/un-page?p=7#

3.2.8. Real Estate

The real estate sector may be susceptible to abuse by nefarious actors seeking to conceal illicit funds or finance proliferation-related activities. Real estate agents and brokers, in particular, may facilitate PF schemes through their involvement in property transactions which can involve substantial capital flows and asset transfers that can be exploited for PF activities. LFIs involved in financing real estate transactions or providing mortgage services are at risk of inadvertently facilitating PF through their indirect involvement via loans, credits, or other financial services linked to real estate. These vulnerabilities fall into two main categories: **transactional methods** and **ownership structures**.

(1) **Transactions Methods**:

- *Cash Transactions*: Like any other large transaction in cash, real estate transactions in cash pose a significant risk, as cash holds no record of its source or owner, and the purchase of real estate can be abused by proliferators to place large sums of cash into the financial system.

- *Over or Under-valuation of Properties*: Proliferators may over- or under-value properties to facilitate PF. Manipulating the value of real estate properties (either inflating or deflating values) is a method to move funds under the guise of legitimate transactions. A buyer of under-valued property is able to receive value (profit) from the seller. A buyer of over-valued property is able to transfer value (profit) to the seller, which could be used as a means of payment for goods that are relevant to the development or acquisition of WMDs.

- *Use of Intermediaries:* Real estate brokers and agents can be unwittingly used to mask the identities of buyers and sellers, thereby facilitating transactions that could support proliferation. The involvement of

intermediaries adds layers of complexity that can hinder the tracing of illicit funds intended for PF activities.

(2) Ownership Structure:

- *Shell Companies*: Proliferators may use shell companies and business establishments to conceal the identity of beneficial owners when purchasing and selling real estate. The opaqueness of shell companies hinders the identification of individuals who may be linked to PF activities.

- *Complex Ownership Structures:* Complex ownership structures in the real estate sector often involve the use of corporate vehicles (such as companies, trusts, and foundations) to hold property rights, often layered across multiple jurisdictions. These structures can obscure the true ownership of assets and the source and destination of funds, presenting challenges to detecting and preventing illicit financial flows.

- *Luxury Real Estate Market*: Investing in high-value properties enables proliferators to move and store large sums of illicit funds and often requires multiple types of financing, further complicating efforts to identify the source of funds and ultimate beneficial owner. The luxury real-estate market also involves both high transaction values and international clientele, which can reduce the transparency within real estate transactions and the incentive for implementing appropriate CDD/KYC controls. Purchasing luxury real estate is often an investment strategy that can generate a large return, thus enabling proliferators to hide behind a legitimate premise for acquiring and selling property.

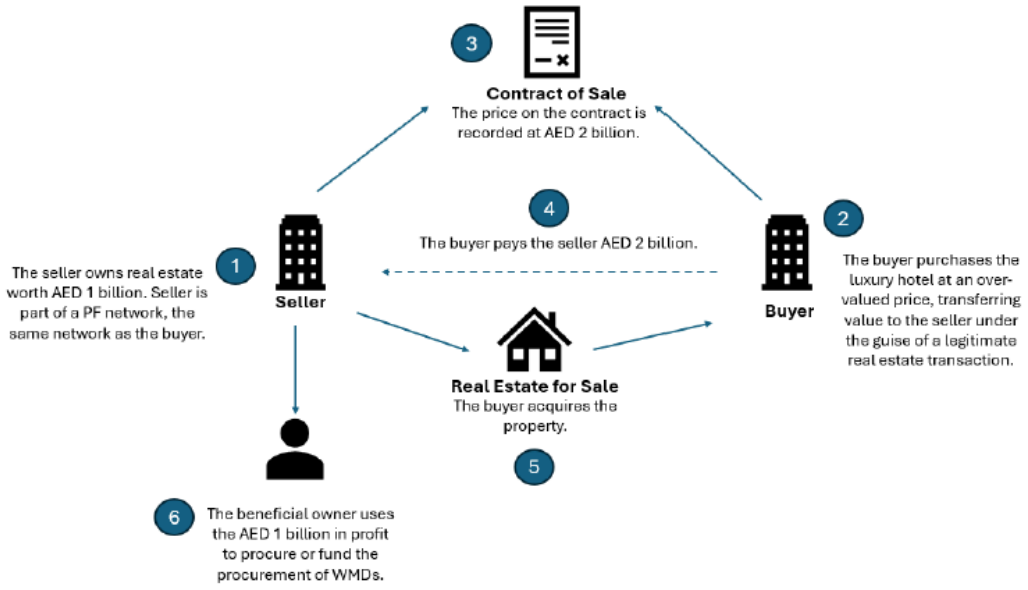


Figure 9 *– This figure illustrates how real estate can be over-valued in order to use the profit gained from a sale for PF-related activities. In this case, the identity of the beneficial owner is obscured through corporate structures, and the beneficial owner uses the funds from the real estate sale to procure WMD materials.*

3.2.9. Dealers in Precious Metals and Stones

Precious metals and stones dealers, particularly those involved in gold trade are particularly exposed to PF risks given their intrinsic characteristics, such as high value, ease of trade, mutability, portability, liquidity, transferability, anonymity and availability in the UAE. As such, these items are particularly susceptible of being used in international trade transactions to obfuscate the BOs or as means of payment in order to fund the procurement or procure WMDs by State actors, particularly DPRK, and non-State actors, as highlighted by the UN Panel of Experts in 2019.[17] LFIs providing services to dealers in precious metals and stones ("DPMSs") or financing precious metals and stones ("PMS") transactions might be unwittingly involved in PF activity by facilitating trade finance transactions or servicing customers dealing with these high-value goods.

LFIs should implement commensurate EDD measures to understand the nature and business of a DPMS (e.g., whether the DPMS is involved in producing or mining, is a buyer or seller, refiner, intermediary, jewelry manufacturer, retailer, or dealer in the secondary market), including the DPMS's customers, and should identify the origin and destination of the PMSs and how the PMSs are being financed or liquidated. In addition, LFIs should analyze and understand the DPMS's policies, procedures and controls, as mandated for all DNFBPs, to assess whether a DPMS customer has in place appropriate measures to ensure their transactions are not being abused for PF purposes.

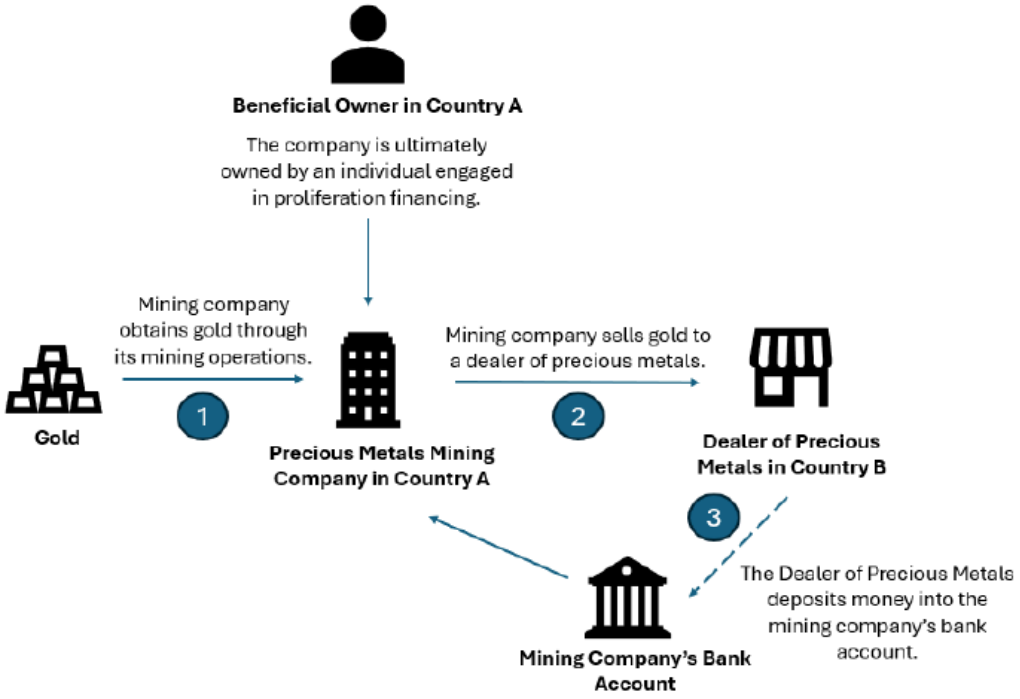


Figure 10 – This figure illustrates how an illicit actor can finance PF-related activities by selling gold as part of international trade transactions. In this case, the beneficial owner of a mining company in Country A uses the funds from the sale of gold to a dealer of precious metals in Country B to procure WMD materials.

[17] UN Panel Experts Report to President 2019; S/2019/171, available at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf

4. Assessing and Mitigating Proliferation Financing Risks

4.1. International Obligations

The global CPF regime was first developed through United Nations Security Council Resolutions, with Resolution 1540 (2004) introducing the first global expectations on states to counter the financing of proliferation given concerns regarding non-state actors and WMD.[18] Subsequent resolutions created new requirements related to specific countries of proliferation concern, such as North Korea and Iran. At the same time, leading jurisdictions pushed for the FATF to become a forum for leadership and intergovernmental coordination, since the organization's leading role on AML/CFT issues positioned it to address the financial flows that were still facilitating WMD proliferation despite expanding export control regimes.[19] The FATF has been a CPF standard-setter since 2008, with FATF Recommendations 1, 2, and 7 covering CPF issues,[20] as addressed in greater detail in following sections on this Guidance.

[18] Andrea Berger and Anagha Joshi, *Countering Proliferation Finance: Implementation Guide and Model Law for Governments*, RUSI Guidance Paper (July 2017), *available at* https://rusi.org/explore-our-

research/publications/special-resources/countering-proliferation-finance-implementation-guide-and-model-law-governments.

[19] Idem.

[20] "International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation: The FATF Recommendations," Updated February 2023, available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

4.1.1. United Nations Security Council

The global framework to control PF includes UNSCRs and relevant national legislation and regulation that establish unilateral sanctions or export-control measures. All UN Member States are obliged to implement UNSCRs, but in practice not all jurisdictions have the necessary domestic legislation in place to do so comprehensively, and fewer enforce such legislation effectively. Even fewer still have published guidance for their respective financial sectors. All UN Security Council sanctions regimes include provisions for exceptions on humanitarian grounds, and jurisdictional requirements in these respects vary globally, which may give rise to additional complications in implementation.

4.1.1.1. Non-State Actors

UNSCR 1540 (2004) constitutes the overarching global requirement related to PF. It focuses on malign activities and is not a state-specific sanctions resolution. There are no requirements, for example, to freeze assets of named individuals or entities under this Resolution. Rather, it mandates that states refrain from providing any form of support to non-state actors that attempt to develop acquire, manufacture, possess, transport, transfer, or use nuclear, chemical, radiological, or biological weapons and their means of delivery, particularly for terrorist purposes. In addition, it requires states to adopt and enforce appropriate laws.

4.1.1.2. North Korea

Sanctions against North Korea under the UN Security Council's 7 8 Committee combine targeted financial sanctions, activity-based sanctions, and sectoral sanctions. Resolution 1718 (2006) was issued in the aftermath of North Korea's first nuclear test. The UNSC has issued nine subsequent sanctions resolutions, the most recent in 2017. Before 2016, measures were narrowly limited to prohibiting conduct connected to weapons proliferation and were enforced through targeted financial sanctions and a luxury goods ban. Since 2016, measures have included significant increases in the scope and nature of prohibitions, including a variety of sectoral and activity-based measures in addition to targeted financial sanctions.

The Security Council's Panel of Experts' annual or bi-annual reports include details of attempts by North Korean actors to raise revenue by hacking into banks (including through vulnerabilities in the SWIFT network) and into cryptocurrency exchanges. As noted above, in the case of North Korea, revenue generation is generally categorized as PF, and if cryptocurrencies become commonly used for trade finance, they can be expected to become a significant element of PF in this respect as well.

The UAE does not house a North Korean embassy or maintain diplomatic ties with the DPRK. However, there may be potential vulnerabilities especially for those FIs processing or facilitating transactions associated with trade finance (see section 2.2.1 above). The DPRK is known to "re-flag" vessels and engage in ship-to-ship transfers, especially of petroleum products, to obscure their ultimate destination and/or origins.

As of the date of this Guidance, the DPRK is listed on the FATF List of Jurisdictions Subject to a Call for Action, also known as the FATF "Black List," due to serious strategic deficiencies in the country's AML/CFT/CPF regime. The DPRK is also included on the EU's list of high-risk third countries having strategic deficiencies in their regime on AML/CFT.

4.1.1.3. Iran

FIs should be aware of the potential vulnerabilities associated with processing or facilitating Iran transactions associated with trade finance (see section 2.2.1 above), and should put in place controls to mitigate the PF risks. With the passage of UNSCR 2231 (2015) and implementation of the Joint Comprehensive Plan of Action ("JCPOA"), also known as the Iran Nuclear Deal, on January 16, 2016, most United Nations sanctions relating to Iran's nuclear activities were formally lifted. The few outstanding sanctions were lifted on the transition date in October of 2023. However, unilateral and multilateral sanctions relating to Iran's conventional weapons or ballistic missile activities remain in place.

Moreover, Iran remains on the FATF list of High-Risk Jurisdictions subject to a Call for Action. While UAE entities are not bound by the sanction regimes of other countries, there may be potential secondary sanctions implications for engaging in significant transactions violating U.S. sanctions.

4.1.2. Financial Action Task Force

The FATF plays an important role in assessing countries' technical compliance with and effective implementation of targeted financial sanctions pursuant to UNSCRs relating to the prevention, suppression, and disruption of proliferation of WMD and its financing.

4.1.2.1. Recommendations 1, 2, and 7

Recommendation 1 (Assessing National Risks) and its interpretive note were updated in 2020 and requires countries, FIs, DNFBPs, and virtual asset service providers ("VASPs") to identify, assess, understand, and mitigate their PF risks.[21]

Recommendation 2 (National Cooperation and Coordination) requires countries to adopt risk-based policies to combat illicit financing threats (including PF) and to designate an authority to review and update policies and ensure that all relevant competent authorities can cooperate and exchange information regarding the development and implementation of policies and activities to combat PF.

Recommendation 7 (TFS related to Proliferation Financing) requires countries to implement TFS relating to the prevention, suppression, and disruption of proliferation and its financing. Generally speaking, countries are required to immediately freeze the funds or other financial assets of any person or entity designated by a UNSCR related to PF and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of such a person or entity (including through persons providing support for, acting on behalf of, or owned or controlled by designated parties or assisting them in evading sanctions requirements).[22]

---

[21] FATF's revised Recommendation 1 and Interpretative Note 1 require countries, financial institutions, DNFBPs, and VASPs to identify, assess, understand, and mitigate PF risks. For more information, please refer to: fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.

[22] For more information related to specific measures related to TFS for DPRK and Iran, refer to Recommendation 7 of the "International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation: The FATF Recommendations," Updated February 2023, available at fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.

4.1.2.2. Immediate Outcome 11

To demonstrate an effective CPF system under Immediate Outcome ("IO") 11, persons and entities designated by the UNSCRs on proliferation of WMD must be identified, deprived of resources, and prevented from raising, moving, and using funds or other assets for PF. TFS must be fully and properly implemented without delay and monitored for compliance, and countries must establish adequate cooperation and coordination between the relevant authorities to prevent sanctions evasion and develop and implement policies and activities to combat the financing of PF.[23]

[23] Immediate Outcome 11 of the "International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation: The FATF Recommendations," Updated February 2023, available at https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

4.1.2.3. Related FATF Guidance

The FATF's 2018 *Guidance on Counter Proliferation Financing*[24] assists jurisdictions in understanding and identifying the threat from PF. The guidance extends to UNSCR sanctions on North Korea and Iran not covered by Recommendation 7, such as activity-based and sectoral sanctions.

The FATF's 2021 *Guidance on Proliferation Financing Risk Assessment*[25] complements the above and contains guidelines for countries, FIs, DNFBPs, and VASPs to conduct national or institutional PF risk assessments.

The FATF's 2008 *Proliferation Financing Report*[26] lays out red flag indicators related to PF, provided in Annex 2 of this Guidance.

[24] Available at: https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html
[25] Available at: https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html
[26] Available at: https://www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf.

4.2. Compliance with Local Requirements

The UAE legal and regulatory framework counters PF through the implementation of targeted financial sanctions related to PF, export controls, and AML/CFT preventive and detective measures that assist public authorities and private sector entities in preventing, suppressing, and disrupting the proliferation of WMD and its financing. Key elements of the UAE CPF framework include:

- **Federal Decree Law No. (20) of 2018,** Article 16.e.1 specifies that FIs and DNFBPs shall undertake "Prompt application of the directives when issued by the competent authorities in the state for implementing the decisions issued by the UN Security Council under Chapter (7) of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, and other related directives".

- **Federal Decree-Law No. (20) of 2018**, Article (28) of which provides for a penalty of imprisonment of no less than a year and no more than (7) years, or a fine of no less than AED 50,000 for anyone who violates any of the directives of Chapter 7 of the UN Convention for the Suppression of the Financing of Terrorism and Proliferation of WMD and other related directives.

- **UAE Cabinet Decision No. (74) of 2020**, concerning the implementation of UNSCRs on the suppression and combating of terrorism, terrorist financing, and countering the proliferation of WMD, is central to the UAE's framework for countering the proliferation of WMD.

- **Cabinet Resolution No. (50) of 2020**[27] contains the list of strategic and dual-use goods controlled under UAE law.

- **Federal Decree Law No. (43) of 2021** concerns commodities subject to non-proliferation and provides for restriction of certain commodities and the issuance of permits to trade in such items.

[27] Available at: https://www.uaeiec.gov.ae/en-us/un-page?p=7

4.3. Proliferation Finance Risk Assessments and Risk-Based Approach

Under Article 4 of the AML-CFT Decision, any LFI is required to identify, assess, and understand its ML/TF risks. For this purpose, and pursuant to Notice No. CBUAE/BIS/2023/5960, LFIs should also perform, document, and keep up to date an institutional-level risk assessment that includes identifying, assessing, understanding and mitigating risks related PF, and have the appropriate mechanisms to provide PF risk assessment information to the CBUAE. An LFI's risk assessment should be based on a comprehensive understanding of the PF threats and vulnerabilities, including the methods, actors, and networks involved in financing proliferation activities[28]. When assessing inherent risks, LFIs should also consider the results of the Proliferation Financing National Risk Assessment (PFNRA) or any Topical Risk Assessment, as well as information from official sources, including the Supervisory Authorities, the FIU, the FATF, MENAFATF and other FSRBs, the Egmont Group, etc. Specifically, LFIs should consider PF risk factors arising in relation to their:

- Customers;
- Products, services, and transactions (new and existing);
- Delivery channels (new and existing);
- Geographic locations and markets; and
- Operating structure (such as cyberthreats).

Risk assessments should be an ongoing process, and should be reviewed regularly to ensure that they remain relevant and effective. LFIs should also ensure that their risk assessments are integrated into their overall risk management frameworks. LFIs should incorporate the outcomes of their controls, like the number of PF-related alerts generated by the transaction monitoring system, into their PF risk assessment.

LFIs should apply risk mitigation methods that are appropriate to the types and levels of risk identified in their institutional risk assessment. PF risk management should be incorporated into an FI's larger counter-illicit finance program, and institutions can use many of the same controls to mitigate and manage their PF risk that they already employ for ML/TF and sanctions purposes. LFIs should consider, however, the following aspects of an effective program specifically in connection with PF risks:

- **Use of technology to detect sanctions evasion behavior:** LFIs with higher risks should consider the use of data analysis programs that detect linkages, patterns, and relationships between or among networks.
- **Incorporating PF-specific information in the CDD process:** Based on their risk assessments, LFIs should adapt their onboarding and CDD processes to collect additional information that may help to more accurately risk-rate customers for PF risk and develop detailed customer risk profiles.
- **Including PF risk in correspondent banking risk-ratings and EDD**: Correspondent banking relationships are one of the main sources of PF risk for LFIs, but not all relationships present equal risk. LFIs should ensure that their risk-rating and EDD processes for correspondent banking relationships consider, assess, and manage PF risk.
- **Training to the FI's leadership and staff at all levels on PF-related issues:** Effective PF training should go beyond internal list-based screening processes to cover PF risks and sanctions evasion typologies, the findings of the LFI's PF risk assessment, and the controls the institution has put in place to manage PF risk.

The following sections provide further detail regarding PF-specific risks that LFIs should account for identifying, understanding, assessing, and mitigating PF risks.

[28] Please refer to the EOCN PF Institutional Risk Assessment Guidelines, for further details online of questions to assess customers' exposure to PF risks. Customer risk also includes a customer's business activity, occupation and/or industry.

4.3.1. Customer Risk

Individuals and entities already designated for their involvement in PF activities clearly present prohibitive risks to LFIs, but LFIs should also be aware of the risks of providing financial services to individuals that are associated with designated persons and to entities that are owned or controlled by sanctioned parties.

PF risk can also impact an LFI through its customers in certain business sectors or industries. These customers may include, for instance, producers of sensitive goods, producers of dual-use goods, and companies or institutions involved in advanced research. Shipping companies and general trading companies, particularly those serving high-risk regions, may also present significant PF risk. Such customers, particularly those that produce dual-use goods, or trade dual-use goods, may not be familiar with relevant import/export requirements and controls and may be unaware of the need to implement their own CPF safeguards, thus presenting higher risk to LFIs.

Additionally, proliferation networks often rely on shell and front companies to mask end users and to disguise payments. These companies present higher levels of PF risk for a number of reasons including their potential roles in PF-related activities and schemes.

Published case studies[29] suggest that the following customer types may present higher levels of PF risk:

- Parties with links to a country that is of PF concern, for example, dual national and entities owned by companies in the country of concern.
- Producers of dual-use (sensitive or restricted) goods.
- Small and medium-sized trading companies, particularly if they switch business to trade in potentially proliferation-sensitive goods or materials.
- Customers who use personal accounts for trade or business-related transactions.
- Customers who largely conduct cash-based businesses and originate from, reside or are associated with high-risk jurisdictions for TF/PF.
- Shell and front companies.
- Newly incorporated entities with no known background/history.
- Shipping and logistics companies, particularly if they are identified as consignees on shipping documentation.
- Entities operating in the maritime sector, through which proliferation actors can both move components and materials necessary for proliferation and generate funds for PF though economic activities through otherwise licit activities, such as the sale of natural resources.
- Academic and research institutions, as there have been cases of such entities—particularly state-owned institutions—procuring sensitive goods and materials on behalf of sanctioned WMD programs.

- Among DNFBPs, including trust and company service providers ("TCSPs") and DPMSs, which have been abused by proliferation actors to conceal their interests in a transaction (through the creation of shell or front companies) and to move funds across borders through the purchase and sale of gold, diamonds, and other precious metals and stones.

- VASPs, which can allow proliferators to move funds across borders instantly, can provide access to fiat currencies, and have been abused to launder proceeds of crimes committed to support proliferation.

Certain customer behavior may also indicate higher levels of risk and thus require additional scrutiny, including cross-border transactions involving legal persons and arrangements or multiple shell or front companies; high transaction volumes involving individuals acting on behalf of legal persons or arrangements; and customers who frequently transact with high-risk countries or whose transaction behavior is not related to their stated business purposes. Additional PF-related customer risk indicators identified by EOCN are presented in Annex 3 of this Guidance. LFIs should be cognizant of customer types that pose an elevated risk for PF and should assess the risk of these customers who may seek to or be part of schemes that involve obtaining funding or financing for WMD program activities or dual-use or proliferation sensitive goods or services.

---

[29] Available at: https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf

4.3.2. Product, Service, and Transaction Risk

Certain trade finance transactions implicating controlled goods or technology present elevated PF risks for LFIs because these transactions are often complex in ways that allow individuals and entities to mask their intentions or underlying illicit activities. Likewise, correspondent banking services are an important source of PF risk. Activities such as clearing intermediary wires can expose an LFI to additional risk because the institution should process or execute transactions for its customer's customer. In such circumstances, the LFI will lack a complete understanding of the customer and the customer's transactional history and should therefore rely on its respondent to apply effective, risk-based AML/CFT/CPF preventive and detective measures.

Although trade transactions have traditionally been associated with letters of credit and documentary collection, trade transactions have increasingly relied on the use of "open account" cross-border wire transfers. This development poses challenges to risk management. Although wire transfers are generally less complicated mechanisms of financing trade transactions and can be processed more quickly and easily, it is often more challenging for FIs to obtain sufficient information to understand the purposes of transactions, the underlying goods or services paid for by the transactions, the shipping or transportation of the goods involved, and other parties related to the transactions (*e.g.*, importers and exporters). By contrast, illicit activity is generally more difficult to execute through traditional trade finance instruments such as letters of credit precisely because of the extensive documentation and diligence usually associated with issuing and processing these instruments.

Trafficking of dual-use or proliferation-sensitive goods and materials is typically funded or financed in the same way as legitimate international trade, through open-account transactions (cross-border wires) or trade finance mechanisms. According to the International Chamber of Commerce, 80 percent of international trade takes place on open account terms, however, wire transfer messages (e.g., SWIFT messages) related to such transactions contain little information about the nature of the underlying transactions.

LFIs are better placed to assess PF risk of international trade conducted using documentary trade finance mechanisms. These documents typically provide information about the type and quantity of goods and materials involved, the identities and locations of buyers and sellers, the shipping routes, the destinations and the names of vessels and shipping companies. However, this documentation may still not describe the contents of shipments in a way that enables them to be easily identified as proliferation-sensitive dual-use goods and materials.

LFIs should be cognizant of those product and services that pose an elevated risk of abuse for PF and should assess the risk that products and services they offer may be used to obtain funding or financing for WMD program activities

or obtain dual-use or proliferation sensitive goods or services critical to the programs. An LFI's enterprise-wide ML/TF/PF risk assessment or standalone product risk assessment should evaluate the PF risk associated with a new product before the product is launched. The risk assessment should periodically assess the ML/TF/PF risk of all products and services the LFI offers.

LFIs should place special focus, among others, on:

- Traditional/documentary/open account trade finance;[30]
- Cross-border wires, including those related to trade and those that may be related to the sending of proceeds of criminal activity to intermediary countries;
- Correspondent banking services; and
- Products and services related to VA.

PF-related risk indicators specific to the maritime sector, trade finance services, and specific types of transactions are presented in Annex 3 of this Guidance.

---

[30] Please note, the LFI may seek to engage in a sampling methodology to verify shipment documentation by an independent source.

4.3.3. Geographic Risk

Although only a relatively small number of countries have developed illicit WMD programs, activities related to these programs can span the globe due to the volume and transnational nature of international shipping and trade, flexible trade finance agreements (e.g., open-trade accounts), and correspondent and nested banking relationships. As such, no country is immune to PF risk, and some face heightened exposure based upon their location vis-à-vis major trade routes and/or proximity to other jurisdictions of PF concern.

Countries led by governments that are known or strongly suspected to be developing WMD present the highest geographical risk for FIs, particularly where these countries have been subject to UNSCR sanctions programs (i.e., North Korea).

When UN sanctions were in place, the sourcing, shipment, and financing of proliferation-sensitive goods, materials, and technologies carried out by Iran's nuclear procurement networks—and related sanctions-evasion activities—extended to Europe, North America, and Asia, according to reports of the UN Panel on Iran. Similarly, North Korea's MD procurement and sanctions-evasion networks also extend globally, as documented by the UN Panel on North Korea. Assessments of PF risk at the jurisdictional level should therefore take account the potential global reach of WMD procurement and financing networks.

Geographic risk is not restricted to proliferating countries themselves. Countries and terrorist groups rely on transnational connections to procure illicit goods and services. For instance, North Korea relies on extensive corporate networks hosted in China, Hong Kong, Singapore, and Malaysia; in China, related companies are especially active in Liaoning and Jilin provinces.[31] Proliferators may aim procurement efforts at countries with weak export control laws, and they may choose to have sensitive or dual-use items delivered initially to transshipment hubs rather than directly to their home countries.

The UAE lies directly across the Persian/Arabian Gulf from Iran and is a significant partner for international trade, increasing the UAE's potential exposure to sanctioned persons or entities in the region as well as to international trade and financial flows that carry heightened PF risks.

LFIs should be cognizant of proliferating countries and the geographic risks posed by transnational connections that illicit actors seek to exploit when funding or financing WMD program activities or obtaining dual-use or proliferation

sensitive goods or services.

[31] Emil Dall, Tom Keatinge, and Andrea Berger, *Countering Proliferation Finance: An Introductory Guide for Financial Institutions*, RUSI Guidance Paper (April 2017) at 12 and 26, https://rusi.org/sites/default/files/201704_rusi_CFP_guidance_paper.1_0.pdf.

4.3.4. Delivery Channel Risk

Delivery channel risk stems from the e tent to which an LFI's methods of account origination, account servicing, and transaction facilitation limit its understanding of its customers' identities, activities, and counterparties. The following are key drivers of inherent ML/TF delivery channel risk:

- Use of non-face-to-face channels;
- Proportion of unsolicited (e.g., walk-in) customers;
- Reliance on delivery by or through a third party; and
- Near-instantaneous or irrevocable settlement or processing (also a driver of product and service risk).

Services provided through higher-risk delivery channels are more susceptible to abuse by illicit actors, including, in the PF context, persons and entities subject to PF-related targeted financial sanctions and those providing support for, acting on behalf of, or owned or controlled by designated parties or assisting them in evading sanctions requirements. LFIs should be cognizant of delivery channels that pose an elevated risk of abuse for PF and should assess the risk that delivery channels can be used to obtain funding or financing for WMD program activities or for obtaining dual-use or proliferation sensitive goods or services critical to the programs.

4.3.5. Operational Risk

Operational risk is a concept in enterprise-wide risk management that encompasses risks of loss and disruptions to business that stem from ineffective or failed internal processes, people, or systems or from external events. In the AML/CFT/CPF context, operational risk is a function of the stability of an institution's compliance staff, systems, and policies; the stability of its exposure to the other risk categories such as customers; and whether the institution has experienced risk events such as a hack or other malicious cyber event.

With respect to PF risks specifically, LFIs should identify, understand, assess, and mitigate risks associated with:

- Inadequate or fluctuating staffing levels in key CPF control functions;
- Material changes in the size or composition of the customer base;
- Fluctuations in sanctions screening, customer risk rating, and other technological systems or models used to support CPF compliance;
- The emergence of backlogs of transaction monitoring alerts or CDD/KYC refreshes;
- The occurrence of PF-related internal or external risk events, including material compliance breaches and changes to the risk or regulatory environment; and
- Lower levels of understanding and application of CPF controls amongst employees, due to lack of training and familiarization with PF red flags and CPF regulatory requirements.

4.4. Mitigating Controls

Effective risk mitigation is critical to protecting the LFI, complying with its legal obligations, and meeting supervisory expectations. LFIs should establish policies, procedures, and processes to understand their risk and take effective, risk-based steps to protect themselves from abuse and from illicit actors and transactions. The sections below discuss how LFIs can apply specific preventive measures to identify, manage, and mitigate PF risks. LFIs should consult the legal and regulatory framework currently in force. The controls discussed below should be integrated into the LFI's larger AML/CFT program and supported with appropriate governance and training.

4.4.1. CDD and EDD Measures

4.4.1.1. General CDD Measures

Customer due diligence ("CDD"), and where necessary enhanced due diligence ("EDD"), are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers. Under Article 5 of AML-CFT Decision, LFIs must conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. An LFI's CDD program should cover, at a minimum:

- Customer identification and verification;
- Beneficial ownership identification and verification;
- Understanding the nature and purpose of the customer account and relationship for the purpose of establishing a risk profile (see also section 3.4.2 below); and
- Ongoing monitoring, including periodic and event-driven updating of customer and beneficial ownership information and the customer risk profile throughout the business relationship.

Utilizing the information collected through general CDD, an LFI should screen the following parties against lists of sanctioned persons, internal watchlists (such as lists of customers previously exited for financial crime reasons), and, on a risk basis, relevant ML/TF/PF information sources (such as negative media databases) prior to a customer's onboarding:

- All customers, regardless of risk rating or risk profile;
- Beneficial owners of legal entity customers (natural persons);
- Natural persons appointed to act on behalf of the customer (agents acting on behalf of customers);
- Directors, partners, and managers of customers that are legal persons; and
- Natural persons having executive authority over customers that are legal arrangements, including individuals with power of attorney.

With respect to sanctions lists, the parties listed above should be screened prior to a customer's onboarding and on an ongoing basis. To support this effort, all systems containing customer data and transactions need to be mapped to an LFI's screening system to ensure full compliance. The results of screening and assessment by the LFI should be documented.

LFIs should consult the UAE legal and regulatory framework currently in force and related CBUAE Guidance for a full discussion of their CDD obligations and of the CBUAE's expectations for CDD procedures. Consistent with local

regulatory requirements, all LFIs must ensure compliance, where applicable, with Recommendation 10: Customer Due Diligence, as outlined in the FATF 40 Recommendations.

Additional detail regarding general CDD measures is available in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.1 through 6.3.

4.4.1.2. Establishing a Customer Risk Profile that Incorporates PF Risks

Under Article 8 of the AML-CFT Decision, LFIs are required to understand the nature of the customer's business and the nature and purpose of the LFI's relationship with the customer, including the expected uses to which the customer will put the LFI's products or services. This step requires the LFI to collect information that allows it to create a risk profile of the customer, including the types and volumes of transactions the customer is expected to engage in for each customer account, and to assess the risks associated with the relationship.

Establishing a risk profile that incorporates a customer's PF-specific risk attributes is a critical component of effective CPF measures for FIs and can include assessing and assigning risk ratings to customers based on their potential exposure to proliferation financing activities. Customer risk rating enables FIs to prioritize their resources and efforts in managing PF risks and helps identify and allocate appropriate levels of due diligence, monitoring, and mitigation measures based on the types and levels of a customer's risk.

LFIs should consider various PF risk factors when assigning customer risk ratings. Key risk factors, among others, include:

- **Customer-specific attributes**, including the customer's background, ownership structure, geographic location, and business activities. Factors such as involvement in high-risk sectors[32], presence in high-risk jurisdictions, or connections to politically exposed persons ("PEPs") can increase the risk rating.

- **Transactional behavior**, particularly the customer's transaction history, including the frequency, volume, and nature of transactions. Unusual transaction patterns, such as large or rapid fund transfers, transactions involving dual-use goods, or transactions with high-risk jurisdictions, may elevate the risk rating.

- **Red flags and risk indicators**, including involvement in sanctioned or embargoed countries, presence on watchlists or control lists, or connections to entities or individuals involved in proliferation activities.

- **External factors** such as industry-specific risks, regulatory changes, or geopolitical developments that may impact the customer's risk profile.

Although LFIs are not necessarily expected to have a dedicated customer risk rating methodology for PF risks, they should incorporate PF risk factors into internal processes or methodologies for establishing an overall customer risk profile and provide clear guidelines for segmenting customers and assigning risk ratings, scores, or levels. The methodology may take into consideration the following:

- **Risk categories:** Define risk categories (e.g., low, medium, high) based on the institution's risk appetite and regulatory requirements. Each category should have predefined criteria aligning with the identified risk factors.

- **Scoring system:** Develop a scoring system to assess the risk factors and assign a numerical score to each factor. The cumulative score can then be used to determine the overall risk rating for the customer.

- **Risk rating scale:** Define a risk rating scale corresponding to the risk categories, indicating the level of scrutiny and control measures required for each rating. This scale should align with the institution's risk

management framework.

[32] As per best practice, consideration of a customer's industry codes (HS Codes – Harmonized System Codes) can allow for targeted approaches to a specific customer set with PF-related questions, such as by helping determine the specific technology or equipment the customer is manufacturing or trading to determine whether the customer is exposed to heightened PF risks.

4.4.1.3. EDD Measures for Heightened PF Risks

The AML-CFT Law and the AML-CFT Decision impose EDD obligations on LFIs with respect to three classes of customers or transactions:

- Customers that are PEPs, which include the direct family members or associates known to be close to the PEPs (AML-CFT Decision, Article 15);[33]
- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries (AML-CFT Decision, Article 22); and
- Correspondent banking or other similar relationships (AML-CFT Decision, Article 25).

In addition to these classes of customers and transactions, for which EDD is mandatory, LFIs are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for illicit finance.

In the PF context specifically, where an LFI has determined that a customer or beneficial owner presents heightened risks for PF, or where it is required under UAE laws and regulations, LFIs should take the following steps:

- **Obtain senior management approval before establishing a business relationship or continuing an existing one.** The specific senior management member within the LFI who shall be responsible for approving these relationships will vary based on the LFI's own unique governance arrangements. If the approving member represents the business (e.g., the Chief Executive Officer, Chief Operating Officer, or Business Unit Head) as opposed to the compliance function (e.g., the Compliance Officer), the LFI's policies and procedures should clearly require that the head of the LFI's compliance function give an opinion as to whether the risk associated with the customer is acceptable. When approving an existing relationship with a customer identified as high risk for PF, senior management should be notified required by policy to approve the continuance of the relationship.
- **Take risk-based measures to establish the source and destination of funds.** This requirement encompasses two distinct concepts:
    - **Source of funds:** The direct source of the funds that are used to initially fund the account and of any funds that are transacted through the account during the course of the business relationship.
    - **Destination of funds:** The final destination of the funds used for the customer's transactions during the course of the business relationship.

  In both cases, where the LFI receives insufficient, implausible, inconsistent, or potentially suspicious information regarding the source or destination of funds, it should consider additional measures to corroborate such sources using independent documentary or non-documentary sources (or a combination).

- **Ascertain whether the customer conducts business in a high AML/CFT-risk jurisdiction, a jurisdiction of PF concern, or a third-party jurisdiction in close proximity to a jurisdiction of PF concern.** On a risk basis, LFIs should collect and maintain up-to-date information on the main geographic locations where a customer operates and/or conducts business in order to determine, on a risk-sensitive and case-by-case basis, if individual transactions to high-risk PF jurisdictions are legitimate, consistent with the stated purpose, and within the LFI's risk tolerance.

- **Conduct enhanced ongoing monitoring of the relationship.** LFIs should perform risk-based ongoing monitoring of the business relationship for all customers. In cases of heightened PF risk, LFIs should consider:

    - Subjecting the customer file to more frequent review and updating, including a manual review of transactions. All customer files should be reviewed on a risk-based schedule. For customers presenting the highest PF-related risks, reviewing the file as frequently as every six or nine months may be appropriate. This review should also include a review of substantial transactions on the account to ensure that they are consistent with information provided by the customer regarding expected activity and the jurisdiction(s) where it conducts business or has physical presence.

    - Applying risk-based transaction monitoring rules calibrated to address specific PF risks and typologies. Where automated transaction monitoring systems allow it, LFIs should apply PF-specific monitoring rules to all customers. These rules should have more sensitive thresholds for alerts.

    - Requiring pre-approval for atypical transactions. It may be appropriate for LFIs to require pre-approval from the compliance function for any transactions that falls out of the customer's ordinary behavior, that not correspond with the nature of customer's business, or that involve dealings in a new jurisdictions of PF concern, taking into consideration the LFI's defined risk appetite.

---

[33] For more information on PEPs, please refer to CBUAE's *Guidance for LFIs on the Risks Relating to PEPs,* available at: https://www.centralbank.ae/media/tvdchxqk/amlcft-guidance-for-licensed-financial-institutions-on-the-risks-relating-to-politically-exposed-persons.pdf

4.4.2. Transaction Monitoring and Suspicious Transaction/Activity Reporting

4.4.2.1. Transaction Monitoring

Under Article 16 of the AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of an STR or SAR. Moreover, as required by Article 7 of the AML-CFT Decision, LFIs must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity, and the risks they pose, including, when necessary, the source of funds. As with all customer types, LFIs that use automated monitoring systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behavior. When monitoring and evaluating transactions, the LFI should take into account all information that it has collected as part of CDD.

On a risk basis, LFIs should embed PF-specific indicators, typologies, and scenarios into their transaction monitoring systems to identify red flags, such as:

- Unusual patterns of transactions, such as round-tripping or layering;

- Transactions involving high-risk jurisdictions or individuals;
- Transactions involving dual-use goods or technology;
- Transactions involving front or shell companies;
- Transactions involving cash or non-face-to-face transactions;
- Transactions involving unusual or non-commercial routes or channels;
- Transactions that are inconsistent with the customer's business profile;
- Transactions that are inconsistent with expected transaction patterns; and
- Transactions originating from or associated with suspicious IP addresses or IP addresses located in high TF/PF risk jurisdictions.

Finally, LFIs should ensure that transaction monitoring systems include rules or scenarios designed to detect the above risk indicators and other transactions associated with PF and PF-related financial crimes that may involve third-party activity through the LFI's account or relationship. Furthermore, it is imperative that the PF risk be incorporated into the LFI's typology assessment in order to assess an LFI's PF risk exposure as well as current and prospective automated transaction monitoring controls. Of note, emerging technologies such as data analytics and artificial intelligence have considerably enhanced transaction monitoring capabilities within LFIs. The use of this emerging technology can prove a powerful tool in detecting new patterns of suspicious behaviors and activities related to PF.

4.4.2.2. Suspicious Transaction Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file a suspicious transaction report ("STR"), suspicious activity report ("SAR"), or other report types with the UAE Financial Intelligence Unit ("FIU") when they have reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.[34] Beyond the filing of STRs/SARs, it is crucial that LFIs cooperate with law enforcement and intelligence authorities to effectively combat PF networks.

[34] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

4.4.3. Targeted Financial Sanctions Obligations

The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the competent authorities of the UAE for implementing the decisions issued by the UNSC under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, the Cabinet Decision No. (74) of 2020 sets out the legislative and regulatory framework regarding TFS, including the Local Terrorist List and the UN Consolidated List.

In addition, under Article 21 of the AML-CFT Resolution No. (74) of 2020, LFIs are required to have suitable risk management systems and take sufficient measures to identify whether a customer, or the beneficial owner of a customer, has been added to an international sanctions list or the Local List. LFIs are required to conduct screening prior to onboarding and on an ongoing basis, as discussed under section 3.4.1 above.

Federal Law (50) of 2020 regarding goods subject to import and export controls contains the UAE list of dual-use and PF-sensitive goods. Lists of controlled chemical and non-chemical goods can be found on the EOCN website at: https://www.uaeiec.gov.ae/en-us/control-list-good.

For more information and details on their obligations in relation to their sanction obligations, LFIs should consult the EOCN's *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*[35] and the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*" and *Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*.[36]

As a best practice, LFIs should maintain an internal watchlist of parties that are related to sanctioned persons or entities or that pose elevated risk to the LFI for other illicit finance-related reasons. LFIs should consider implementing such lists and screening against these lists during customer onboarding and on an ongoing basis thereafter. In addition, following a sanctions designation, further intelligence can be derived from an investigation into any linkages with a sanctioned party. This could include reviewing past transactions to identify the designated individuals and entities operating before they were sanctioned.

---

[35] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.
[36] Available at: https://www.centralbank.ae/en/cbuae-amlcft

4.4.3.1. Confirmed Matches

If an LFI identifies a confirmed match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List is identified, LFIs are required to take the following actions:

- Implement all necessary measures without delay as outlined in Article 15 of Cabinet Resolution No. (74) of 2020, to include freezing without delay, refraining from offering any funds or other assets and services, and reporting freezing measures to the EOCN and CBUAE; and

- If the confirmed match is a potential customer, reject the transaction immediately and report the case.[37]

Per section (5) of Article 21 of Cabinet Resolution No. (74) of 2020, LFIs are expected to report any freezing measures, prohibition to provide funds or services, and any attempted transactions immediately via the goAML platform by selecting the Funds Freeze Report ("FFR") option. LFIs should also ensure that all necessary information and documents regarding the confirmed match are submitted along with the FFR. Pursuant to Section (1) of Article 22 of Cabinet Resolution No. (74) of 2020, supervisory authorities should receive all information within five working days.

---

[37] See also EOCN, *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*, section 4, available at: https://www.uaeiec.gov.ae/en-us/un-page?p=7

4.4.3.2. Partial Name Matches

If an LFI identifies a partial name match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List is identified, LFIs should take the following actions:

- Cross-check the identifiers published on the relevant sanctions list with the LFI's internal customer, beneficial ownership, and other data as well as external sources where appropriate to determine whether the partial name match is a confirmed match or can be waived as a false positive;

- If the LFI is unable to determine whether the partial name match is a confirmed match or a false positive, the LFI should suspend any transaction and report the case under Partial Name Match Report ("PNMR") through the goAML platform to the EOCN and the CBUAE and uphold the suspension measures until a response is received from the EOCN on the status of the partial name match.

LFIs are expected to submit a PNMR through the goAML platform within five business days of implementing the suspension measures. LFIs should ensure that all necessary information and documents regarding the potential match are submitted with the PNMR.

4.4.4. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces and organized in accordance with the "three lines of defence" model. All three lines of defence should report up to and have the active support and oversight of the LFI's senior management, defined broadly to include executives, senior leadership, and the Board of Directors. Furthermore, Management Information and Reports related to PF alerts and internal investigations should be provided to senior management to enhance their understanding of the severity or scale of PF risks to the institution. Flagging alerts and investigations related to PF would enable Governance and Audit functions to accurately review and assess how the institution's PF controls are functioning and enable deficiencies to be addressed. See section 8 of the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* for additional detail.[38]

[38] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

4.4.5. Training

As with all risks to which the LFI is exposed, the CPF training program should ensure that employees are aware of the risks related to PF, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls.

Training should be tailored and customized to the LFI's risk and the nature of its operations and should be clearly documented in the LFI's CPF compliance program and associated training policies, procedures, plans, materials, and attendance records.

Overall, LFIs should conduct periodic assessments of their training curriculum to ensure that the training remains relevant in the face of evolving PF risks.

4.4.6. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures, as well as records, documents, data, and statistics for all financial transactions, records obtained through CDD measures and ongoing monitoring (including copies of personal identification documents), account files and business correspondence, and STRs/SARs and results of any analysis performed.

LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs should make the records available to the competent authorities immediately upon request. Consistent with local regulatory requirements, all LFIs should ensure compliance with FATF's Recommendation 11: Record Keeping.

The aforementioned provisions also require that all records be retained for at least five (5) years from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

5. Export Controls

5.1. General

Export controls regimes around the world are essential in preventing the unauthorized transfer of items and technologies that could be used in WMD proliferation. LFIs play a crucial role in ensuring compliance with export control laws and regulations, as they are often involved in processing and facilitating the financing and settlement aspects of international trade transactions. By understanding and complying with export controls, FIs can help in mitigating the UAE's risks of PF.

While sanctions themselves do sometimes include specific technology or arms related restrictions, export controls are typically administered through authorities other than sanctions authorities. They are generally designed to control access to sensitive technologies and items that may have military application or the potential for dual-use and implicate LFIs to the extent that they prohibit the financing of prohibited exports.

LFIs should be familiar with the regulatory framework and international standards related to export controls associated with CPF. Among others, LFIs should be acquainted with the following:

- **National export control laws:** LFIs should understand the export control laws and regulations applicable in the UAE, including the relevant lists of controlled items, technology, and services.[39] The national bodies responsible for implementing export controls include:
    - Executive Office for Control and Non-Proliferation (EOCN);
    - Ministry of Defence (MOD);
    - Federal Authority for Nuclear Regulation ("FANR"), regulating export controls of nuclear goods;
    - Federal Authority of Identity, Citizenship, Customs and Port Security ("ICP"); and
    - Security Industry Regulatory Agency ("SIRA").
- **International export control regimes:** LFIs should be aware of international export control regimes such as the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime. These regimes provide guidelines and control lists to regulate the export of sensitive goods and technologies.
- **United Nations Security Council Resolutions:** LFIs should also be familiar with the relevant UNSCRs that impose sanctions and export controls on specific countries or entities involved in proliferation activities.

[39] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=1852fefa-f0a7-4629-9515-78c13fd7354e

5.2. Dual-Use or Controlled Goods

The EOCN plays an active role in implementing export controls besides curbing the proliferation of weapons of mass destruction with relevant associated technology, based on policies, legislations and partnerships domestically and internationally.[40]

In cases where trade-based transactions potentially involve dual-use or controlled goods, LFIs should screen against the UAE Control List pursuant to Cabinet Resolution No. (50) of 2020 for potential matches and follow the steps set forth in the EOCN's *Guidance on Counter Proliferation Financing for FIs, DNFBPs and VASPs*, section 6.[41]

Cabinet Resolution (50) of 2020 regarding commodities subject to import and export controls contains the UAE's list of dual-use and PF-sensitive goods. LFIs should consider screening for dual-use and other controlled goods when trade finance products involving international trade transactions are being offered. Lists of controlled chemical and non-chemical goods, which includes dual-use goods associated with the proliferation of WMDs, can be found on the EOCN's website[42], and LFIs are encouraged to consult with the EOCN to ascertain whether commodities are subject to export controls or other restrictions, and where applicable verify availability of valid permit from relevant authorities for transactions involving dual-use goods. Lastly, during the recording of and monitoring of transactions associated with, or suspected to be associated with dual-use goods, LFIs should consider leveraging the standardized numerical method of classifying traded products, like the Harmonized System ("HS"), which is a standardized numerical method of classifying traded products.

---

[40] See: https://www.uaeiec.gov.ae/en-us/about-us

[41] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=1852fefa-f0a7-4629-9515-78c13fd7354e

[42] Information available at: https://www.uaeiec.gov.ae/en-us/control-list-good

Annex 1. Select PF Threats Relevant to LFIs

Proliferators may procure licit and illicit goods, and the technology needed for the development of WMD capabilities and related delivery mechanisms. This Annex aims at assisting LFIs in identifying potential PF threats in order to mitigate the related risks.

The following is a list of several potential threats related to products and services that LFIs might offer, or that otherwise can be used for PF purposes.[43]

Financial Products and Services Directly Related to Trade in Proliferation-Sensitive Goods
Use of trade finance products and services and clean payment services in procurement of proliferation-sensitive goods.
Use of front companies, shell companies or brokers to obtain trade finance products and services or as parties to clean payments.
Use of companies to provide unlicensed money remittance services.
Nationals or dual citizens of proliferating states, or family members of such persons (regardless of citizenship), used as intermediaries in countries not of proliferation concern to facilitate procurement of goods and/or for payment of funds. Likely to involve use of personal banking products.
Use of universities or research centers to procure dual-use goods and/or for payment of funds, including Iranian and Syrian institutions.
Money transfer services used to conduct cash transfers related to procurement of goods.
Use of third countries to channel financial transactions related to mining deals. Use of professional intermediaries and firms to mask parties to transactions and end users.
Use of personal accounts to purchase industrial items. Use of non-specific, innocuous or misleading descriptions of goods or purpose of payments.
Use of fake or fraudulent documents related to shipping, customs or payments to facilitate transactions or trade finance.
Use of financial routes that are circuitous to the movement of sensitive goods or to countries not of proliferation concern. Use of vessels that do not attract proliferation concern to obtain maritime or cargo insurance products.
Use of shipping companies, brokers and agents to obtain insurance or other financial services related to maritime transport. Often combined with use of front companies with opaque ownership structures.

The following is a list of underlying licit and illicit activities that LFIs' customers might be engaged in that can potentially be linked to PF efforts:

Licit and Illicit Revenue-Raising Activities
Arms trafficking (small and conventional) used by state and non-state actors to raise revenue.
Sale of non-nuclear arms, military equipment or technologies, or paramilitary equipment or technologies by proliferating states to other states.
Sale of coal used by state and non-state actors to raise revenue.
Construction industry and/or related trades owned or operated by or on behalf of nationals or dual citizens of North Korea or North Korean entities. Profits from payment of contracts form part of North Korea's revenue-raising activities.
Cross-border smuggling of cash, gold or other high-value goods by mules to support state and non-state proliferation activities.
Cross-border smuggling of cash, gold or other high-value goods in diplomatic bags by diplomats or consular officers to support state proliferation activities.
Cybercrime, such as hacking accounts to obtain value, largely used by state actors.
Drug trafficking by state and non-state actors, including through connections with organized criminal networks. Proceeds used to support proliferation activities.
Export of art or statues by North Korea or involving North Korean designated entities and individuals to raise revenue.
Sale of minerals (gold, iron, steel, copper, zinc and so on) by North Korea or involving North Korean designated entities and individuals to raise revenue.
Payments made to laborers or workers (nationals or dual citizens) from North Korea. Payments are then largely confiscated by North Korea as part of its revenue-raising activities.
Restaurants or other small to medium-sized, largely cash-based businesses owned or operated by or on behalf of nationals or dual citizens of North Korea. Profits from businesses are sent to North Korea as part of its revenue-raising activities.
Export of seafood originating from North Korea or involving North Korean designated entities and individuals.
Export of textiles originating from North Korea or involving North Korean designated entities and individuals.
Wildlife trafficking by state and non-state actors including through connections with organized criminal networks.
'Taxes' and 'duties' collected by terrorist groups in controlled areas, as well as donations made to terrorist groups, as part of revenue-raising activities to support procurement of WMD materials, particularly radiological, chemical, or biological weapons.

The following is a list of financial and non-financial products, services, entities, and methods that can be used for PF activities:

Financial and Corporate Infrastructure in Support of the Movement of Finances and Goods
Use of banks and other financial institutions with foreign branches operating in countries of proliferation concern.
Use of cryptocurrencies to avoid the formal financial system.
Use of diplomats, consular officers or diplomatic or consular missions of North Korea to build networks, including corporate networks, within a country. These networks then facilitate a range of revenue-raising activities as well as facilitating financial products or services related to trade in goods.
Use of local branches of banks and financial institutions based in countries of proliferation concern.
Money-exchange businesses used for cash transfers in support of proliferation networks, where transfers involve individuals or entities owned or controlled by proliferation actors. Can also involve structured payments to organized crime networks involved in revenue-raising activities.
Use of hawala or bartering systems of value transfer to pay and settle debts among members of a proliferation network.
Use of a ledger payment system among members of a network that minimizes the need for international financial transactions. Banks may be used to facilitate some end-of-term settlements between companies and/or individuals.

Financial institutions with known histories of providing accounts to, or otherwise facilitating, financial activities of proliferation states.
Use of companies to provide unlicensed money-transfer services among members of networks or to conduct ad hoc transactions.
Use of professional intermediaries and corporate service providers to mask the presence of proliferation actors.
Use of trade or other economic relations of countries with links or significant exposure to a proliferating country. Often facilitated by a complex corporate network.
Use of organized or transnational crime networks, particularly their transport corridors and intermediaries in their networks.
Establishment of corporate networks that facilitate but may not be solely involved in PF activities. Ultimate beneficial ownership, connections and control structures are opaque.

[43] Royal United Services Institute for Defense and Security Studies, *Guide to Conducting a National Proliferation Financing Risk Assessment*, May 2019, available at: https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf

Annex 2. FATF PF Typologies

This Annex includes FATF PF typology reports which can help LFIs develop an understanding of the issues surrounding PF and assist them in identifying and analyzing the existing PF threats and the methods used by the proliferators and the facilitators.

Some sources provide lists of "red flag" indicators for FIs to employ in detecting potential connections to proliferation, even though these are not uniquely determinative of proliferation financing (proliferation financing activities may share similar traits with money laundering, especially trade-based money laundering, and terrorist financing activities).

Indicators listed in Annex 1 of the FATF Typologies Report[44] include:

- Transaction involves person or entity in foreign country of proliferation concern.
- Transaction involves person or entity in foreign country of diversion concern.
- The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of e port control contraventions.
- Customer activity does not match business profile, or end-user information does not match end-user's business profile.
- A freight forwarding firm is listed as the product's final destination.
- Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (*e.g.*, semiconductor manufacturing equipment being shipped to a country that has no electronics industry).
- Transaction involves possible shell companies (*e.g.*, companies do not have a high level of capitalization or displays other shell company indicators).
- Transaction demonstrates links between representatives of companies exchanging goods *i.e.*, same owners or management.

- Circuitous route of shipment (if available) and/or circuitous route of financial transaction.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (*e.g.*, does the country involved normally export/import good involved?).
- Transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination, etc.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- Customer vague/incomplete on information it provides, resistant to providing additional information when queried.
- New customer requests letter of credit transaction awaiting approval of new account.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Stealing funds or sensitive information through cyber operations to finance proliferation activities.
- Employing cryptocurrencies and other digital assets to evade traditional financial tracking system (*e.g.,* through the theft of virtual assets and the mining of cryptocurrencies through crypto-jacking).
- Involvement of company service providers, lawyers, accountants, and financial advisors in the creation or management of companies and other legal persons or legal arrangements to structure transactions and corporate entities in ways that obscure proliferation financing.

---

[44] Financial Action Task Force, Proliferation Financing Report (June 2008) https://eurasiangroup.org/files/FATF_docs/Typologies_Report_on_Proliferation_Financing.pdf

Annex 3. EOCN PF Risk Indicators

As per the EOCN's *2023 Terrorist & Proliferation Financing Red Flags Guidance*[45] which presented a number of PF-related risk indicators that LFIs should consider in identifying, understanding, assessing, and mitigating PF risks, he following sections present relevant risk indicators concerning customer risk, transactional risk, and risks specific to the maritime sector and trade finance activity:

Customer Risk Indicators

- During onboarding, a customer provides vague or incomplete information about their proposed trading activities. The customer is reluctant to provide additional information about their activities when queried;

- During subsequent stages of due diligence, a customer, particularly a trade entity, or its owners or senior managers, appears in sanctioned lists or negative news, e.g., relating to past ML schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including appearing on a list of denied persons for the purposes of export control regimes;

- A customer is a person connected with a country of proliferation or diversion concern, e.g., through business or trade relations, as identified through the national risk assessment process or by relevant national CPF authorities;

- A customer is a person dealing with Dual-Use goods, goods subject to export control goods, or complex equipment for which he/she lacks technical background, or that is incongruent with their stated line of activity;

- A customer engages in complex trade deals involving numerous third-party intermediaries in lines of business that do not accord with their stated business profile established at onboarding;

- A customer or counterparty, declared to be a commercial business, conducts transactions that suggest that they are acting as a money remittance business or a pay-through account; These accounts involve a rapid movement of high-volume transactions and a small end-of-day balance without clear business reasons. In some cases, the originators appear to be entities who may be connected with a state-sponsored proliferation programme (such as shell companies operating near countries of proliferation or diversion concern), and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls;

- A customer affiliated with a university or research institution is involved in the trading of Dual-Use goods or goods subject to export control;

- A customer's activity does not match the customer's business profile, or end-user information does not match the end-user's business profile; and

- A new customer requests a letter of credit transaction while awaiting approval of new account.

Transactional Risk Indicators

- A transaction involves person or entity in foreign country of proliferation concern;

- A transaction involves person or entity in foreign country of diversion concern;

- A transaction involves financial institutions with known deficiencies in AML/CFT controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws;

- Wire transfer activity shows unusual patterns or has no business or apparent lawful purpose;

- The originator or beneficiary of a transaction is a person or an entity ordinarily resident of or domiciled in a country of proliferation or diversion concern, e.g., DPRK and Iran;

- Accounts or transactions involve possible companies with opaque ownership structures, front companies, or shell companies, e.g., companies do not have a high level of capitalisation or display other shell company indicators. Countries or the private sector may identify more indicators during the risk assessment process,

such as long periods of account dormancy followed by a surge of activity;

- Business or compliance personnel identify links between representatives of companies exchanging goods, e.g., the same owners or management, physical address, IP address, or telephone number, or activities that appear to be co-ordinated;

- The account holder conducts financial transactions in a circuitous manner.

- A transaction or account activity involves an originator or beneficiary that is domiciled in a country with weak implementation of relevant UNSCR obligations and FATF Standards or a weak export control regime (also relevant to correspondent banking services);

- A customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or for trade transactions more generally. For financial institutions, the transactions are visible through sudden influ es of cash deposits to the entity's accounts, followed by cash withdrawals;

- Transactions are made on the basis of "ledger" arrangements that obviate the need for frequent international financial transactions. Ledger arrangements are conducted by linked companies that maintain a record of transactions made on each other's behalf;

- Occasionally, these companies will make transfers to balance these accounts;

- A customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business;

- Account holders conduct transactions that involve items controlled under Dual-Use or export control regimes, or the account holders have previously violated requirements under Dual-Use or export control regimes; and

- Transactions associated with a customer's frequent travel to or from high-risk countries associated with proliferation activities.

Maritime Sector Risk Indicators

- An order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user;

- A trade entity is registered at an address that is likely to be a mass registration address, e.g., high-density residential buildings, post-box addresses, commercial buildings, or industrial complexes, especially when there is no reference to a specific unit;

- The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination;

- The destination of a shipment is different from the importer's location;

- Inconsistencies are identified across contracts, invoices, or other trade documents, e.g., contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume, or value of the actual commodities and their descriptions;

- A shipment of goods has a low declared value vis-à-vis the shipping cost;

- A shipment of goods is incompatible with the technical level of the country to which it is being shipped, e.g., semiconductor manufacturing equipment being shipped to a country that has no electronics industry;
- A shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet;
- A shipment of goods is inconsistent with normal geographic trade patterns, e.g., the destination country does not normally export or import the goods listed in trade transaction documents;
- A shipment of goods is routed through a country with weak implementation of relevant UNSCR obligations and FATF Standards, weak export control laws, or weak enforcement of export control laws; and
- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons, e.g., by a shell or front company not involved in the trade transaction.

Trade Finance-Related Risk Indicators

- A trade finance transaction involves a shipment route (if available) through a country with weak export control laws or weak enforcement of export control laws;
- A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws;
- A transaction involves a shipment of goods inconsistent with normal geographic trade patterns (e.g., does the country involved normally export/import good involved?);
- Based on the documentation obtained in the transaction, the declared value of the shipment is obviously under-valued vis-à-vis the shipping cost;
- Prior to account approval, the customer requests a letter of credit for a trade transaction to ship Dual-Use goods or goods subject to export control;
- Lack of full information or inconsistences are identified in trade documents and financial flows, such as names, companies, addresses, final destination, etc.;
- Identifying documents seem to be forged or counterfeited;
- Identifying documents seem to be tampered or modified documents with no apparent explanation, especially those related to international trade; and
- Transactions include wire instructions or payment details from or due to parties not identified on the original letter of credit or other documentation.

---

[45] Terrorist & Proliferation Financing Red Flags Guidance: Published by the EOCN in September 2023 Updated: December 2023

Annex 4. FATF Potential Indicators of Sanctions Evasion Activity (Mentioned in Third-Party Reports)

This Annex provides a list of indicators that can help LFIs identify and detect suspicious PF activities, including those related to the evasion of TFS imposed under UNSCRs or local designations.

The February 2018 FATF Guidance on Counter Proliferation Financing[46] listed additional potential indicators of sanctions evasion activity mentioned in third-party reports (*e.g.*, UN Panel of Experts reports, Study of Typologies of Financing of WMD Proliferation[47]):

- Involvement of items controlled under WMD export control regimes or national control regimes.
- Involvement of a person connected with a country of proliferation concern (*e.g.*, a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.
- Use of cash or precious metals (*e.g.*, gold) in transactions for industrial items.
- Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.
- Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.
- Transactions between companies on the basis of "ledger" arrangements that obviate the need for international financial transactions.
- Customers or counterparties to transactions are linked (*e.g.*, they share a common physical address, IP address or telephone number, or their activities may be coordinated).
- Involvement of a university in a country of proliferation concern.
- Description of goods on trade or financial documentation is non-specific, innocuous or misleading.
- Evidence that documents or other representations (*e.g.*, relating to shipping, customs, or payment) are fake or fraudulent.
- Use of personal account to purchase industrial items.

---

[46] Financial Action Task Force, FATF Guidance on Counter Proliferation Financing (February 2018), available at: https://www.fatf-gafi.org/en/publications/Financingofproliferation/Guidance-counter-proliferation-financing.html.
[47] Available at: https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf

Annex 5. EOCN PF Sanctions Evasion Red Flags and Typologies

This Annex provides a list of indicators, as identified by the EOCN, that can help LFIs identify and detect suspicious PF activities related to sanctions evasion.

Below is a list of UAE-specific PF sanctions evasion red flags indicators identified by the EOCN[48]:

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.

- Dealings with sanctioned goods or under embargo. For example:
    - Oil or other commodities
    - Dual-Use items (wire nickel, inverters, etc.)
- Identifying documents that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
    - For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
    - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.

[48] Available at: https://www.uaeiec.gov.ae/en-us/un-page?p=3#

Annex 6. PF-Related Reasons for Reporting

This Annex aims at assisting LFIs in drafting potential SARs or STRs by providing PF-related Reasons for Reporting (RFRs) to accurately characterize reportable activity, as per the guidance of the UAE FIU.

goAML PF-related RFRs
A shipment of goods is incompatible with the known business activity and nature of products or services provided by the entities involved in the transaction.
A shipment of goods is made in a circuitous fashion (if information is available), including multiple destinations with no apparent business or commercial purpose, indications of frequent flags hopping, or using a small or old fleet. Possible TBML.
A transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.
Based on the documentation obtained in the transaction, the declared value of the shipment is obviously under-valued vis-à-vis the shipping cost. (Possible TBML).
Customer or transaction is suspected of being linked (directly or indirectly) to DPRK's nuclear-related, WMD-related, or ballistic missiles weapons program.
Customer or transaction is suspected of being linked (directly or indirectly) to IRAN's nuclear weapons program.
Customer or transaction is suspiciously involved in the supply, sale, delivery, export, or purchase of dual-use, controlled, or military goods to countries of proliferation concerns or related to illegal armed groups.
Sender or originator appears to be entities who may be connected with a state-sponsored proliferation program and the beneficiaries appear to be associated with manufacturers or shippers subject to export controls.
The customer uses a personal account to purchase industrial items that are under export control, or otherwise not associated with corporate activities or congruent lines of business.

The person or entity preparing a shipment lists a freight forwarding firm as the product's final destination. Possible TBML.
Trade finance transaction(s) involving shipment route through country with weak export control laws or weak enforcement of export control laws.
Transaction involves sale, shipment, or export of dual-use goods incompatible with the technical level of the country to which it is being shipped.

Annex 7: Synopsis of the Guidance

Purpose and applicability of this Guidance	**Purpose**	The purpose of this Guidance is to assist the understanding and effective performance by CBUAE licensed financial institutions (LFIs) of their statutory obligations related to counter proliferation financing (CPF) under the legal and regulatory framework in force in the UAE.
	Applicability	This Guidance applies to all natural and legal persons, which are licensed and/or supervised by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers; and insurance companies, agencies, and brokers.
Understanding ML/TF Risks Related to PF	**Threats Related to PF:**	▪ PF threats and related sources of funding mainly derive from three categories, i.e., financial products directly related to trade in PF-sensitive goods; revenue-raising activities; and the use of financial and corporate structures to support movement of funds and cash. ▪ PF threats can be posed by state and non-state actors attempting to obtain WMD and their delivery systems or raising, moving, or using funds to procure such items. Under the FATF Standards, PF threats and CPF requirements are provided under: (i) UNSCR 1540 (2004), regarding non-state actors; (ii) UNCSRs 1718 (2006), 2087 (2013), 2094 (2013). and 2270 (2016), regarding the Democratic People's Republic of North Korea ("DPRK" or "North Korea"); and (iii) UNCSR 2231 (2015), regarding the Islamic Republic of Iran ("Iran").
	Other Select Threats Relevant to LFIs	▪ **Financial Products and Services Directly Related to Trade in Proliferation-Sensitive Goods**, including: (i) Nationals or dual citizens of proliferating states, or family members of such persons used as intermediaries in countries not of proliferation concern to facilitate procurement of goods and/or for payment of funds; (ii) Use of universities or research centers to procure dual-use goods and/or for payment of funds; ▪ **Licit and Illicit Revenue-Raising Activities**, including (i) Arms trafficking (small and conventional) used by state and non-state actors to raise revenue; (ii) Sale of non-nuclear arms, military equipment or technologies, or paramilitary equipment or technologies by proliferating states to other states; (iii) Construction industry and/or related trades owned or operated by or on behalf of nationals or dual citizens of North Korea or North Korean entities; (iv) Cybercrime, such as hacking accounts to obtain value, largely used by state actors, and (v) Export of art or statues by North Korea or involving North Korean designated entities and individuals to raise revenue, (vi) Export of seafood and textiles originating from North Korea or involving North Korean designated entities and individuals, and (vii) Restaurants or other small to medium-sized, largely cash-based businesses owned or operated by or on behalf of nationals or dual citizens of North Korea.

		▪ **Financial and Corporate Infrastructure in Support of the Movement of Finances and Goods**, including: (i) Use of diplomats, consular officers or diplomatic or consular missions of North Korea to build networks, including corporate networks, within a country; (ii) Use of organized or transnational crime networks, particularly their transport corridors and intermediaries in their networks, and (iii) Use of professional intermediaries and corporate service providers to mask the presence of proliferation actors.
	Vulnerabilities Related to PF	▪ LFIs vulnerabilities associated with PF, : **(i) Trade finance** transactions, where trade-based illicit finance may facilitate the purchase or transfer of goods and services used in procurement of WMDs; **(ii) Correspondent banking** relationships, and nested relationships where heightened PF risk is present insofar as it can involve the rapid and repeated transfers of large quantities of funds on behalf of parties that are not the direct customers of the correspondent; **(iii) Hawala and other alternatives to traditional banking**, in particular unlicensed hawala providers (UHP), MSBs, VASPs and new technologies, where illicit actors may exploit these alternatives to traditional banking channels to transfer funds to proliferators; **(iv) Offshore accounts** can be abused given the opacity and complexity of cross-jurisdictional regulations to obscure the trail of funds; **(v) Free trade zones**, in which incentives are offered sometimes without the appropriate AML/CFT safeguards, relaxed oversight, week inspection procedures and adequate coordination with other authorities; **(vi) Shell and front companies and complex ownership structures**, which can be ideal vehicles for nefarious actors to conduct illicit activities and conceal their true identities; **(vii) Insurance and reinsurance**, which may be susceptible to abuse by illicit actors insofar as they are seeking to move goods and funds, insure illicit activities and goods, or manipulate insurance claims to obtain funds for PF purposes; **(viii) Non-profit organization (NPOs) and charities** may be used to provide financial support to entities or individuals involved in proliferation activities; **(ix) Real estate** sector, may be susceptible to abuse by nefarious actors seeking to conceal illicit funds in real estate transactions, and **(x) Dealers in precious metals and stones (DPMS)**, particularly those involved in gold trade given their intrinsic characteristics, such as high value, ease of trade, mutability, portability, liquidity, transferability, anonymity and availability in the UAE.
Mitigating PF Risks	PF Risk Assessment and Risk Based Approach	▪ Pursuant to Notice No. CBUAE/BIS/2023/5960, LFIs should perform, document, and keep up to date an institutional-level risk assessment that includes identifying, assessing, understanding and mitigating risks related PF, and have the appropriate mechanisms to provide PF risk assessment information to the CBUAE. Specifically, LFIs should consider PF risk factors arising in relation to their customers; products services and transactions; delivery channels; geographic locations and markets, and operating structures. ▪ PF risk management should be incorporated into an LFI's larger counter-illicit finance program, and institutions can use many of the same controls to mitigate and manage their PF risk that they already employ for ML/TF and sanctions purposes. Specifically, LFIs should consider: (i) The use of technology to detect sanctions evasion

		behavior; (ii) Incorporating PF-specific information in the CDD process; (iv) Including PF risk in correspondent banking risk-ratings and EDD, and (v) Training to the LFI's leadership and staff at all levels on PF related issues.
	Customer Due Diligence	**General CDD Measures**. The following elements of CDD must be carried out for all customers, no matter the customer type. ▪ Customer identification and verification ▪ Beneficial owner identification and verification ▪ Understanding the nature of the customer's business and the nature and purpose of the business relationship, including determining the nature of any VASP or VA activity ▪ Ongoing monitoring ▪ Sanctions screening
		Establishing a Customer Risk Profile that Incorporates PF Risks. LFI should collect information that allows it to create a risk profile of the customer that incorporates a customer's PF-specific risk attributes, including: ▪ Customer specific attributes, such as customers' background, ownership structure, involvement in high-risk sectors and connections to PEPs ▪ Transactional behavior, such as the transaction history, and unusual transaction patterns involving dual-use goods. ▪ Red flags and indicators, including involvement in sanctioned or embargoed countries, presence on watchlists or control lists, or connections to entities or individuals involved in proliferation activities. ▪ External factors, such as industry-specific risks, regulatory changes, or geopolitical developments that may impact the customer's risk profile ▪ Understand and assess the VASP's reputation.
		Enhanced Measures for Higher-Risk Customers ▪ **EDD for High-Risk Customers**: Where LFIs have identified indicators of heightened PF risk related to a customer, such as Customer that are PEPs, Business relationships in high-risk jurisdictions, and correspondent banking relationships, they should perform the following: (i) Obtain senior management approval before establishing a business relationship or continuing an existing one; (ii) Take risk-based measures to establish the source and destination of funds; (iii) Ascertain whether the customer conducts business in a high AML/CFT-risk jurisdiction, a jurisdiction of PF concern, or a third-party jurisdiction in close proximity to a jurisdiction of PF concern, and (iv) Conduct enhanced ongoing monitoring of the relationship.
	Transaction Monitoring and Suspicious Activity Reporting	**Transaction Monitoring**. In the context of PF risks, LFIs should ensure that transaction monitoring rules or keyword are embedded with PF-specific indicators, typologies, and scenarios into their transaction monitoring systems to identify red flags. **Suspicious Activity Reporting**. LFIs are required to file an STR or SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount,

		the proceeds of crime, are related to a crime, or are intended to be used in a crime.
Mitigating ML/TF Risks Related to VASP Customers and VA-Related Customer Transactions	Targeted Financial Sanctions Obligations and Freezing Without Delay	▪ The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the competent authorities of the UAE for implementing the decisions issued by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations ("UN") and the Cabinet Decision No. (74) of 2020 which sets out the legislative and regulatory framework regarding TFS, including the Local Terrorist List and the UN Consolidated List. LFIs are required to have suitable risk management systems and take sufficient measures to identify whether a customer, or the beneficial owner of a customer, has been added to an international sanctions list or the Local List. ▪ LFIs are required to conduct screening prior to onboarding and on an ongoing basis. ▪ LFIs should maintain an internal watchlist of parties that are related to sanctioned persons or entities or that pose elevated risk to the LFI for other illicit finance-related reasons.
	Training	As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks related to PF, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls.
	Governance and Independent Audit	The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces and organized in accordance with the "three lines of defence" model. All three lines of defence should report up to and have the active support and oversight of the LFI's senior management, defined broadly to include executives, senior leadership, and the Board of Directors. Furthermore, Management Information and Reports related to PF alerts and internal investigations should be provided to senior management to enhance their understanding of the severity or scale of PF risks to the institution.
	Record Keeping	▪ LFIs must maintain detailed records associated with their ML/FT/PF risk assessment and mitigation measures, as well as records, documents, data, and statistics for all financial transactions, records obtained through CDD measures and ongoing monitoring (including copies of personal identification documents), account files and business correspondence, and STRs/SARs and results of any analysis performed. ▪ **LFIs should make the records available to the competent authorities immediately upon request**.
UAE CPF Legal and Regulatory Framework	▪ Federal Decree Law No. (20) of 2018, Article 16.e.1 specifies that FIs and DNFBPs shall undertake "Prompt application of the directives when issued by the competent authorities in the state for implementing the decisions issued by the UN Security Council under Chapter (7) of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, and other related directives". ▪ Federal Decree-Law No. (20) of 2018, Article (28) of which provides for a penalty of imprisonment of no less than a year and no more than (7) years, or a fine of no less than AED 50,000 for anyone who violates any of the directives of Chapter 7 of the UN Convention for the Suppression of the Financing of Terrorism and Proliferation of WMD and other related directives.	

	▪ UAE Cabinet Decision No. (74) of 2020, Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions, wherein, inter alia, Article (11.1) designates the EOCN as a National Coordination body. ▪ **Federal Decree Law No. (43) of 2021**, on the Commodities Subject to Non-Proliferation, wherein prohibits or restricts certain commodities, requires the issuance of permits to trade such commodities, lays out obligations for the permit holder and establishes penalties for violation of said statute. ▪ **Federal Decree Law No. (13) of 2007**, on Items Subject to Import and Export Control and its Amendments, including Federal Law No. (12) of 2008. ▪ **Cabinet Resolution (50) of 2020**, on the Schedule of Strategic Items Attached to Federal Law (13) of 2007, which implements internationally agreed dual-use goods subject to import and export control.
UAE authorities involved in matters related to CPF	▪ **EOCN**: is the authority responsible for implementing the provisions of Federal Decree Law No. (43) of 2021 On the Commodities Subject to Non-Proliferation which replaces Federal Law No. (13) of 2007 Concerning Commodities Subject to Control of Import and Export. This is for the aim of preventing the illegal and unauthorized circulation of dual-use goods that contribute to the production or development of weapons of mass destruction, along with their associated technology and means of delivery. In cooperation with the Ministry of Foreign Affairs and International Cooperation (MoFAIC) and other government agencies exert extreme efforts in following up the application of the resolutions and requirements of the United Nations Security Council and other relevant international and regional organizations and coordinates to and supervises the application of targeted financial sanctions (TFS) relating to terrorist lists system, as well as the implementation of Security Council resolutions on the prevention and suppression of terrorism, its financing, the cessation of arms proliferation and financing, in addition to other relevant resolutions in coordination with competent stakeholders. ▪ **FANR**: is the regulatory authority responsible for overseeing the nuclear industry's compliance with Federal Law No. (6) of 2009, Concerning the Peaceful Uses of Nuclear Energy. ▪ **ICP**: was established in 2002 and is charged with implementing the UAE's unified customs law and executing the UAE's obligations under the Gulf Cooperation Council's (GCC) customs union.
Export Controls	Export controls regimes around the world are essential in preventing the unauthorized transfer of items and technologies that could be used in WMD proliferation. LFIs play a crucial role in ensuring compliance with export control laws and regulations, as they are often involved in processing and facilitating the financing and settlement aspects of international trade transactions.
Dual Use or Controlled Goods	In cases where trade-based transactions potentially involve dual-use or controlled goods, LFIs should screen against the UAE Control List pursuant to Cabinet Resolution No. (50) of 2020 for potential matches and follow the steps set forth in the EOCN's Guidance on Counter Proliferation Financing for FIs, DNFBPs and VASPs, section 6 ▪ LFIs should consider screening for dual-use and other controlled goods when trade finance products involving international trade transactions are being offered. Lists of controlled chemical and non-chemical goods, which includes dual-use goods associated with the proliferation of WMDs, can be found on the EOCN's website ▪ LFIs are encouraged to consult with the EOCN to ascertain whether commodities are subject to export controls or other restrictions, and where applicable verify availability of valid permit from relevant authorities for transactions involving dual-use goods ▪ LFIs should consider leveraging the standardized numerical method of classifying traded products, like the Harmonized System ("HS"), which is a standardized numerical method of

Guidance for Licensed Financial Institutions on Risks Related to Trade-Based Money Laundering ("TBML") and Transshipment

Effective from 7/11/2025 **Status:** In-Force

1. Introduction

As a major financial centre, trade is central to the United Arab Emirates ("UAE")'s economy. Situated at the crossroads of significant trade routes, the UAE's ports make the country an essential distribution hub in global supply chains and the international movement of goods. In addition, the UAE's commitment to business and commerce, as evidenced through the expansion of the country's Financial Free Zones ("FFZs") and Commercial Free Zones ("CFZs"), has led to the UAE playing an increasingly important role in global trade and the international financial system as a whole.

Accordingly, the UAE is exposed to illicit financing risks associated with trade, commonly referred to as "trade-based financial crime." Trade-based financial crime encompasses a wide range of illicit activities, including money laundering ("ML"), terrorist financing ("TF"), proliferation financing ("PF"), sanctions violations, illicit transshipment, and proliferation of weapons of mass destruction ("WMD"). This guidance ("Guidance") seeks to explore risks specifically associated with trade-based money laundering ("TBML") and illicit transshipment. The Guidance has been developed to assist licensed financial institutions ("LFIs") with identifying and understanding TBML and illicit transshipment activities, and to manage the risks associated with TBML and illicit transshipment.

LFIs are uniquely positioned to identify TBML activities and illicit transshipment and to report suspicious activity, which enables law enforcement to connect the dots in the often-fragmented sets of trade-related transactions. No single typology can be used to identify TBML or illicit transshipment activities, and as a result, LFIs should use a combination of the typologies highlighted (but not exhaustive) in this Guidance when designing or enhancing their policies, procedures, and processes.

1.1. Purpose and Scope of the Guidance

Article 44.13 of the *Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance of LFIs licensed by the Central bank of the United Arab Emirates ("CBUAE") of their statutory obligations under the legal and regulatory framework in force in the UAE, as detailed in Section 1.3 below. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, circulars, and notices, and outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"),[2] and red flag indicators identified by the FATF and other relevant international bodies.[3] These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

---

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft.
[2] For example, please *see*: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf.
[3] For example, please *see*: https://library.iccwbo.org/content/tfb/pdf/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers ("RHPs"); and
- Insurance and re-insurance companies, agents, and brokers.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");
- Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments; and
- CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

1.4. Acronyms and Definitions

Terms	Description
AML	Anti-money laundering
BAFT	Bankers Association for Finance and Trade
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence

CFT	Counter the financing of terrorism
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ICC	International Chamber of Commerce
LFI	Licensed financial institution
ML	Money laundering
RHP	Registered hawala provider
SAR	Suspicious activity report
SBML	Service Based Money Laundering
STR	Suspicious transaction report
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TBML	Trade-based money laundering
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council

Bank guarantee: A formal assurance from a lender or an LFI that a borrower will be able to pay its counterparty, irrespective if the borrower fails to perform against their obligations and pay the counterparty.

Buyer: A party to a trade transaction that purchases goods either for their direct use, to manufacture into another good, or for further resale.

Documentary trade finance products: Trade finance products that require a party to present certain documents to an LFI in order to trigger a payment obligation for the trade transaction.

Dual-use items: Items, including goods, technologies and software, that have both commercial and military applications, and/or contribute to the proliferation of weapons of mass destruction.

Forfaiting: A method in trade finance where exporters obtain cash by selling their receivables at a discount on a "without recourse" basis.

Import and export factoring: The process of purchasing account receivables from an exporter in one country and collecting the invoice value later from the importer in the second country.

Landlocked country: A sovereign state that lacks direct access to the seas.

Letter of credit: A letter issued by an LFI guaranteeing that the LFI will make a full payment for goods under specified conditions, namely, that the LFI will provide payment to a seller or supplier once the seller or supplier presents the documents that enable the buyer to take possession of the goods.

Non-documentary trade finance products: An arrangement that does not tie payment from an LFI to the presentation of all the documentation related to the trade.

Open account trade: A trade transaction in which the goods are shipped and delivered before payment is due, and invoices and shipping documents are sent directly from the supplier to the buyer, rather than through the banking system. The only role of an LFI is processing the payment, which may or may not indicate that it relates to a trade transaction.

Phantom shipping: A fraudulent technique used in TBML in which documents indicate that goods are shipped from a supplier/exporter to a buyer/importer when, in fact, no product has moved at all.

Seller or Supplier: A party to a trade transaction that sells goods to a buyer.

Structured trade finance: A type of debt finance that aims to reduce the gap between the time a manufacturer procures materials until the final product is sold to a consumer by structuring trade finance products across the

supply chain.

Trade finance: The provision of finance products, typically by LFIs, to facilitate movement of goods and services between two parties, either within a country or cross-border. In trade finance LFIs take on certain payment or supply risk.

Trade-based money laundering: The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origins or finance illicit activities.

Transshipment: The shipment of goods from the country of origin to one or more intermediate destinations prior to shipment to the country of ultimate destination.

2. Understanding and Assessing TBML

According to the FATF, illicit actors move funds for the purpose of hiding their illicit origin and integrating them into the formal economy through three main methods:[4]

- Moving value through the financial system (e.g., through wire transfers);
- Moving value through the physical movement of money (e.g., through the use of bulk cash smuggling or other valuable items like gold); or
- Moving value under the disguise of a transaction related to traded goods or services.

Due to strengthened controls related to the first two methods and the growth of global trade overall, TBML has become an attractive method for laundering funds. TBML is defined by the FATF as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins."[5] TBML therefore can be understood as the manipulation of trade transactions to disguise the true nature of the underlying financial activity and/or the identities of trade participants. In this Guidance, "trade transactions" refers to both domestic and international transactions involving the buying and selling of goods or services. As trade has become an attractive option for money launderers to disguise the proceeds of crime, the UAE faces a range of threats from a number of illicit actors—international organized criminal groups and third-party money launderers—seeking to exploit the UAE to engage in TBML.[6]

[4] FATF, *Guidance on Trade-Based Money Laundering*, 2006, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf
[5] Ibid.
[6] FATF, *United Arab Emirates Mutual Evaluation Report*, April 2020, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-United-Arab-Emirates-2020.pdf.coredownload.pdf

2.1. Background of International Trade System and Trade Finance

Over the past several years, the volume and the value of international trade have increased, and the value of global trade reached a record level of more than USD 32 trillion in 2022.[7] The UAE, in particular, has attracted an increase of goods and capital in recent years, as one of the world's largest exporters of goods and services[8], and a central logistics and trading hub in the Middle East.[9] The increasing volume of trade in the international economy is underpinned by an inherently complex, diverse, and complicated set of interconnected supply chains spanning the globe. For example, the transit of goods in a trade often involves several parties across multiple countries other than the supplier and buyer.

This Guidance seeks to detail the role of LFIs in detection and prevention of trade based financial crime. LFIs often facilitate trade transactions by: (i) providing financing (credit) through trade finance products, and (ii) settling payments for trade transactions, sometimes on an open account. **Trade finance** typically involves short-term financing to facilitate the movement of goods either within a country or cross-border. In this capacity, LFIs address the lack of trust between the parties in a trade transaction, provide financing to parties in need of capital, and take on the role of a guarantor. LFIs also facilitate trade transactions by transferring value from the buyer to the supplier when processing payments related to trade, whether as part of a trade finance settlement or on an open account.

In the following sections, this Guidance differentiates between **documentary trade finance** and **non-documentary trade finance,** and the role of LFIs across trade finance products. Each type of trade products carries specific risks, hence LFIs are required to implement controls based on the type of trade transaction, the level of information available and their role in the transaction.

---

[7] Global Trade Update (March 2023), UNCTAD, March 2023, available at: https://unctad.org/publication/global-trade-update-march-2023.
[8] UAE Ministry of Economy, *UAE ranks 11th globally in commodity exports in 2022 with a 41 per cent growth*, April 6, 2023, available at: https://www.moec.gov.ae/en/-/uae-ranks-11th-globally-in-commodity-exports-in-2022-with-a-41-per-cent-growth
[9] World Bank, *United Arab Emirates*, 2023, available at: https://thedocs.worldbank.org/en/doc/5bae5632e2d8425830fbf0bac721cce3-0280012021/original/17-mpo-sm21-united-arab-emirates-kcm3.pdf

2.1.1. Documentary Trade Finance

Traditional documentary trade finance products include **performance-based products**, such as letters of credit ("LCs"), in which payment is due once the supplier has performed according to contract terms and presents the required documents. Traditional documentary trade finance products also extend to **non-performance-based products**, such as guarantees and standby LCs, that provide compensation to one of the transacting parties in the event that a party fails to perform according to contract terms.

In documentary trade finance transactions, a party to the trade transaction approaches an LFI to open a documentary product, such as a LC, a documentary collection, or a guarantee. At the initiation stage, the parties agree on the conditions of the settlement and establish the documents a party should present to the LFI against the payment or acceptance. Once goods are shipped (or a supplier has failed to act), the beneficiary presents certain documents to the LFI in order to trigger a payment obligation. The LFI reviews the presented documents related to the underlying transfer of goods and pays the invoice (or a claim in the case of a guarantee), if it finds the documents conform with the terms of the agreement and applicable rules. Such documentation can include title and transport documents, bills of lading, invoices, packing lists, and certificates of origin or inspection.

Based on these documents, the LFI may have access to information relevant to identifying potentially suspicious activity. Even though transaction information may be difficult to verify based on the documents alone, the LFI may have information regarding the type and quantity of the underlying goods involved in shipment; the identity and location of the supplier and buyer; the vessel name and shipping company; and applicable shipping routes and destinations.

As a best practice, LFIs should review the presented documents to detect potential red flags or involvement of sanctioned parties once they are made available to an LFI and before processing a payment related to a trade finance product or instrument. If an irregularity is detected, LFIs should review the irregularity for indicators of potentially suspicious activity and report suspicious activity to the FIU. LFIs should also take appropriate follow-up measures to address the risk associated with the transaction in question and the parties involved, including if an LFI identifies a confirmed match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the United Nations Security Council ("UNSC") Consolidated List, as further discussed in Section 4.3 on Targeted Financial Sanctions Obligations.

2.1.1.1. Description of Documentary Trade Finance Products and Instruments

There are several types of documentary trade finance products that differ in payment terms, presented documents, LFI's involvement, and other characteristics. LCs and bank guarantees, two of the most prevalent types, are discussed in further detail below. However, all trade finance products, even if not explicitly referenced in this guidance, can be exploited in TBML. Therefore, it is important for an LFI to assess the types of products it offers, their characteristics, and mitigating measures the LFI can apply to such products based on principles discussed in Section 4.

2.1.1.1.1. Letters of Credit

An LC is a letter from an LFI guaranteeing that the LFI will make a full payment to the supplier once the supplier presents the documents that confirm their performance and that would allow the buyer to receive the ownership of goods and services. If the supplier presented the full and correct documents and the buyer is unable to make a payment on the agreed-upon date, the LFI will be required to cover the full or remaining amount of the purchase. There are different types of LCs, **commercial LCs, standby LCs,** and **bank guarantees**, discussed in further detail below:

(1) Commercial LC (also known as a documentary LC or simply an "LC"): Commercial LCs are extensively used as a means of payment in cross-border or domestic trade. The buyer's LFI (i.e., the issuing bank) pays a pre-determined amount to the supplier's LFI (i.e., the advising bank) upon presentation of certain pre-agreed documents that prove that the goods were shipped by the supplier. Since the terms of each LC could be different, different documents might be presented as part of the trade transaction. These documents contain information about the underlying trade that should be used by LFIs to determine the legitimacy of the transaction. These documents are discussed in Section 2.1.1.2 Types of Documents Available in Documentary Trade Finance Instruments.

Commercial LCs can have many other variations, as follows:

Revocable versus Irrevocable LC	**Irrevocable LC** means that the LC cannot be cancelled or amended unless all parties to the LC agree to do so (i.e., the buyer and the supplier). **Revocable LC** allows the buyer or the buyer's LFI (i.e., issuing bank) to amend or cancel the LC at any time and without notice to the supplier, and as a result of these conditions, revocable LCs are less common than an irrevocable LC.
Confirmed versus Unconfirmed LC	**Unconfirmed LC** is a type of the LC where only the buyer's LFI (i.e., issuing bank) guarantees performance. **Confirmed LC** is used when a supplier would like additional assurances of performance under the LC. In this case, the supplier can ask a reputable LFI or its own LFI to add a confirmation to the LC. With a confirmed LC, even if the buyer's LFI (i.e., issuing bank) fails to pay, the LFI that has confirmed the LC has to make the payment against complying presentation of the documents presented by the supplier.
Transferable versus Non-transferable LC	**Transferable LC** is a type of LC where the beneficiary can transfer all or part of the payment due under the LC to another party (i.e., a second beneficiary). **Non-transferable LC**, by definition, means that the LC cannot be transferred.

(2) **Standby LC**: In contrast to a commercial LC, standby LCs serve as a secondary payment method (i.e., it will only be called upon when one of the parties to a standby LC fails to perform against their contractual obligations in a trade). For example, if a supplier plans to dispatch 10 shipments of goods in a year to a buyer, it may ask the buyer to open a standby LC valid for that period of time. The supplier and the buyer then continue their relationship (e.g., exchange documents and payment) without involving the issuing bank or calling upon the standby LC. However, if a buyer fails to pay under one of those 10 shipments and the standby LC's term is still valid, the issuing LFI will have to pay the supplier. Similar to commercial LCs, presentation of certain documents may be required in order for the issuing LFI to make the payment. Such documents contain information about the underlying trade that should be used by LFIs to determine the legitimacy of a transaction. These documents are discussed in Section 2.1.1.2 Types of Documents Available in Documentary Trade Finance Instruments.

2.1.1.1.2. Bank Guarantee

A bank guarantee is largely similar to a standby LC, as it represents an undertaking from an issuing LFI to pay to a beneficiary if one of the parties to a contract has failed to perform against their contractual obligations in a trade. The major difference between the two instruments is that bank guarantees have a wider application and are not limited to securing a performance under a trade-related transaction.

Thus, for example, a bank may issue a guarantee that a certain construction project will be completed in time and under a certain specification. If a builder fails to perform against the agreed-upon terms, the beneficiary can demand a payment from the bank. In connection with a trade transaction, a bank may issue a guarantee, for example, that a supplier will manufacture and dispatch certain goods within an agreed-upon period of time and will have to pay the buyer if the supplier fails to do so.

Letter of Credit:

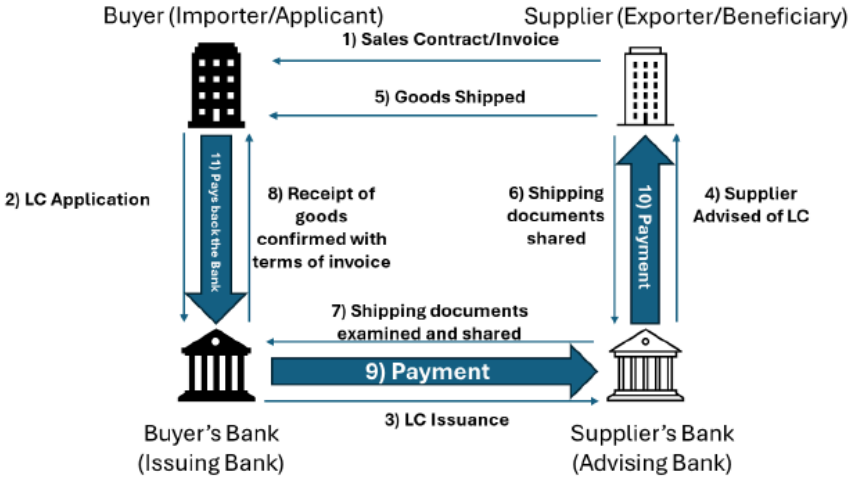


Figure 1 – *The above figure illustrates a typical payment flow for an LC. The Buyer (Importer/Applicant) applies for an LC with the Buyer's Bank (Issuing Bank), and the Buyer's Bank (Issuing Bank) guarantees that it will make a full payment to the Supplier's Bank (Advising Bank) (Step 3: LC Issuance) once the Supplier (Exporter/Beneficiary) presents certain documents (in this case, shipping documents) that confirm goods have been shipped to the Buyer (Importer/Applicant).*

LC and Bank Guarantee Vulnerabilities: LCs and bank guarantees are especially vulnerable to the risk of TBML as they can create the illusion of legitimacy for an otherwise illicit transaction. At the same time, LCs involve the most detailed documentation that an LFI may collect under a trade transaction (bank guarantees may have less detailed

documentation), allowing LFIs to carefully review the transactions for suspicious activity, red flags indicating TBML, or indicators of potential sanctions evasion.

2.1.1.2. Types of Documents Available in Documentary Trade Finance Instruments

The following documents are the most common types of documents available in documentary trade finance products. The terms of each LC and bank guarantee will differ, and the parties involved in a trade transaction may decide to request more or fewer documents, depending on the nature of their relationship. Please refer to Section 4.3 Targeted Financial Sanctions Obligations for further information on sanctions screening best practices involving documentary trade finance products.

- **Air Waybill:** An air waybill is a document dispatched by an international air courier, furnishing important details about the shipment and facilitating its tracking. An airway bill generally would consist of multiple originals designed to be assigned to different parties. The important aspect of this multi-part document an LFI would require is the original for consignor or shipper, whereas the recipient would receive the original for consignee, which is the document that travels alongside goods. An air waybill typically includes:
    - Names and addresses of the shipper and the recipient;
    - International Organization for Standardization ("ISO") codes for the origin and destination airports;
    - Description of the cargo, and, occasionally, the declared value of the cargo; and
    - The number and gross weight of the cargo.
- **Bill of Lading**: If the goods are shipped by sea, the title and ownership of the goods will be covered by a bill of lading. This is a document that can be issued by multiple parties (e.g., a master, carrier, owner, charterer, or their agents) acknowledging the receipt of cargo on board the vessel. The issuer issues the original bill of lading to the shipper that in turn presents the same to the LFIs. A bill of lading will indicate:
    - The name and address of the shipper of the goods;
    - The name and address of the recipient of the goods;
    - Carrier information, including the name of the vessel and number of loaded containers;
    - Type(s) of goods and its weight or volume;
    - The date of shipment;
    - Ports and places of receipt and delivery;
    - Number of originals issued; and
    - Issuer details.
- **Certification of Inspection/Quality**: A certification of inspection/quality is typical for exports of perishable items or items that require special handling instructions. The certificate will typically indicate:
    - The type of goods;

    - Whether the goods have been inspected by either a government agency or a private entity; and
    - The requested quality, quantity, or packaging of the goods.

- Certificate of Origin: A certificate of origin document is not always required in documentary trade finance; however, when included in a trade, it confirms the country where the goods have been manufactured and can also state the manufacturer, the authority/party issuing the certificate, as well as contain a general description of the goods.

- Customs Bond: A customs bond, when available, is a contract that guarantees a specific obligation will be fulfilled between a customs authority and an importer; specifically, it ensures compliance with a country's customs regulations and payment of duties and taxes by the importer. There are three parties to customs bonds: importer or principal, surety firm who issues the bond and pays any fees to the customs authority, and the customs authority. Customs bonds typically indicate:
    - The name and the address of the importer or broker;
    - The name and the address of the surety firm who issues the bonds;
    - The port of entry; and
    - Transaction and execution dates.

- Insurance Certificate: An insurance certificate is used by parties to a trade transaction that choose to insure goods in transit. The certificate, if available, will typically indicate:
    - Type of goods shipped and insured;
    - The type and name of the vessel used;
    - The dates and other details of insurance coverage; and
    - The beneficiary of the certificate in case of a loss.

- Invoice: An invoice will typically indicate:
    - A general description of goods;
    - The type and weight of goods;
    - The price per unit and total price of goods;
    - Currency of the invoice;
    - The name and address of the buyer and the supplier; and
    - The terms of delivery.

- Packing List: A packing list contains information about the shipment by itemizing all of the products being shipped. The packing list will indicate:

- The name and address of the shipper of the goods;
- The name and address of the recipient of the goods;
- Type(s) of goods and type, number, dimensions, and weight of each package, container details; and
- Invoice number.

- **Underlying Contract**: An underlying contract is a document that will be most common for a bank guarantee to understand the nature of the transaction and performance it will guarantee. Sometimes LFIs also request an underlying contract as part of an application for an LC, in accordance with their internal policies.

- **Other Transportation Documents**: LCs may also contain other transportation documents such as a railway transportation note or trucking invoice. These documents would typically contain information on, similar to the bill of lading, the name and address of the shipper, the name and address of the recipient, the type(s) of good and its weight or volume, the place of loading, and the destination point.

2.1.2. Non-Documentary Trade Finance and Open Account Trade

In recent years, suppliers, buyers, and their LFIs have shifted away from traditional, document-based trade finance products and toward non-documentary finance and open account trade. According to the Wolfsberg Group, the International Chamber of Commerce, and Bankers Association for Finance and Trade ("BAFT"), open account trade comprises approximately 80 percent of all international trade transactions.[10]

In **non-documentary trade finance**, an LFI still acts as a financing party; however, in this scenario, the trade transaction requires a smaller subset of documents, if any, and such documents typically relate to the creditworthiness of a party involved in trade. Examples of non-documentary trade finance products include trade loans in the context of structured trade finance, and financing of receivables/payables through import/export factoring and forfaiting, discussed below.

In **open account trade**, goods are shipped and delivered without involvement of an LFI as an intermediary, and the supplier and the buyer exchange shipping and other documents directly, rather than through an LFI. The parties then settle the balances due via a bank payment. As a result, even the LFIs that are originating the payment on behalf of their customers may lack critical information regarding the goods, shipping vessels, or transport routes associated with a given transaction. Sometimes they may not even know a payment relates to a trade transaction. LFIs processing open account trade transactions may therefore have little visibility into the type of goods involved in the underlying shipment; who is transporting the goods, including whether they are sanctioned or high-risk entities; and whether the shipment is originating, passing through, or stopping in a sanctioned jurisdiction. Whereas, if the buyer utilizes the trade finance facilities of the LFI, all details can be derived, and all controls checks and measures can be exercised prior to completing the transaction.

As a result, non-documentary trade finance and open account trade are among the highest-risk activities in which LFIs routinely engage, as illicit actors seek out methods where LFIs have a reduced role, namely less oversight, than in traditional documentary trade finance. LFIs should therefore be aware of the particular transparency challenges associated with non-documentary trade finance and open account trade transactions, which typically provide LFIs with less risk-relevant information regarding the parties and goods involved in the underlying trade activity than traditional, document-based instruments.

---

[10] Wolfsberg Group, ICC and BAFT Trade Finance Principles, *The Wolfsberg Group, ICC and BAFT Trade Finance Principles*, 2019, available at: https://library.iccwbo.org/content/tfb/pdf/trade-finance-principles-2019-amendments-wolfsberg-icc-baft-final.pdf

2.1.2.1. Description of Open Account Trade and Non-Documentary Trade Finance Products and Instruments

The following section discusses open account trade as well as the most common types of non-documentary facilities used in trade-related transactions. As noted above, precisely because these products do not involve an LFI collecting, inspecting, and accepting the underlying trade documents, the TBML patterns are very hard to detect. Instead, an LFI should focus on Customer Due Diligence ("CDD")/Know Your Customer ("KYC") and Enhanced Due Diligence ("EDD")-related processes, as well as transaction monitoring that may alert an LFI to indicators of suspicious activity associated with TBML.

(1) Open Account Trade: this is a type of a sale that is very advantageous to the buyer (importer). The exporter (seller) ships the goods to the buyer and specifies when the payment is due (typically within 30, 60, or 90 days after the shipment). This is a type of financing extended directly by the seller to the buyer, without involvement of a third-party LFI or trade finance provider. In theory, the buyer should then pay the invoice (e.g., via wire transfer or a cheque) when it becomes due; however, if the buyer fails to pay the seller has little recourse against the buyer other than bringing a legal action for non-payment. Typically, an exporter is willing to trade on open account in situations when it knows the importer well and the two have a long-established relationship. In the alternative, if the exporter overproduced certain goods that it cannot easily sell in the open market, it might be willing to sell the goods on an open account to a willing buyer, taking on the risk of non-payment. Some importers in developing markets may also pressure exporters on the basis that LCs or other traditional types of finance have prohibitive costs for the buyer. The opposite but similar type of a settlement in a trade transaction that is advantageous to the seller is cash in advance, i.e., a scenario where the buyer pre-pays the seller via wire transfer/cheque/credit card the entire value or a percentage of the goods to be shipped before the shipment.

Open Account and Cash In Advance Vulnerabilities:

- Considering hundreds of millions of wire transfers processed by global banks daily, it may be hard for an LFI to identify trade conducted on an open account, even in instances where the transfer references an invoice or a type of good. Thus, manual intervention and review becomes impossible unless a transaction triggers an alert, e.g., in case of a transaction monitoring or sanctions or watch list screening that would then allow an analyst to review the payment and request supporting documentation, if necessary.

- Thus, millions of transactions a day are settled on open account between buyers and sellers without any oversight from LFIs. While the majority of such settlements do not relate to any illicit activity, some illicit actors will abuse trade on open account and may even conduct test transactions to verify if certain types of transfers may trigger compliance review from various banks.

(2) Import and Export Factoring: Import and export factoring (also known as "international factoring") is the process of purchasing account receivables from a supplier/exporter in one country and collecting the invoice value later from the buyer/importer in the second country. The company purchasing the accounts receivables is called a "Factor" and can be a bank or a non-bank "Factoring Company." A factoring transaction will typically involve two Factoring Companies, an Export Factor and an Import Factor, each of which are local companies for, respectively, an exporter and an importer. As international trade continues to shift away from LCs and documentary trade finance, and towards open account terms, factoring gains more traction.

Factoring is particularly relevant as it helps parties to a transaction manage their cash flow, helping suppliers that would otherwise have to wait a certain period of time before a buyer makes a payment.

While factoring can take several forms, Figure 2 below illustrates this typical Import and Export Factoring arrangement:

Import/Export Factoring:

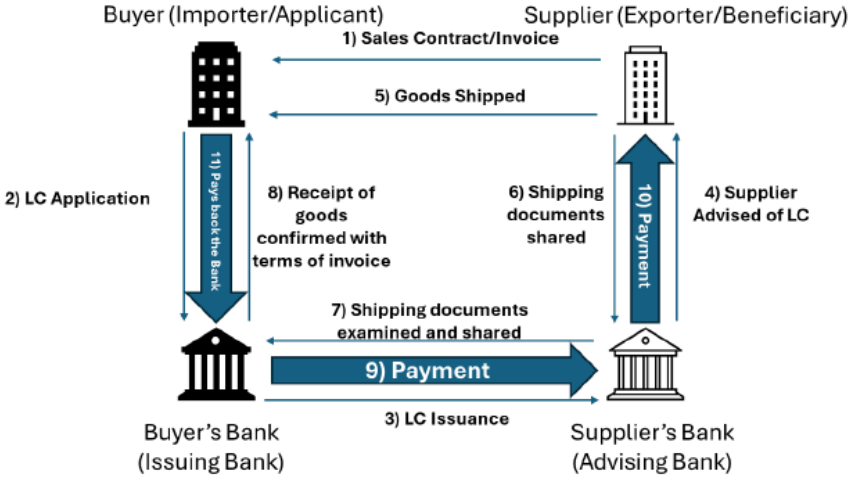


Figure 2 – The above figure illustrates a typical Import and Export Factoring arrangement. The Buyer (Importer) orders goods from the Supplier (Exporter). The Supplier (Exporter) ships the goods and issues an invoice to the Buyer (Importer). The Supplier (Exporter) then assigns the invoice to the Export Factor B who pays up to 80% of the invoice value to the Supplier (Exporter). The Buyer (Importer) meanwhile pays the invoice to Import Factor A, and when the funds are remitted to Export Factor B, the Export Factor B pays the remainder of the invoice, minus interest and fees, to the Supplier (Exporter).

Import and Export Factoring Vulnerabilities: The following are particular vulnerabilities of Import and Export Factoring:

- An Import/Export Factoring Company may undertake less stringent CDD/KYC and trade-related controls than a typical bank. Factoring Companies also often advertise their services as an alternative to banking, targeting companies that may have previously been denied banking services (although under banking may be caused by numerous reasons unrelated to illicit activity).

- A bank or an Import/Export Factoring Company participating in a transaction will receive fewer documents than in a documentary trade transaction. The documents may be limited to, for example, an invoice and a bill of lading, making it difficult to understand the trade transaction and all the parties and goods involved in the underlying trade activity.

(3) **Forfaiting:** Forfaiting is similar to the factoring example above. A forfaiting company is either a bank or a specialized finance firm that purchases an exporter's receivables at a discount. The key difference is the fact that forfaiting is non-recourse, meaning a forfaiting company assumes the risks of a buyer's non-performance and cannot ask the supplier to pay if the buyer fails. At the same time, in forfaiting, unlike factoring, the receivables are typically guaranteed by the importer's bank. The receivables in forfaiting also take on a form of a debt instrument that can later be traded in a secondary market. Forfaiting is typically used in capital goods transactions (e.g., equipment) and commodities trading.

Forfaiting Vulnerabilities: Similar to factoring, a forfaiting company will have limited visibility into the underlying trade transaction and would collect fewer documents than in a documentary trade finance. Thus, a forfaiting company is unlikely to detect illicit activity.

(4) **Structured Trade Finance**: Structured trade finance helps manufacturers, suppliers, and buyers reduce the gap between the time a manufacturer procures materials until the final product is sold to a consumer. A financial company, typically a bank, will loan funds to a company to cover the multiple stages of a trade. For example, the bank can loan funds to the supplier/exporter to finance the pre-export activities, such as manufacturing and storage. The bank can also loan funds to the buyer/importer that has received a shipment of goods but has yet to sell these goods. The borrowed funds are then repaid through the lifecycle of production, storage, transfer, or sale of the goods. Common trade finance structures are **warehouse financing** and **pre-export finance**, discussed below:

- **Warehouse Financing:** A type of inventory financing where a company or a manufacturer secures a loan from an LFI by using their goods as collateral. The commodities are kept in a warehouse approved by the lending institution or managed by a third party. For example, a buyer of wheat or another commodity secures a warehouse financing. If the buyer fails to repay the loan or delays the payments, the lender can seize and sell the goods to recover the losses.

Warehouse Financing:

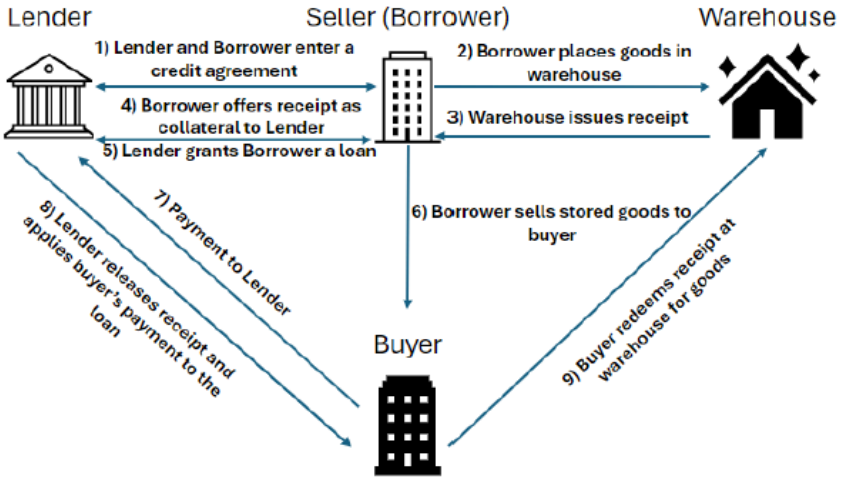


Figure 3 – The above figure illustrates a typical warehouse financing arrangement. The Lender and Seller (Borrower) enter a credit agreement, after which, the Seller (Borrower) places goods in a warehouse. The warehouse issues a receipt to the Seller (Borrower), and the Seller (Borrower) provides this receipt to the Lender as a collateral. The Lender then proceeds to issue a loan to the Seller (Borrower). The Seller (Borrower) sells stored goods to the Buyer, and the Buyer makes a payment to the Lender. The Lender then releases a receipt and applies the Buyer's payment to the loan. The Buyer then redeems receipt at the warehouse for the goods.

Warehouse Financing Vulnerabilities: LFIs that engage in warehouse financing should pay attention to the valuation of the inventory in trade since over-valuation may be used by illicit actors to gain funds that would otherwise not be available to them. Similarly, warehouse financing may be used to cover "phantom shipments", referred to in Section 2.2.2. Over- and Under-Shipment of Goods and Services, and/or involve commodities trade, which is particularly susceptible to TBML. LFIs should consider conducting additional due diligence on the warehouse(s) and the supplier of the goods to make sure they are legitimate and operating businesses. Finally, in warehouse financing, the financing LFI may have little visibility into the origin of the goods or the underlying documentation that supports the trade transaction.

- **Pre-Export Finance:** In pre-export finance, funds are paid to the supplier/exporter of the goods based on the confirmed orders from buyers. Typically, the borrower uses the funds to meet working capital needs which can include the purchase of raw materials, manufacturing costs, and costs associated with storing and movement of goods. LFIs should ensure they have controls in place so

that a trade transaction matches the description provided at the time of pre-export financing.

Pre-Export Financing:

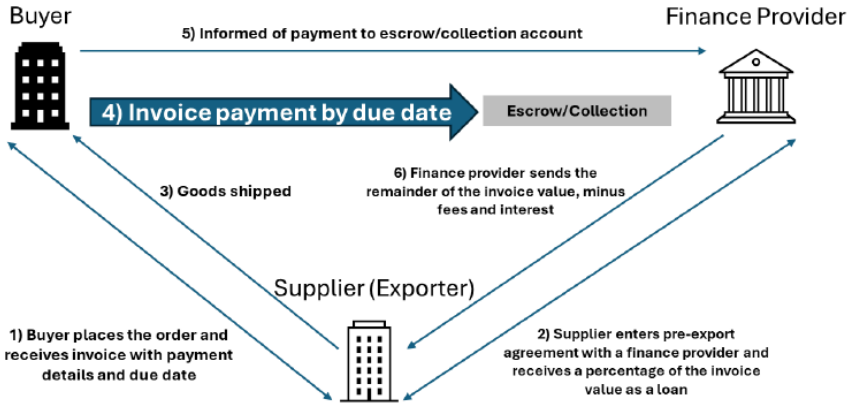


Figure 4 – The above figure illustrates a typical pre-export financing arrangement. The Buyer places an order and receives an invoice that specifies the payment details and due date. The Supplier then enters a pre-export agreement with a Finance Provider and receives a percentage of the invoice value as a loan, after which, the goods are shipped to the Buyer. Based on the payment due date, the Buyer is required to pay the invoice payment as part of the escrow/collection terms with the Finance Provider, and the Finance Provider is informed of payment to the escrow/collection account. The Finance Provider sends the remainder of the invoice value, minus fees and interest to the Supplier (Exporter).

Pre-Export Finance Vulnerabilities: In pre-export finance, an LFI has visibility only into one aspect of a trade transaction (i.e., activities by a borrower before shipment of goods). Therefore, in this scenario, it is harder for an LFI to identify any red flags or verify whether the borrower used the financing for the specified purpose. Thus, CDD/KYC measures play a particularly important role in pre-export finance, as further discussed in Section 4.2. CDD and EDD Measures.

(5) **Countertrade**: Countertrade is a reciprocal form of international trade in which goods or services are exchanged for other goods or services rather than for hard currency. This type of international trade is more common in developing countries with limited foreign exchange or credit facilities. A major benefit of countertrade is that it eliminates the need for one country to procure stable foreign currency that is often expensive and/or spend such currency from its reserves, which is a prime consideration for cash-strapped nations and provides an alternative to traditional financing that may not be available in developing countries. Offsetting is also more common for larger, more expensive items.

An example of countertrade is a barter arrangement, whereby the supplier/exporter exports certain goods to the buyer/importer, and instead of receiving a payment, the supplier/exporter receives a different type of a good or commodity from the buyer/importer or a third party nominated by the buyer/importer. Another example of a countertrade is a buyback agreement where a supplier/exporter exports certain manufacturing equipment and training services to the buyer/importer and accepts a percentage of the buyer/importer's manufacturing output as a form of payment.

Countertrade Vulnerabilities: Countertrade is the least transparent form of a cross-border trade since the parties do not involve any LFIs, and thus, are not subject to CDD/KYC, transaction monitoring or other transaction checks. It may also take place in a country with weak AML/CFT and recordkeeping regulations, making it nearly impossible to reconstruct the transaction or understand the parties involved.

2.2. TBML Typologies

The following sections examine common features of TBML activities by outlining specific TBML typologies identified by global standard-setters and industry groups. TBML typologies—ranging from basic to highly intricate schemes—all capitalize on the movement of goods in exchange for payment to move value within and across borders. Illicit actors may engage in one or several TBML typologies to complicate a trade transaction.

LFIs should therefore assess their exposure to trade activity and determine whether customers involved in trade transactions should be subject to EDD measures. When dealing with high-risk customer relationships, an LFI may decide to de-risk the relationship by either limiting the types of products offered to a customer or exiting the customer relationship if risks cannot be sufficiently mitigated. LFIs should incorporate this assessment into their AML/CFT program and update their policies, procedures, and processes with the aim to detect TBML and manage associated illicit financing risks.

In addition to the typologies listed below, the Guidance provides several risk indicators across the following four categories in Annex 1:

- Red flags relating to payments and trade transactions;
- Red flags relating to jurisdictions;
- Red flags relating to goods; and
- Red flags relating to corporate structures used.

LFIs should consider and incorporate these red flags into their internal controls, as appropriate. Furthermore, it is recommended that LFIs review the red flags, risk indicators, and examples provided in the Updated Strategic Analysis Report on TBML published by the UAE's FIU in June 2024.[11]

[11] Updated Strategic Analysis Report, Trade-Based Money Laundering, June 2024, The UAE's FIU, available at https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

2.2.1. Over- and Under-Invoicing of Goods and Services

Over- or under-invoicing of goods and services is one of the most common techniques used by illicit actors to transfer value across borders without detection by law enforcement or customs officials. This technique requires a level of collusion between the "supplier" and "buyer" to misrepresent the price of the good or service. In some cases, the supplier and the buyer are part of the same criminal organization.

While the value of goods and services could vary based on the quality of the underlying goods and services, LFIs are able to identify over- and under-invoicing by independently inquiring about the market value of the same, or similar, goods and services as those involved in a trade transaction. LFIs should consider using external resources to determine whether the price of underlying goods or services is in line with the market value, and in this context, identify over- or under-invoicing of the goods and services. Such external sources are most relevant in the context of commodities trading where the price of the commodity in question is less prone to variation. This control may also be referred to as "price-validation."

Over-Invoicing: By invoicing the goods or service at a price above the fair market price, the supplier is able to receive value (profit) from the buyer, as the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market.

Under-Invoicing: By invoicing the goods or services below the fair market price, the supplier transfers value (profit) to the buyer. The buyer sells the under-invoiced goods in the market for real value, and the difference between the real value and the invoiced price is the value (profit) transferred to the buyer.

- **Example**: A criminal organization (i.e., supplier in this case) exports 1,000 high-end electronic widgets at the fair market cost of AED 6,000 per widget (total market value of AED 6,000,000). Commercial invoices, the sales agreement, and the bill of lading show an export of 1,000 widgets at the price of AED 5,000 each, as the criminals have **under-invoiced** the high-end electronic widgets. The customs officials in the exporting country release the export, as they can confirm that the exported goods are the same as described on the shipping documentation. The buyer, which is also part of the criminal organization in question, receives the widgets and pays the supplier AED 5,000,000 via a wire transfer through its bank, referencing the invoice number in the free text field. Since there is nothing suspicious on the face of the transaction, this transaction is not stopped for further review by the bank. The buyer proceeds with selling the widgets in the market at AED 7,500 each, the actual retail price, generating a total of AED 7,500,000 in their bank account. This effectively results in the supplier transferring a surplus (profit) of AED 2,500,000 to the buyer.

2.2.2. Over- and Under-Shipment of Goods and Services

Prices are not the only piece of information that can be misrepresented; the quantity of the goods shipped and the services provided are also subject to misrepresentation. By over- or under-stating the quantity of goods in a trade transaction, the supplier and the buyer can transfer value to one another. In extreme cases, the supplier may not ship any goods to the buyer but will send a fake invoice and other supporting documentation to the buyer for so-called "phantom shipments." Phantom shipment was relevant in 61% of SARs and STRs filed in 2022 and 2023 analysed by the UAE's FIU.[12]

While LFIs normally do not have the opportunity to inspect the shipments to detect over- and under-shipment of goods and services, they may compare different pieces of information provided to them by their customer. For instance, the quantity of the shipped goods should match across different trade documents, such as invoices, shipping documents, and other custom clearing documents. Also, LFIs should ensure that the quantity of goods or services provided matches the profiles of the supplier, buyer, or any intermediary involved in the trade transaction, such as by reviewing the size and geographic location where the parties do business and have operations. When in doubt, LFIs may ask for attestation from the parties to the trade.

- **Example**: Company A located in Dubai sells 10,000 laptops to Company B in Central Asia, at a fair market price of AED 4,500 each. However, Company A only ships 5,000 laptops to Company B (**under-ships** the declared number of goods) with the invoice and shipping documentation stating 10,000. Company B pays Company A AED 45,000,000 via a wire transfer. Company A reimburses its suppliers AED 22,500,000. This results in the surplus of AED 22,500,000 that Company A moved to Dubai for future use.

[12] Id.

2.2.3. Multiple Invoicing of Goods and Services

Illicit actors may issue more than one invoice for the same trade transaction. In applying this technique, illicit actors request payment from different LFIs for the same underlying goods or services. This technique does not misrepresent any piece of information, and as such, it may be more difficult to detect. In addition, even if multiple payments relating to the same shipment of goods or delivery of services are detected, the illicit actors can claim "legitimate" explanations such as amendment of the price terms, payment of late fees, or additional logistics charges.

Close examination of invoices to detect potential anomalies and evaluating the invoices in the context of the customer's profile is beneficial to LFIs to detect such practices. LFIs should also be on the lookout for fictitious

invoices. When the authenticity of a document is doubted, information accompanying the documents, including the meta data of the digital files, could help LFIs determine whether an invoice is fictitious or not.

- **Example**: Company A located in Central America ships 500kg of bananas to Company B, a trading company in a Financial Trade Zone in the Middle East. Company A issues an invoice for AED 150,000 to Company B to be paid to Company A's bank account held with Bank X. Company A has all the documents that proves the bananas were shipped at the stated price. Company A produces documents, including the bill of lading, that shows the delivery term was for Company A to deliver them to a Financial Trade Zone in the Middle East. Company A issues another invoice for AED 150,000 for the same shipment to Company C located in Central Asia to be paid to Company A's bank account held at Bank Y. Company C, in fact, distributes illicit drugs throughout the region and often accumulates significant funds in its bank accounts. In this case, Company A uses the same documents that it used for Company B in the FTZ. The LFIs involved, which checked the documents, did not detect any irregularities, and as such, the transactions went through. The transaction helped Company C to move AED 150,000 to Central America under the disguise of payment for legitimate goods.

2.2.4. Falsely Described Goods and Services

Similar to misrepresentation of the value or the quantity of the goods shipped or services provided, the quality or type of good or service can also be misrepresented. In this case, there is a discrepancy between the description of goods on the shipping documents (such as a high-priced luxury item) and the goods that the supplier actually shipped (such as a low-priced commodity item or a lower quality item). Falsely describing goods and services is also particularly relevant in the context of proliferation finance, as illicit actors substitute controlled or restricted goods for similar non-controlled or restricted goods.

While this typology is very difficult for LFIs to detect, LFIs may ask for representation in cases where other red flags, including those listed in the Annex 1 of this Guidance, signal the risk of a false description of goods and services.

- **Example**: Company A sends a shipment described as two tons of bronze to Company B in another country for AED 32,000, while in fact, the shipment contained two tons of silver valued at AED 2,755,000. By falsely describing the goods, Company A transferred AED 2,723,000 in value to Company B under the disguise of a trade transaction. Company A systematically declared the nature of the goods as bronze in all trade documents which went undetected by customs agents. Company A was the beneficiary of an LC issued by Company B's bank. Company A takes all the documents, including customs clearing, bill of lading, and invoice, to the advising bank. The advising bank confirms the conformity of the documents and informs the issuing bank. Once the issuing bank approves the conformity of the documents, it pays AED 2,755,000 to Company A.

2.2.5. Use of Shell, Front, or Shelf Companies

The use of shell, front, or shelf companies is commonplace across different types of illicit finance activities; TBML is not an exception. Those engaged in TBML schemes involve shell, front, or shelf companies to conceal the beneficiaries behind trade transactions, obfuscate the payment flow, and otherwise complicate a trade transaction with the objective of making it difficult for LFIs and law enforcement to detect irregularities. Similarly, these types of companies are often used by sanctioned persons who cannot act in their own name, knowing that an LFI's screening software would otherwise be able to detect their involvement. As a result, these sanctioned persons set up a front or shell company under a generic name to avoid detection. Corrupt government officials also hide behind shell or front companies, as many countries' laws prohibit government officials from owning or operating a business.

Strong initial and ongoing CDD/KYC controls are the most effective measures to mitigate the risks posed by the illicit use of such companies for TBML schemes. LFIs should be particularly aware of companies established in tax havens, at an address where hundreds of other companies are registered, or companies represented by lawyers, secretaries, or other agents appointed by a corporate formation law firm. Additionally, to detect front companies, LFIs may add scenarios to their transaction monitoring systems that are designed to detect sudden activation of a

longstanding dormant account, a payment request under a trade finance document to an unrelated third party, unusual geographic patterns of a trade transaction, or transaction volumes that are not in line with a company doing a similar type of business as the party in question. Shell, front, and shelf companies are defined as follows:

- **Shell company**: A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees.
    - **Example**: Members of a criminal organization with ties to a government official in Country A use shell companies to participate in cross-border trade backed by the government of Country A. Government contracts that involve importing goods to Country A are first directed to the shell companies, portrayed as legitimate actors. In fact, these shell companies are only intermediaries, buying low-quality goods in a third country and re-supplying them to Country A at inflated prices, while keeping the price difference.
- **Front company**: A front company is another type of a company that may lack operations, assets, or employees. The only difference between a front company and shell company is that occasionally a front company is a functioning company created with an intent to hide the true beneficiaries or stakeholders.
    - **Example**: Company A is located in Country A with stringent export controls that prevents it from exporting goods to Country B. However, a purchaser in Country B is willing to pay a high premium for Company A's goods. They agree that Company A will set up a front company with a different name and untraceable ownership in Country C. Company A then proceeds to ship the goods to Country C, where there are no restrictions, for further reexport to Country B, without raising a suspicion from its banks or law enforcement.
- **Shelf company**: A shelf company is an incorporated company with inactive shareholders, directors, and secretary that is left dormant for a long period of time. Shelf companies may even have open bank accounts to bolster their legitimacy. An illicit actor may attract less scrutiny by using a company that on paper appears to have been incorporated and operating for several years.
    - **Example**: Company A was incorporated in 2010, and since then, has had no activity. In 2016, the company starts to engage in the trade of high-value electronic items. It engaged in over-invoicing activities and managed to transfer additional value under the disguise of trade. Company A was not subject to strict controls since the bank involved has lowered the risk rating of Company A as it did not have any high-risk transactions in the first five years of its relationship with the bank.

2.2.6. Use of Free Trade Zones

Free Economic Zones ("FEZ") are designated areas within a country's borders where certain economic activities are encouraged and facilitated by special regulatory and legal frameworks. One of the most common types of FEZs is a Free Trade Zone ("FTZ"). FTZs are designed to attract trade and investment by suspending the collection of import duties and taxes and also implementing simplified customs procedures. In addition, the process of setting up a company is typically less complicated in an FTZ. As a result, FTZs are ideal locations for storing and distributing products, and function as critical logistics hubs for importing, transshipping, and re-exporting goods.

While FTZs promote legitimate trade, they also attract illicit actors who try to exploit the eased controls (such as through illicit goods manufacturing and smuggling) and high volume of trade conducted in FTZs. As a result, illicit actors benefit from minimal checks and transparency requirements in an FTZ,[13] and for the UAE, the complexity of TBML in FTZs, combined with the country's high number of FTZs, poses a significant challenge to LFIs in combatting illicit financing flows.

Accordingly, LFIs can mitigate the risk of FTZs by inquiring about the reasons a customer chose to use a FTZ for their activity and to evaluate a customer's response as part of the CDD/KYC process. LFIs may also ask for the names and the location of a customer's counterparties to evaluate if there are any suspicious indicators involving the customer (e.g., whether the customer's counterparties are all located in high-risk jurisdictions and lack a legitimate business connection to the customer).

- **Example**: Company A located in Country A's FTZ orders navigation equipment from a manufacturer, Company B, in Country B. Country B has restricted the exportation and re-exportation of navigation equipment produced in Country B to Country C. Company A applies for a LC for the benefit of the manufacturer, Company B, in Country B. Once goods are shipped to Country A, the manufacturer, presents relevant documents to the advising bank which then passes them to the issuing bank. One of the documents is a bill of lading in which the consignee is Company A in Country A's FTZ. Nothing on the face of the documents suggests that the navigation equipment will be transported elsewhere. The consignee from Company A in Country A's FTZ receives the navigation equipment and re-packages the goods into boxes that suggest the navigation equipment are household kitchen appliances. The consignee from Company A in Country A's FTZ re-exports these goods to Country C in violation of laws of Country B with a packing list stating the navigation equipment represents household appliances.

---

[13] To see more about the risks associated with FTZs, *see* Improving Governance and Tackling Crime in Free-Trade Zones, RUSI, October 2020, Available at: https://static.rusi.org/20201012_ftzs_web_2.pdf

2.2.7. Illicit Cash Integration

Cash is vulnerable to abuse by illicit actors to conduct ML activities and finance criminal activities. Illicit actors use different techniques to integrate criminally derived cash into the financial system. The three main ways that illicit actors integrate cash into the financial system are the following: exploitation of non-bank financial institutions, offsetting schemes, and infiltration of legitimate supply chains. The specific characteristics of cash—anonymity, interchangeability, and transportability—make it an attractive method by illicit actors seeking to conceal the proceeds of crime within the context of trade. Unlike other monetary instruments, such as wire transfers, cash holds no record of its source or owner. Cash transactions are also instantaneous and widely accepted across jurisdictions.

Strong CDD/KYC controls help LFIs to lower the risk of engaging with customers involved in criminal activities that generate illicit cash proceeds. Also, by filing reports to the FIU, LFIs contribute to helping the FIU detect illicit actors who use the following techniques to integrate illicit cash into the UAE's financial system.

- **Exploitation of non-bank financial institutions**: Illicit actors seeking to circumvent the AML/CFT controls applied by banks may opt to use non-bank financial institutions to introduce and integrate illicit cash into the financial system as part of a TBML scheme. While a large bank may detect unusual activity in the case of large or frequent payments and ask for supporting documentation, non-bank financial institutions are perceived to have less stringent controls to detect TBML schemes. Thus, by using non-bank financial institutions, the criminals ensure movement of funds without additional inquiries. This is particularly important as numerous financial technology companies with various degrees of compliance programs start offering payment services.

- **Offsetting schemes**: When one criminal organization has excessive cash and another criminal organization needs cash, illicit actors may engage with one another and offset cash funds they have in different locations. One of the best ways for such illicit actors to offset their cash is to engage in trade. For example, one criminal organization can purchase high-value goods for cash and export it to a country where cash is the predominant means of payment. The buyer/importer sells the goods and transfers cash proceeds to another criminal organization operating in the importing country. By hiding behind trade transactions, illicit actors can move cash between criminal organizations.

- **Infiltration of legitimate supply chains**: Sometimes illicit actors take over a stake in a legitimate business and use the business' legitimate supply chain as a method to introduce and integrate illicit cash into the financial system. Money launderers slowly and steadily increase the amount of illicit cash they introduce into the business while maintaining the business' operations.

- **Surrogate shopping networks:** A network of individuals, known as surrogates or personal shoppers, who purchase products on behalf of others to circumvent customs controls, export controls, or other forms of trade or tariff restrictions. These networks could be exploited as part of TBML schemes, whereby illicit actors provide local currency that are the proceeds of crime to surrogate shoppers to compensate for the items surrogates purchase using their credit cards, as well as incentives or fees. The decentralized and often anonymous nature of these transactions can make it difficult for LFIs to track the funds and identify the real beneficiaries, increasing the risk of money laundering.

  Example: Criminal organization A in Country A sells illicit drugs through a network of individuals, selling it for cash. Each individual deposits the cash they have collected to their personal accounts. Later they use their debit cards linked to the accounts at a point-of-sale in a supermarket that is owned by the criminal organization. While it appears that all these individuals are purchasing food items at the supermarket, in fact they are not purchasing anything.

  By doing so, they aggregate the funds collected from the sale of the illicit drugs in the account of the supermarket. Criminal organization A then uses the funds to pay to Company B for the supply of the illicit drugs to Country A under the disguise of a transaction related to importation of food items to the supermarket. None of these transactions appear to be related to any illicit activities. In this case, the criminal organization infiltrated the legitimate supply chain to launder funds under the disguise of trade between the supermarket, customers, and Company B which supplies the illicit drugs.

2.2.8. Third-Party Intermediaries

A third-party intermediary may take part in a trade transaction by settling an invoice on behalf of an illicit actor. Sometimes such third-party intermediaries are incorporated in offshore jurisdictions that offer corporate secrecy. Even though there may be legitimate grounds for a third party's involvement in a trade transaction, whether financially or through physically supporting a trade (e.g., a service provider acting in the capacity of a shipping company), illicit actors have often used this technique to transfer value. This TBML technique is particularly challenging for LFIs to detect because it often occurs as part of open account trade where LFIs have very limited information about the underlying transaction.

To the extent that information is available on an underlying transaction, LFIs should question the involvement of unrelated third parties if there is no economic justification for the third party's involvement in the trade transaction and if the third party was not previously identified as a principal counterparty during the customer's onboarding.

- **Example**: Company A exported 500 widgets to Company B which is located in another country. 15 days after the delivery of the goods, Company A received funds from Company C located in yet another country. Company A's bank stopped the payment and conducted due diligence. Since Company C is incorporated in an offshore jurisdiction which is perceived to be high-risk, the bank asked for further documents. Once Company A provided documents, it revealed a third party was paying for the goods delivered to Company B. The bank compliance proceeded to request further information, including trade documents, showing the relationship between Companies B and C, and the source of funds for the transaction coming from Company C. In providing the requested information, Company A shared contradictory documents that did not match the transaction detail. Specifically, the information regarding the ultimate creditor of the transaction that was provided in the MX/ISO 20022 message did not match the information on the purchase agreement provided by the customer. The bank returned the transaction in question since it could not determine whether it was a legitimate transaction. The bank filed a suspicious activity report with the FIU

that later led to an investigation that unearthed a ML scheme which involved the movement of funds gained from illegal gambling in a country where Company C was located.

2.2.9. Back-to-Back Letters of Credit

Back-to-back LCs are a financing arrangement made up of two distinct LCs, one issued by the buyer's LFI for the benefit of an intermediary and the other issued by the intermediary's LFI for the benefit of the supplier. Such back-to-back letters of credits can be used for legitimate purposes when, for example, the intermediary is a commodities broker purchasing goods at one price and then selling at a higher price to a willing buyer. In this case, the broker wishes to maintain a certain level of secrecy, because otherwise, in the future, the buyer can acquire goods directly from the supplier without the mark-up. However, this technique is also used by illicit actors to complicate the financing arrangements, making it harder to trace the flow of funds.

This technique can also be used to evade sanctions. Back-to-back LCs allow the intermediary to hide certain information that could have led to detection of a sanctions target in the trade. For instance, if the issuing bank of the first LC is a sanctioned bank, with a back-to-back LC, the ultimate beneficiary receives the second LC from an unsanctioned bank of the intermediary without mention of the original issuing bank.

LFIs should carefully consider when any customer requests to open back-to-back LCs and conduct appropriate due diligence on the customer. In addition, LFIs should monitor customer accounts for frequent incoming and outgoing funds transfers that occur in a short period of time and involve similar amounts, as this can be a sign of back-to-back transactions in a TBML scheme.

- **Example**: An oil extraction company in Country A sells 200,000 barrels of crude oil to a broker in Country B. Country A is sanctioned by several jurisdictions prohibiting purchase of oil originating in it. The broker arranges for the oil to be transported via railroad to Country B that does not maintain sanctions against Country A, where it is then onloaded onto a vessel for delivery to Country C. The broker, using a bank in Country B, opens an LC in favour of the supplier. The buyer in Country C opens the second LC in favour of the broker (note that the buyer and buyer's bank will be unaware of the nexus to Country A in the transaction and will not be able to conduct a sanctions analysis). The documentation provided as part of the second LC shows Country B as the origin country.

2.2.10. Fictitious Documents

Presenting fictitious documents is a ubiquitous technique money launderer use when transferring funds under the disguise of a trade transaction. As stated in the Updated Strategic Analysis Report on TBML published by the UAE's FIU in June 2024, fictitious documents are the most frequently used technique used in TBML based on the SARs and STRs analysed by the FIU in 2022 and 2023.[14] Trade transactions usually involve multiple documents, increasing the opportunity for criminals to temper with the documentation or create fake documents. Considering that there is no uniform model for trade-related documents, parties facilitating the trade, such as LFIs, shippers, vessel owners, and insurers, cannot always detect fraudulent documents absent obvious red flags. However, LFIs should conduct further due diligence in instances when there are clear discrepancies or visible alterations among documents presented. Additionally, LFIs may also benefit from creating an internal repository of different documents that are commonly used in trade finance by their customers to have a comparison point when reviewing documents. While there are several varieties for each type of document (e.g., several versions of invoices), this practice will help LFIs detect fictitious documents that can be carelessly generated by illicit actors who try to defraud the LFI.

- **Example**: Company A in Asia exported 60 tons of steel to Company B in Africa. Both Companies A and B are in a secret agreement to inflate the volume of shipped steel to 600 tons. The two companies decide to settle the transaction via open account. Company B sends a wire with an MX/ISO 20022 message to Company A, but an intermediary bank stops the transaction as suspicious and asks for supporting documentation. Company B prepares a fictitious invoice and also finds online a sample export origin declaration prepared by

a government authority of the Asian country. Company B drafts a fraudulent export origin declaration and submits both documents to the intermediary bank which finds them acceptable.

[14] Updated Strategic Analysis Report, Trade-Based Money Laundering, June 2024, The UAE's FIU, available at https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

2.2.11. Accounts Used as Pass-Through

Money launderers and criminal organizations may set up accounts that are merely used to complicate the ability to trace funds. This could be achieved by opening a separate account for an existing shell or front company, or a legitimate business. Money launderers and criminal organizations may alternatively create new entities with no economic purpose other than acting as a pass-through account in a trade transaction.

By passing funds through such accounts, money launderers try to make it more difficult for LFIs involved in payments to investigate the origin of funds or purpose of a transaction. Furthermore, if such pass-through accounts are opened at jurisdictions whose risk of ML is perceived to be lower, the money launderers will be able to move funds with less scrutiny.

This technique can be used in TBML to further complicate the financial flows pertaining to trade transactions, which in many cases, are already complex. Trade transactions often involve multiple parties such as shippers, ship brokers, local transport companies, consignees, commodities brokers, and others, making it easier for illicit actors to justify multiple payments to pass-through accounts that serve no other purpose other than layering funds. LFIs should ask for more information if they find that a transaction is unnecessarily complicated. For example, LFIs should seek explanation in these cases: (1) when there are entities involved in a trade transaction without a rational justification; (2) when the trade transaction is going through several currency exchanges even though it is not necessary for the trade; or (3) where the shipping route passes through countries that makes the route longer without a clear purpose.

- Example: A criminal organization located in Europe creates a legal entity, Company A, in the Middle East and opens a bank account for Company A at a local bank in the Middle East. It then creates a website for the company suggesting it is a local logistics company, even though Company A has no legitimate business operations. The criminal organization then starts making regular payments to Company A. When the bank asks about the purpose of the payments, Company A provides fake invoices suggesting it facilitates movement of goods that the criminal organization allegedly (or actually) exports to the Middle Eastern country. The criminal organization that has control over Company A's account effectively transfers funds from Europe to the Middle East and can use the accumulated funds to buy goods or services elsewhere.

2.2.12. Use of Registered Hawala Providers and Alternative Remittance Systems

When illicit actors are seeking to place and layer illicit funds into the financial system, they often turn to alternative remittance systems to structure remittances for the import and export of potentially prohibited or restricted goods, disguising the illicit funds as legitimate transfers abroad. With regards to RHPs, RHPs are more vulnerable to abuse for TBML schemes if the provider conducts larger transfers on behalf of businesses to conduct commercial operations and trade-related transactions.

For RHPs seeking to detect TBML schemes, RHPs should obtain a clear understanding of the intended purpose and nature of a transaction and whether it is consistent with what they know about the customer. If the customer appears to be acting on behalf of a business, the RHP should perform CDD/KYC on the business, and the business must be registered and based in the UAE to carry out transactions through the RHP. By conducting CDD/KYC on the customer, the RHP will be in a position to identify TBML and potentially suspicious activity associated with the

customer (e.g., a customer who is from Country A states that they are sending funds to a family member, but the beneficiary is located in Country B; a customer who says he works as a labourer wishes to transfer a sum that is greater than the average yearly income for someone in his/her position; etc.).

> **Example**: Individual A, a representative of Company A in Country A, uses a local hawala service provider in Country A to transfer cross-border remittances to individual B, who was a representative of Company B, unbeknownst to the hawala service provider, in Country B. The payments were for counterfeit high-end apparel items sold by Company B to Company A, but were indicated to be funds that were sent to family members in Country B.

2.3. Services-based Money Laundering

To date, efforts to combat TBML have focused primarily on the trading of goods to facilitate ML, but TBML can also involve the provision of services as part of **services-based money laundering ("SBML")** schemes. SBML schemes rely on exploiting the trade of services or other intangibles, such as information, to disguise the proceeds of crime. Global trade in services provides opportunities for ML as the intangible nature of services makes it difficult to detect anomalies in the price of services offered and to prove whether such services have been provided. For instance, it is common to bill for retainer or penalty fees in certain services sectors, such as in consulting and legal professions, even if the service has not been supplied. While this Guidance does not cover SBML schemes in great detail, it is important to understand that similar to TBML, SBML schemes utilize invoice fraud and manipulation in order to justify the movement of funds as payment for the invoiced services. This can involve billing for non-existent services, inflating the cost of services, or using legitimate services to mix illicit funds with legitimate revenue.

The most common services and sectors involved in SBML schemes are parties that provide services related to gambling, software, financial services, consultancy and advisory, and intellectual property rights.[15]

- **Example**: A strategic consulting firm located in Country A billed hundreds of hours of advisory services to a company in Country B. The ultimate beneficial owner of both companies was the same person, who was a professional money launderer. Using the consulting firm, the owner transferred large amounts of funds moved from Country B to Country A without being suspected of any wrongdoing.

[15] FATF, *Trade-Based Money Laundering: Trends and Developments*, 2020, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

2.4. Economic Sectors and Products Vulnerable to TBML

The FATF has indicated that a number of sectors are vulnerable to TBML, spanning sectors that involve the purchase and sale of both high-value, low-volume goods or low-value, high-volume goods. Common traits of sectors that are more vulnerable to TBML include sectors that experience wide pricing margins, extended supply chains, and goods that are hard for customs authorities to examine.[16] As a result, the origin or quality these goods or commodities can be easily mispresented, making it difficult for LFIs to verify the accuracy of trade transactions in these sectors. The following sectors are particularly susceptible to abuse for TBML activity.

[16] FATF:, *Trade-Based Money Laundering: Trends and Developments*, 2020, available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

2.4.1. Gold, Precious Metals, and Minerals

Gold, precious metals, and minerals function as an alternative form of value within the TBML process and thus can be exploited for either moving or storing value. Such materials and metals are also often used for sanctions evasion

purposes or to launder the proceeds of government corruption, as governments are the primary owner of mineral exploration rights.

- Example 1: Country A charged four individuals for their involvement in a large international gold ML scheme. The defendants purchased billions of dollars of gold derived from criminal sources (e.g., corruption, illegal mining, and smuggling). After exporting the gold to Country B using a fictitious certification of origin and invoices, a dealer in precious metals based in Country A helped them sell the gold to Country B's refineries. In exchange, the defendants received wire transfers that appeared to be legitimate payments for wholesale gold purchases.

In this example, the illicit actors relied on fictitious certification of origin and invoices to misrepresent the source of the commodity (i.e., gold). The illicit actors also benefited from the high value of the underlying commodity to quickly move a large amount of funds. The illicit actors also used a third-party intermediary to facilitate the trade transaction.

- Example 2: Because of sanctions, Country A has very limited food and medicine supplies. Government of Country A purchases food at inflated prices from illicit companies in Country B. Instead of distributing it for free, Country A requires citizens to bring scrap gold items in exchange for food. Government officials then recast them as gold bars and export the bars to Country B by declaring them as lead bars using documents that falsely describe gold bars as lead bars including fraudulent bills of lading. The importer pays the price equivalent to the cost of lead bars to the food suppliers. From Country B, government officials move the gold to other countries to store in private bank vaults.

In this example, the illicit actors benefitted from a high-value, low-volume commodity, and the fact that one commodity can be substituted for another. In addition, the illicit actors were able to melt and recast the goods to resemble another type of good.

2.4.2. Agricultural Products and Food Items

Transactions related to agricultural products and food items may invite less scrutiny; however, they can also be exploited by illicit actors. Illicit actors may purchase foodstuffs from farmers or small suppliers for cash and then export the goods and receive incoming wire payments into their bank accounts.

- Example: A TBML scheme was discovered by three European countries where a network of drug traffickers used the illicit cash they accumulated as part of their crimes to purchase potatoes and onions in Europe. Working with an accomplice in an export/import company, they would then send these goods to Country A in North Africa and ask the buyers in Country A to pay the price via wire transfers to the accounts held by the drug traffickers.

In this example, the drug traffickers did not use any of the common TBML techniques; instead, they exploited legitimate supply chains to move their cash proceeds into wire transfers that appeared legitimate, relying on the fact that certain industries remain cash-intensive industries.

2.4.3. Car Parts and Vehicles

Car parts and vehicles, including second-hand or luxury vehicles, are frequently paid for in cash. Purchasing car parts and vehicles is therefore an effective way to turn illicit cash into goods that will be traded and could even generate additional profit.

- Example: Country A and B jointly disrupted a scheme in which criminals laundered proceeds of drug trafficking and tax fraud. The criminals used illicit cash to purchase luxury vehicles and subsequently exported the vehicles for sale to other jurisdictions, often inflating the price. To do so, the criminals established several legal entities and utilized fake paper trails, including fraudulent sale agreements, for the sale and purchase of vehicles to deceive parties involved in the export and sale network. The criminals also secured a large contract with a legitimate second-hand luxury vehicle supplier in Country B, further giving

the appearance of legitimacy to their scheme. After layers of sales, the criminals would export the luxury cars to drug traffickers in other countries as a means of payment or sell them to unwitting buyers who would wire the purchase price.

In this example, the criminals chose an industry in which cash transactions are common. Furthermore, the criminals exploited legitimate trade flows to layer the illicit funds and use falsified documents to hide the illicit nature of their trade transactions. The high-value luxury car industry allowed the criminal actors to integrate large sums of money into the financial system.

2.4.4. Clothing and Second-hand Textiles

Clothing and second-hand textile and apparel can be easily mispriced due to the varying prices of clothing items and general lack of common methods to assign value to such goods. The increasing popularity of second-hand apparel makes this sector more attractive for illicit actors.

- Example: Authorities in Country A noticed a sharp increase in importation of clothing and footwear from Country B with which Country A had a free trade agreement. Upon further investigation, authorities discovered that a drug cartel had been purchasing clothing items in Asia with criminally derived funds, exporting these clothing items to Country B, and then reexporting them from Country B to Country A. This scheme operated under the pretence that the clothes were made in Country B, enabling the cartel to gain a large margin of profit and introduce the illicitly gained funds into the banking system.

In this example, illicit actors abused high-volume, low-value goods to conduct TBML. The cartel used fictitious documents (such as fake invoices and packing lists) to hide the origin of the goods. Because the traded goods had a large margin for price misrepresentation, the cartel inflated the value of clothing on the supporting trade documentation.

2.4.5. Portable Electronics

Portable electronics, especially high-end electronics (smart phones, laptops, or watches), can be deliberately misrepresented and incorrectly valued. As such, they create the opportunity to quickly move significant criminal proceeds.

- Example: Authorities in Country A discovered that millions of dollars were laundered through its banking system. The scheme involved criminals using drug proceeds in Country B to purchase small, high-end electronic devices. The items were then exported to Southeast Asia and the Middle East, with exporting documentation and invoices significantly undervaluing the cost of items, while the import documentation, including re-issued invoices and customs declarations, stating the true price. This allowed the criminals to increase the illicit value being transferred offshore.

In this example, the criminals moved low-volume, high-value goods and used an undervaluation technique that declared low export prices. At the same time, the importers sold the goods in Southeast Asia and the Middle East at the actual price, generating larger sums of funds in third countries that were subsequently integrated into the banking system.

2.4.6. Art and Antiquities

The art and antiquities sector is particularly susceptible to TBML due to the high value and subjective pricing of items, which can facilitate the movement of large sums of money under the guise of legitimate transactions. The sector's opacity and the difficulty in assessing the true value of art and antiquities make it an attractive channel for laundering illicit funds.[17] The art and antiquities sector also frequently employs the use of third-party intermediaries, such as art dealers, that can help launder the proceeds of crime across international transactions, with artwork or antiquities purchased in one country and kept in another country.

- **Example**: Trust A, a shell company that ostensibly specializes in rare art, uses illicit funds to purchase an ancient sculpture from an auction house. This transaction allows Trust A to move a substantial amount of money internationally under the pretence of a legitimate art deal. The sculpture, obtained from a legitimate auction house, can continue to increase in value and can later be resold at a premium, concluding the ML cycle.

In this example, the criminals obtained high-value, unique goods using illicit funds. Because the sculpture was purchased at an auction, it has been authenticated, and there is an existing record of an auction sale.

In the future, the criminals can sell the sculpture, potentially at a higher price, generating additional profit. Even if the criminals sell the sculpture at the same price or slightly below the purchase price, the criminals were able to launder a substantial amount of money that now appear as legitimate funds.

---

[17] FATF, *Money Laundering and Terrorist Financing in the Art and Antiquities Market, Financial Action Task Force*, February 2023, available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html

2.4.7. Construction Materials

Due to their low-value-high-volume nature and at the same time prevalence in international trade, construction materials are appealing for over- or under-invoicing as well as over- or under-shipment. As stated in the Updated Strategic Analysis Report on TBML published by the UAE's FIU in June 2024, construction materials were involved in 10% of the SARs and STRs filed in 2022 and 2023, analysed by the UAE's FIU.

- **Example**: Company A allegedly shipped 15 tons of rolled stainless steel to Company B. Instead, the shipment consisted of rolled and lighter aluminium that appeared to be visually the same. Thus, Company A received a value that was larger than the fair market price of the actual shipment, resulting in transfer of inflated value from Company B to Company A.

3. Understanding and Assessing Illicit Transshipment Risks

Transshipment refers to the shipment of goods from the country of origin to one or more intermediate destinations prior to shipment to the country of ultimate destination. Although transshipment is often employed to streamline the logistics of cross-border shipping and for other legitimate economic reasons, transshipment can be manipulated by illicit actors to evade trade restrictions, including sanctions and export controls. Because export control authorities around the world maintain varying levels of restrictions across different countries or types of end-users, illicit actors employ transshipment to export restricted items to or from **embargoed** or **sanctioned jurisdictions**.

- **Embargoed jurisdictions:** Certain countries that are subject to embargoes have a comprehensive or near comprehensive prohibition on any export or reexport to such country.

- **Sanctioned jurisdictions:** Countries facing unilateral or multilateral sanctions have numerous categories of goods and services that cannot be provided to, or sourced from, such country.

In these scenarios, because end-users in embargoed or sanctioned jurisdictions are aware of trade restrictions involving the import and export of goods, end-users will often pay a premium to importers or exporters willing to ship goods or services via a third, less controlled country. This often leads to violations of the export control and/or sanctions laws of the exporting country and may implicate LFIs assisting the re-exporter or the transshipment party. For instance, illicit actors may target countries with weak export control laws as part of WMD proliferation efforts. In this scenario, illicit actors have importers or exporters deliver sensitive or dual-use items initially to transshipment hubs rather than directly to their home countries.

Accordingly, the UAE lies directly across the Arabian Gulf from Iran and is a significant partner for international trade, increasing the UAE's potential exposure to illicit transshipment risks. As a result, LFIs should be aware of the different techniques that illicit actors use to evade trade restrictions and engage in transshipment. Particularly, illicit actors have been found to use the following techniques in transshipment schemes:

- **An illicit actor ships goods from a sanctioned country to a non-sanctioned location**. Illicit actors first ship goods originating in a sanctioned country to a non-sanctioned location. The illicit actors then ship these goods to a third location, with the underlying documentation showing the non-sanctioned location as the country of origin. Sometimes the re-exporter repackages the goods or adds non-sanctioned country seals of origin to the packaging to further obscure the true origin.

- **An illicit actor located in a jurisdiction with fewer export restrictions imports goods, allegedly for use in the country**. An illicit actor (e.g., import/export company) located in a jurisdiction with fewer export restrictions imports goods, allegedly for use in the country. The illicit actor then forwards the goods to either prohibited end-users (i.e., users blacklisted by the countries where the goods originated) or to embargoed or sanctioned countries. Often such schemes involve networks of import/export companies registered in jurisdictions world-wide, with goods travelling across multiple jurisdictions before they reach the prohibited end-user or destination.

- **An illicit actor located in a country susceptible to corruption imports goods controlled for export**. An illicit actor (e.g., import/export company) located in a country susceptible to corruption imports goods. The illicit actor then uses government connections to mislabel the goods or forge customs declarations and reexport goods to a prohibited destination.

- **An illicit actor establishes another company in a third jurisdiction**. An illicit actor subject to sanctions or export control restrictions establishes a company in a third jurisdiction. To disguise the connection, the non-restricted company is registered in the name of residents of the third country and bears a generic name. The company is then used as a transshipment hub, accumulating export controlled or restricted goods and moving them to the prohibited parent company.

- **An illicit actor "peels" part of a shipment while transshipping**. An illicit actor "peels" part of a shipment while transshipping to another non-sanctioned country; as in, the illicit actor delivers a shipment while passing through a sanctioned country (e.g., when a vessel docks in a port in a sanctioned country while enroute to another location).

- **An illicit actor exports or reexports under the disguise of transshipment**. An illicit actor exports or reexports under the pretence of transshipment. An illicit actor located in a landlocked country states that it has to ship the goods via a sanctioned country due to difficulties arranging other routes, while in fact, the country in question is the final destination of the goods.

Separately, LFIs should also consider risks related to landlocked countries as part of their enterprise-wide risk assessment, as further discussed in Section 4.1. Enterprise-wide Risk Assessment and Risk-Based Approach. Without direct access to coastal ports, landlocked countries must rely on transit countries to connect them with international markets. Sometimes such transit countries can be subject to restrictive sanctions or export controls, increasing the risk of potential non-compliance for an LFI.

4. Mitigating TBML and Illicit Transshipment Risks

To mitigate risks associated with TBML and illicit transshipment, LFIs should design and implement controls that are commensurate with the nature and size of their business. The sections below discuss how LFIs that are involved in trade transactions can apply preventive measures to identify, assess, manage, and mitigate the risks associated with the TBML and illicit transshipment. This is not a comprehensive discussion of all AML/CFT requirements imposed on LFIs. LFIs should therefore consult the UAE legal and regulatory framework currently in force.

The controls discussed below should be integrated into each institution's broader AML/CFT compliance program and supported by appropriate governance, independent audit, and training.

4.1. Enterprise-wide Risk Assessment and Risk-based Approach

Under Article 4 of the AML-CFT Decision, LFIs are required to identify, assess, and understand the ML/TF risks to which they are exposed in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. For this purpose, LFIs should also perform, document, and regularly update an enterprise-wide risk assessment that includes an assessment of risks related to trade. Conducting a risk assessment is the first step in LFIs effort to counter illicit finance, including TBML and illicit transshipment. Specifically, LFIs should evaluate the risks associated with customers involved in trade and the LFI's geographies, products, services, and role in a trade transaction. To form a clear understanding of their risk exposure, LFIs may opt to perform a standalone risk assessment of their trade finance business.

When performing the risk assessment, LFIs should take into account different categories of risk. The most common categories of risk are associated with **customers**, **intermediaries**, **geographies, products and services**, **delivery channels,** and **operations**.

- **Customers:** LFIs should identify customers with exposure to and involvement in trade. To better understand customer risk, LFIs should also assess customers engaged in potentially higher-risk activities, including industries that are recognized by global standard-setters and regulators as high-risk for TBML (as discussed in Section 2.4) and sanctions evasion (commodities trading, export/import, and related shipping and insurance, among others). Certain customer behaviour may also indicate higher levels of risk and thus require additional scrutiny, including cross-border transactions involving legal persons and arrangements or multiple shell or front companies; high transaction volumes involving individuals acting on behalf of legal persons or arrangements; customers who frequently transact with high-risk countries; customers located in a landlocked jurisdiction, and customers whose transaction behaviour is not related to their stated business purposes.

    - **Intermediaries**: As part of the customer risk assessment, LFIs should consider assessing to what extent customers involve intermediaries either in payment transactions or in the process of exporting/importing goods. In cases in which the involvement of an intermediary can decrease the level of transparency or does not appear to have a legitimate business purpose, LFIs should consider implementing controls that would require collection of additional information from the relevant customers as a best practice.

- **Geographies**: LFIs should consider the countries their customers are exposed to (e.g., customers' locations of incorporation or registration, primary place of business, and locations of beneficial owners), flow of the transactions facilitated by the LFI, and the LFI's own locations around the world. Identifying and understanding jurisdictions and regions exposed to specific sanctions evasions risks is particularly important in the context of international trade. LFIs should consider its geographic proximity to a country or region that is subject to sanctions as a risk factor in the risk assessment, including publicized instances of specific countries flagged by the regulators or reputable news sources as common transshipment hubs.

  As discussed in Section 3, LFIs should also consider the risks related to landlocked countries, whether through their customers' locations or the LFI's own locations. A landlocked country may rent port space, warehouses, and other facilities from neighbouring countries that have seaports, and these neighbouring countries may be subject to restrictive sanctions or export controls. LFI should therefore seek to understand the true origin or destination of goods based on a thorough review of trade finance documents provided by their customers.

- **Products and Services**: LFIs should consider their products and services and assess the inherent risk associated with such products by taking into account product transparency, complexity, potential for

intermediation, settlement times and terms, usage of cash, and cross-border funds flows. Specifically, LFIs should evaluate products and services that finance trade transactions and the extent to which these products and services can be abused for illicit activity, such as by masking end-users and disguising payments. Generally, trade-related transactions carry more risk for LFIs compared to other financial transactions due to the fact that the LFIs do not always know all the parties involved in a trade and the goods that are being traded.

For example, although wire transfers are generally less complicated mechanisms of financing trade transactions, it is often more challenging for LFIs to obtain sufficient information to understand the purpose of transactions, the underlying goods or services paid for by the transactions, the shipping or transportation of the goods involved, and other parties related to the transactions (e.g., importers and exporters).

- **Delivery Channels:** Delivery channels are an important element of risk that is closely related to products and services. The primary drivers of risk for delivery channels include whether a particular delivery channel involves non-face-to-face transaction initiation mechanisms, is operated by or through a third party, or offers rapid or near-instantaneous processing and settlement. Services provided through higher-risk delivery channels—that create anonymity and obscure the source or destination of funds—are more susceptible to abuse by illicit actors for TBML and sanctions evasion.

- **Operations:** Operational risk encompasses risks of loss and disruptions to business that stem from ineffective or failed internal processes, people, or systems or from external events. Operational risk includes inadequate or fluctuating staffing levels; material changes in the size or composition of the customer base; fluctuations in technological systems and models used to support AML/CFT compliance; and the emergence of backlogs of transaction monitoring alerts or CDD refreshes.

Risk assessments should provide a consolidated assessment of an LFI's ML/TF risks across all business units, including those of branches, subsidiaries, parent entities, or other affiliates located outside the UAE. The identified risks should be consistently reported to senior management, and any internal control deficiencies noted during the risk assessment process should be appropriately tracked and remediated. LFIs should also ensure that their risk assessments are integrated into their overall risk management frameworks. Risk assessments should be an ongoing process and should be reviewed regularly to ensure that they remain relevant, effective, and up to date.

4.2. CDD and EDD Measures

4.2.1. General CDD Measures

Under Article 5 of the AML-CFT Decision, LFIs should conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no business relationship. An LFI's CDD program should cover, at a minimum: customer identification and verification; beneficial owner identification and verification; understanding of the nature of the customer's business and purpose of the business relationship; and ongoing monitoring. CDD, and where necessary EDD, are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers.

In the context of trade, each LFI should identify which party to a trade transaction is their customer and subject to the LFI's CDD process. Although it is not the responsibility of the LFI to perform due diligence on all parties to a trade transaction, an LFI should have an appropriate understanding of their customer's business model. CDD measures are particularly important for clients that engage in open account trade where it is difficult to gather information about each trade at transaction level. In addition, trade settlement on open account in and of itself may serve as a red flag if the underlying LFI customer is an exporter and/or if trade transactions involve particularly complex goods or delivery methods, since open account trade is one the least preferable means of settlement from the exporter's

perspective. As a best practice, the LFI should consider requesting specific information in order to appropriately understand the customer's business model, which could include:

- Purpose of the customer's trade activities;
- History and geography of operations;
- Goods or services exchanged and industries serviced;
- Licenses required for the trade of underlying goods or services, if applicable;
- Principal counterparties with whom the customer intends to transact with;
- Parties involved in the trade (e.g., shipping company, freight forwarder, insurer, etc.);
- Countries where the counterparties are located; and
- The anticipated transaction volumes, value, frequencies, and flows.

If an LFI determines that a customer or prospective customer has materially misrepresented itself or its business, it should not accept the customer; should exit the relationship if one has been established; should add the customer, its beneficial owners, directors and managers to its internal watchlists; and should file a suspicious activity report ("SAR") or suspicious transaction report ("STR") with the FIU. Please refer to the goAML platform to view a list of red flags and SAR and STR options relevant to TBML.

In addition, if the LFI detects a change in a customer's trade-related activities from the customer's profile established at onboarding, the LFI should request further CDD information to assess whether there are legitimate grounds for the customer's activity. For instance, the irregularity in a customer's trade-related activity could be caused by a change in a customer's CDD information that should be reflected in the customer's CDD file (e.g., the customer changed their headquarters office without informing the LFI). If the LFI is unable to establish a reasonable explanation for the customer's activity, the LFI should have protocols in place to escalate the activity for further review, as discussed in Section 4.4.2. Suspicious Transaction/Activity Reporting.

LFIs should ensure proper documentation and record-keeping of both the CDD conducted at onboarding and any updated information collected on the customer throughout the customer's business relationship (such as a record of site visits; call logs; and the rationale for onboarding a high-risk customer).

Utilizing the information collected through general CDD, an LFI should screen the following parties against lists of sanctioned persons, internal watchlists (such as lists of customers previously exited for financial crime reasons), and, on a risk basis, relevant ML/TF information sources (such as adverse media databases) prior to a customer's onboarding:

- All customers, regardless of risk rating or risk profile;
- Beneficial owners of legal entity customers;
- Natural persons appointed to act on behalf of the customer;
- Directors, partners, and managers of customers that are legal persons;
- Natural persons having executive authority over customers that are legal arrangements; and
- Principal counterparties with whom the customer intends to transact, if collected as part of CDD.

With respect to sanctions lists, the parties listed above must be screened prior to a customer's onboarding and on an ongoing basis thereafter. The results of screening and assessment by the LFI should be documented.[18]

LFIs should consult the UAE legal and regulatory framework currently in force and related CBUAE Guidance for a full discussion of their CDD obligations and of the CBUAE's expectations for CDD procedures. Consistent with local regulatory requirements, all LFIs must ensure compliance, where applicable, with Recommendation 10: Customer Due Diligence, as outlined in the FATF 40 Recommendations.

Additional detail regarding general CDD measures is available in the CBUAE's *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions*, sections 6.1 through 6.3.[19]

---

[18] Please see Section 4.3. to see more about sanctions screening best practices.
[19] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

4.2.2. EDD Measures for Heightened Trade-related Risks

The AML-CFT Law and the AML-CFT Decision impose EDD obligations on LFIs with respect to three classes of customers or transactions:

- Customers that are politically exposed persons ("PEPs"), which include the direct family members or associates known to be close to the PEPs (AML-CFT Decision, Article 15);
- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries (AML-CFT Decision, Article 22); and
- Correspondent banking or other similar relationships (AML-CFT Decision, Article 25).

In addition to these classes of customers and transactions, for which EDD is mandatory, LFIs are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for illicit finance.

In the context of trade and as a best practice, in order to mitigate the risk of illicit transshipment, an LFI should consider implementing procedures to identify certain dual-use or high-risk goods, if warranted based on its risk assessment. Such procedures may include obtaining additional information when a customer provides a vague description of the goods (for example, software, chemicals, and technology), which presents challenges to reasonably identify the intended use for these goods. This may also include incorporating certain key search words into the LFI's screening system (for example, defence, military, unmanned aerial vehicles, ammunition, and lasers) to ensure that screening software intersects payments referencing such items for manual review. More generally, if a customer appears to be involved in dual-use or high-risk goods, LFIs should request further information on the goods or services exchanged for this information to be screened by the LFI.

As part of this due diligence, the LFI should also establish whether the customer will be trading goods subject to export or import controls and whether any of the goods traded by the customer will ultimately be transported to or through a sanctioned country. Additionally, LFIs should inquire whether their client engages in open account trade and if the client does, the LFIs must ensure that they understand the trade activities of their client. For particularly sensitive goods or industries (for example, goods with military applications, oil, minerals and other natural resources), an LFI may consider having a customer complete a tailored due diligence questionnaire, indicating its internal compliance policies.

In cases where customers, products, or countries involved in a trade transaction are deemed to be "high risk;" where the goods are seen as being high risk or of a "dual use" in nature; or where a customer is the subject of frequent requests for information either from counterparty banks or from government authorities, LFIs should apply EDD which may include a combination of the following steps:

- Putting a transaction on hold until the LFI understands, and obtains supporting documentation for, the full picture of the transaction including the goods, countries, and parties involved;
- Using independent databases to verify customer and beneficial owner(s) identifying information and business industry to inform the individual customer risk assessment;
- Using third party service providers that offer trade finance documents authentication services;
- Ensuring that the customer is aware of the risks associated with trade, including TBML and sanctions evasion;
- Conducing additional searches (e.g., verifiable adverse media searches, open-source intelligence) to inform the individual customer risk assessment;
- Obtaining an intelligence report on the customer or beneficial owner(s) to better understand the risk that the customer or beneficial owner(s) may be involved in TBML;
- Verifying the source of funds or source of wealth involved in the business relationship to be satisfied that they do not constitute the proceeds of illicit activities;
- Collecting and screening additional trade-related documentation from the customer, such as invoices, bills of lading, and certificates of origin;
- Collecting and reviewing information (e.g., route, ownership/management, vessel picture and class, IMO number, AIS activity, etc.) about the vessels involved in a transaction, if relevant;
- Collecting business references for the customer and conducting other market research; and
- Seeking additional information from the customer about the purpose and intended nature of the business relationship.

While, as stated in section 2.1.2.1, it remains challenging for LFIs to identify trade conducted on an open account, LFIs can nevertheless apply additional measures such as conducting random transaction sampling, increasing the risk profile of customers engaged in such trade as determined based on KYC refresh, or adding particularly high risk clients engaged in such trade to internal watch lists to ensure manual review of their transactions meeting certain thresholds. LFIs may also detect unusual transactions using transaction monitoring tools. These measures may help LFIs in deciding whether EDD is necessary for a particular client or a transaction.

Following the initial CDD and EDD, the LFI should perform ongoing monitoring. Ongoing monitoring has to be done continuously and if triggered by a specific event, the LFI should conduct additional scrutiny of transactions to determine whether they are consistent with the LFI's knowledge of the customer and the nature and purpose of the business relationship. Monitoring also involves identifying changes to the customer profile throughout the relationship (for example, their behaviour, use of products, payment flows through the account, geographies of operations), and keeping it up to date, which may require the application of new, or additional, CDD measures.

4.3. Targeted Financial Sanctions Obligations

The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the UNSC under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, the Cabinet Decision 74 of 2020 sets out the legal and regulatory framework in the UAE regarding Targeted Financial Sanctions ("TFS"), including the UAE Local Terrorist List and the UN Consolidated List.

In addition, under Article 21 of Cabinet Resolution No. (74) of 2020, LFIs are required to have suitable risk management systems and take sufficient measures to identify whether a customer, or the beneficial owner of a customer, has been added to an international sanctions list or the UAE Local Terrorist List. In practice, it will generally be appropriate to conduct screening prior to onboarding and ongoing screening on all customers.

LFIs should take appropriate steps to screen customers and transactions. Trade transactions frequently use Society for Worldwide Interbank Financial Telecommunication ("SWIFT") messages, and LFIs with a high volume of SWIFT messages should determine whether their screening efforts are adequate to detect involvement of a sanctions target, particularly in the case of screening backlogs, unusual spikes in screening activity, updates to the relevant sanctions lists, and other operational events.

All the information available to an LFI (e.g., payer's information, payee's information, and intermediary's information) should be screened against relevant sanctions list to ensure there is no sanctioned person involved in the transaction. As a best practice, screening can also cover all additional documentation, outside of SWIFT messages, collected as part of a trade transaction. The timing of the screening should be in a manner that allows blocking of assets once such assets are in an LFI's possession.

For more information and details on obligations in relation to sanctions obligations, LFIs should consult the Executive Office for Control and Non-Proliferation ("EOCN")'s *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*[20] and the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*" and *Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*.[21]

Best Practices: Sanctions Screening of Trade Transactions

- LFIs should ensure that their sanctions screening program is able to absorb the data points that might indicate involvement of sanctioned persons in trade-specific message types (such as SWIFT MT 7XX or MX messages), including, for example, names of the beneficiary, originator, ultimate beneficiary, ultimate originator, country codes, where relevant, intermediary banks, and high-risk terms mentioned in free-text fields.

- While the availability and the placement of such information varies depending on the type of transaction and the means of communication (such as SWIFT and other financial messaging protocols), an LFI should screen the following pieces of information when available:

    - *Any names whether individual, entity, or vessel regardless of their role in a trade transaction (i.e., principal parties or intermediaries).*

- LFIs should conduct sanctions screening of documentation that the parties to a trade finance transaction make available to an LFI, such as invoices, bills of lading, shipping documents, and customs declarations, which are examples of documents involving documentary trade finance products. LFIs should consider using technologies that will recognize certain information on trade documents to increase the quality of their sanctions screening controls.

    - Please refer to Section 2.1.1.2. Types of Documents Available in Documentary Trade Finance Instruments for information on the types of documents involved in documentary trade finance.

- LFIs should similarly employ screening technologies that take into account name variations of parties.

- As referred to in Section 4.2.2. EDD Measures for Heightened Trade-related Risks, LFIs should consider implementing procedures to identify certain dual-use or high-risk goods, which may include obtaining additional information when a customer provides a vague description of the goods (for example, software, chemicals, and technology).

- LFIs should verify to what extent a trade transaction may involve a country subject to comprehensive or substantial sanctions imposed by third countries. If an LFI detects such links, it should conduct an analysis on whether the sanctions imposed by a third country could have any impact on the LFI's sanctions exposure and associated risk appetite, even if the sanctions are not applicable in the UAE.

- LFIs should review a customer's location, including whether a customer has exposure to a landlocked country, to determine whether the customer's trade-related activities are in line with the country in question. For instance, an LFI should assess whether the items that are being traded by a customer are produced in that landlocked country. Similarly, an LFI should understand how goods are being delivered to a landlocked country and ensure that a customer's transportation documentation is complete and does not stop with the shipping documentation. This will help the LFI determine whether the customer could be using the landlocked country as a transshipment point to or from another country that might be subject to financial sanctions or trade restrictions.

- LFI should also consider developing a list of high-risk landlocked countries, for example, landlocked countries that are neighbouring or surrounded by countries subject to financial sanctions or trade restrictions. A few examples of such countries include Afghanistan, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan, but this list may change as sanctions continue to evolve.

Best Practices: Sanctions Screening of Trade Transactions (continued)

- LFIs should consider including sanctions clauses in trade finance instruments to allow non-payment in case of a true sanctions hit.

- LFIs should ensure an employee cannot proceed with a trade-related transaction unless an appropriate screening unit within the LFI has cleared all sanctions-related alerts.

Please note, ISO 20022 is global open standard for financial information and provides an improved, standardized way of transacting and communicating between LFIs. The richer data means an increased opportunity for LFIs to detect suspicious activity as part of the LFI's transaction monitoring program. LFIs should ensure they are able to process this enriched data and communicate using the XML format.

[20] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.
[21] Available at: https://www.centralbank.ae/en/cbuae-amlcft

4.3.1. Confirmed Matches

If an LFI identifies a confirmed match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List, LFIs are required to take the following actions:

- Implement all necessary measures without delay as outlined in Article 15 of Cabinet Resolution No. (74) of 2020, to include freezing without delay, refraining from offering any funds or other assets and services, and reporting freezing measures to the EOCN and CBUAE; and

- If the confirmed match is a potential customer, reject the transaction immediately and report the case.[22]

Per Section (5) of Article 21 of Cabinet Resolution No. (74) of 2020, LFIs are expected to report any freezing measures, prohibition to provide funds or services, and any attempted transactions immediately via the goAML platform by selecting the Funds Freeze Report ("FFR") option. LFIs should also ensure that all necessary information

and documents regarding the confirmed match are submitted along with the FFR. Pursuant to Section (1) of Article 22 of Cabinet Resolution No. (74) of 2020, supervisory authorities should receive all information within five working days.

[22] See also EOCN, *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*, section 4, available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.

4.3.2. Partial Name Matches

If an LFI identifies a partial name match of an individual, entity, or group to the key identifiers published in the UAE Local Terrorist List or the UNSC Consolidated List, LFIs should take the following actions:

- Cross-check the identifiers published on the relevant sanctions list with the LFI's internal customer, beneficial ownership, and other data as well as external sources where appropriate to determine whether the partial name match is a confirmed match or can be waived as a false positive; and

- If the LFI is unable to determine whether the partial name match is a confirmed match or a false positive, the LFI must suspend any transaction and report the case to the EOCN and the CBUAE and uphold the suspension measures until a response is received from the EOCN on the status of the partial name match.

LFIs are expected to submit a Partial Name Match Report ("PNMR") through the goAML platform within five business days of implementing the suspension measures. LFIs should ensure that all necessary information and documents regarding the potential match are submitted to the PNMR.

4.4. Transaction Monitoring and Suspicious Transaction/Activity Reporting

4.4.1. Transaction Monitoring

Under Article 16 of the AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may require filing of an STR, SAR, or other report types. Moreover, as required by Article 7 of the AML-CFT Decision, LFIs must continuously monitor all their transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity, and the risks they pose, including, when necessary, the source of funds. Transactions may be suspicious simply by virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries). Alternatively, transactions may be suspicious because, together with other transactions, they form a pattern that diverges from expected or historical transactional activity and may otherwise be indicative of illicit activity.

Transaction monitoring programs should be calibrated to the size, nature, and complexity of each institution. Transaction monitoring can include manual monitoring processes and the use of automated and intelligence-led monitoring systems (e.g., intelligence related to the vessel routes can be integrated into the monitoring program of an LFI to tackle TBML), with automated solutions being the preferred option. LFIs with a larger scale of operations are expected to have automated systems capable of handling, in real time, the risks from an increased volume and variance of transactions. Such systems may incorporate external data points (e.g., use of international trade and commodities pricing databases) to increase the LFI's capability in detecting suspicious activities. LFIs utilizing automated systems should apply rules with appropriate thresholds and parameters that are designed to detect common typologies for illicit behaviour. While smaller LFIs may rely on transaction monitoring systems that are less automated, they should still ensure that their systems and controls are appropriately executed to address the risks from their day-to-day transactional activity. With that understanding, smaller LFIs should look to employ automated systems wherever feasible.

Best Practices: Trade-related Transaction Monitoring

- LFIs should take into account the nature of their trade-related products and services in addition to common TBML typologies and red flags when designing appropriate trade-related monitoring mechanisms.
    - For instance, an LFI may use automated monitoring to flag higher-risk customers for investigation, which may include conducting a lookback to understand a customer's patterns of activity. In all cases, the type and degree of monitoring should appropriately match the ML/TF risks of the LFI's customers, products and services, geographic exposure, and delivery channels, and may therefore vary across an LFI's business lines or units, where applicable.
- LFIs should periodically reassess and test their transaction monitoring systems in the context of trade-related activities, taking into account changes in their customer base, business operations, and ML/TF-related risks and trends.
- LFIs should use intelligence related to vessel(s) involved in a trade to detect anomalies in a customer's behaviour that may be indicative of TBML.
- To detect the risk of transshipment, LFIs should consider trends associated with a customer's transactional behaviour in line with any updates to sanctions and export control restrictions.
    - For instance, an LFI should consider a customer's change in behaviour following new restrictions imposed by international bodies, or other countries. Even though sanctions imposed by other countries are not applicable in the UAE, and though there might be legitimate reasons for such a change in behaviour, those changes in behaviour following new restrictions may be indicative of less transparent practices and potentially fraudulent activities by a customer.
- LFIs should consider using external resources to determine whether the price of underlying goods or services is in line with the market value, and in this context, identify over- or under-invoicing of the goods and services. Such external sources are most relevant in the context of commodities trading where the price of the commodity in question is less prone to variation. This control may also be referred to as "price-validation."
- LFIs should consider the information available in a customer's CDD/KYC file and compare this information with a customer's transactions. For instance, if the customer at onboarding indicated that it would have a certain transactional behaviour, such information should be used when reviewing their transactions. Any unusual or unexplained deviation from a customer's expected activity should be escalated to an LFI's Compliance team for further review.
    - If possible, such information should be used for designing automated controls aimed at detecting unusual and potentially suspicious activities.
- LFIs should use the additional information made available to them by virtue of new ways of communication (e.g., MX messages), such as information related to an ultimate beneficiary or ultimate creditor.

4.4.2. Suspicious Transaction/Activity Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, LFIs must file an STR, SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted

transaction, or certain funds constitute, in whole or in part, or are intended to be used in a crime. This applies equally in relation to suspicious transactions involving trade-related activities.

When an LFI is assessing whether to file an STR or SAR, it should, at a minimum:

- Review existing CDD/KYC information on the customer, and, where required, obtain additional information;
- Use open-source intelligence to augment the information about the parties and/or suspicious transaction or activity;
- Review trade documents associated with the customer and/or transaction (e.g., customs declarations, title and transport documents, bills of lading, invoices, packing lists, certificates of origin and inspection, etc.);
- Conduct independent company verifications and adverse news media searches;
- Conduct customer account activity reviews; and
- Review the results of any available screening and monitoring processes, including on a customer's past transactions.

When analysing trade transactions for unusual or potentially suspicious activity, LFIs should consider obtaining copies of official government import and export forms to assess the reliability of documentation provided. If the LFI obtains what it considers to be a reasonable explanation for the trade transaction and the transaction overall appears to be in line with a customer's business practices, it may conclude that there are no grounds for suspicion and take no further action.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a TBML-related activity, the LFI should consider filing an STR or SAR in the following situations involving higher-risk customers:

- A potential customer decides against utilizing the LFI's products or services after learning about the LFI's CDD requirements;
- A customer cannot provide required information (including documentation) about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- A customer cannot explain an unusual trade structure or routes for its trade-related transactions;
- A customer engages in trade-related transactions that are not in line with its size and profile;
- A customer provides documents that appear fraudulent or forged; and
- Other situations that are suspicious or involve activity with no legitimate business or other lawful purpose.

STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. By filing STRs with the UAE FIU, LFIs alert law enforcement authorities about suspicious behaviour and allow investigators to piece together transactions occurring across multiple LFIs. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.[23]

---

[23] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

4.5. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces and organized in accordance with the "three lines of defence" model. All three lines of defence should report up to and have the active support and oversight of the LFI's senior management, defined broadly to include executives, senior leadership, and the Board of Directors. The senior management plays an important role in the fight against TBML by establishing a strong culture of compliance, allocating appropriate resources, ensuring independence of the compliance function, and supporting the compliance department's efforts to detect and counter TBML. In particular, the senior management can take a proactive role in managing TBML and other ML risks by asking compliance functions to present periodic reports summarizing, for example, identified risks, any instances of non-compliance with LFI's policies, if any, root cause analysis, and remediation measures.

By putting in place appropriate governance, LFIs should be able to continuously monitor and manage TBML and illicit transshipment risks. As such, LFIs should ensure the following points are present in an AML/CFT program:

- The Head of Compliance/Money Laundering Reporting Officer ("MLRO") and an LFI's Compliance team should have the authority, independence, resources, and information necessary to understand, assess, and address TBML and illicit transshipment risks.

- The AML/CFT program should ensure a division of roles and responsibilities and ownership of risks relating to critical functions, including AML/CFT controls that manage the risks associated with TBML and illicit transshipment.

- Reporting lines and escalation channels should be clearly documented, and senior management should be regularly informed on how TBML and illicit transshipment risks are being managed through ongoing reporting and associated metrics.

No AML/CFT program is immune from shortcomings whether operational or structural. Independent testing of an LFI's AML/CFT program plays a crucial role in ensuring the AML/CFT program's ongoing effectiveness. Therefore, it is vital that LFIs regularly undergo risk-based independent audits to evaluate the design and operational effectiveness of AML/CFT program controls, including due diligence, screening, and monitoring processes for reviewing trade transactions and customers engaged in trade activity. The outcome of the independent audit should be shared with an LFI's senior management who are responsible for ensuring that all identified gaps are appropriately tracked and remediated.

See Section 8 of the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* for further information.[24]

[24] Ibid.

4.6. Training

Training and raising awareness are an effective way to manage risks associated with TBML and transshipment. LFIs should implement a training program that is tailored to their risk profile and is delivered to all appropriate employees. LFIs should consider delivering additional training to employees regularly exposed to high-risk customers or trade-related activity.

More specifically, LFIs should ensure that the training:

- Is up-to-date and incorporates the most recent guidance from the relevant authorities;

- Is delivered periodically, with the frequency determined by the risk exposure of each LFI;
- Provides information about various products and services that are exposed to TBML and transshipment risks;
- Describes the system of internal controls designed to mitigate TBML and transshipment risks;
- Includes relevant, and if available, real-life case studies;
- Describes emerging trends and red flags associated with TBML and transshipment; and
- Provides clear guidance on the course of action when a suspicious activity is detected.

LFIs should keep the record of the attendance and test participants knowledge of the training to the extent possible. Such training should be offered to new employees who are exposed to the risk of TBML and transshipment, and the training should be refreshed regularly.

4.7. Record-keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/TF risk assessment and mitigation measures, as well as records, documents, data, and statistics for all financial transactions; records obtained through CDD measures and ongoing monitoring (including copies of personal identification documents); account files and business correspondence; and SARs or STRs and results of any analysis performed.

LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. In the context of processing trade-related transactions, LFIs should record and retain trade-related documents and information in a structured database to comply with record-keeping and AML/CFT and TFS obligations. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs should make the records available to the competent authorities immediately upon request. Consistent with local regulatory requirements, all LFIs must ensure compliance with FATF's Recommendation 11: Record Keeping.

The aforementioned provisions also require that all records be retained for at least five years from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

Annex 1. TBML and Illicit Transshipment Red Flags

The following is a list of red flags and suspicious activity indicators associated with TBML and illicit transshipment. This list is a compilation of guidance provided by the Dubai Financial Services Authority,[25] FATF,[26,27] and other regulatory bodies or industry groups.[28, 29]

Red flags relating to payments and trade transactions:

- The transaction involves receipt of cash (or other payments like wire transfers, checks, bank drafts or postal money orders) from unrelated third parties, an intermediary, or front or shell companies apparently unrelated to the supplier or purchaser of goods or that do not appear on the letter of credit supporting documentation.
- Cash deposits or other transactions of a trade entity are consistently just below relevant reporting thresholds.

- A trade entity makes very late changes to payment arrangements for the transaction (for example, the entity redirects payment to a previously unknown entity at the very last moment, or the entity requests changes to the scheduled payment date or payment amount.)

- Payment for imported commodities is made by an entity other than the consignee of the commodities with no clear economic reasons (e.g., by a shell or front company not involved in the trade transaction).

- The transaction involves the use of repeatedly amended or frequently extended letters of credit without reasonable justification or frequent amendments involving the beneficiary, location of payment, changes to countries of origin or destination without an apparent reason.

- When asked, a customer is unable or refuses to produce appropriate documentation (e.g., invoice or any other document) or fails to provide adequate information about the originator, beneficiary, and purpose of the wire transfer.

- The method of payment appears inconsistent with the risk characteristics of the transaction (for example, an importer makes an advance payment for a shipment from a new supplier in a high-risk country or transactions frequently involve rounding or whole USD/AED/other currency amounts).

- Documents provided as part of a letter of credit are illogical, illegible, appear to have signs of forgery or alteration, or include documents purported to be issued by government authorities but without appropriate stamps or letterhead.

- Documents provided as part of a letter of credit contain significant discrepancies (for example, invoice and bill of lading contain different amount, price, or description of the goods; terms and route of shipment on the bill of lading are inconsistent with the terms of the letter of credit).

- Documents that are provided are inconsistent or include mismatches.

- Documents include the use of trade contracts for transferring value of intangible assets.

- The type and volume of the goods or the overall size or structure of a transaction appear to be inconsistent with the customer's usual business activity (for example, a customer engaged in wholesale of electronics purchases construction materials).

- Transactions or trade finance structures appear beyond customer's capacity or expertise.

- Payments for goods originate in third countries that are not the importing country or from importer's bank account in a country when the importer does not operate.

- Beneficiary or applicant of a letter of credit appears too willing to waive discrepancies in documentation presented for payment.

- Beneficiary of a letter of credit requests the payment to be made to a country other than its stated location.

- Sudden onset and equally sudden cessation of payments – typically wire transfers – within a short duration.

- Customer activity deviates significantly from its historical patterns (new markets, monetary value, frequency of transactions, volume of goods).

- Trade transactions seem to contradict the customer's/organization's core business.
- Customer often asks to open letters of credit that expire unutilized.
- Customer requests an advanced waiver or non-standard clauses without reasonable justification, or engages in an unnecessarily complex trade transaction.
- Customer changes terms of the trade agreement (for example, a customer changes the beneficiary to a trade transaction or changes their payment location without reasonable justification).
- Irregularities related to the shipment including unreasonably long voyage of a vessel, involvement of ports with higher risk of transshipment, manipulated voyage data, and involvement of sanctioned vessels.

Red flags relating to jurisdictions:

- The commodity is shipped to (or from) a jurisdiction designated as "high-risk" for ML/TF activities or jurisdictions under FATF increased monitoring or non-cooperative jurisdictions.
- The commodity is transshipped through one or more such high-risk/sensitive jurisdictions for no apparent economic reason.
- Transaction structure and/or shipment terms appear unnecessarily complex or unusual and may be used to obscure the true nature of the transaction or origin of goods.
- Unnecessarily complicated and complex supply chains, involving multiple transshipment points that do not appear to have a valid business justification.
- Unreasonable involvement of FTZs in trade transactions.
- After an LFI refuses to open a letter of credit or process a payment, customer initiates another transaction with the amended origin or destination of goods.
- Transaction involves unusual shipping routes (e.g., use of circuitous shipment routes) or routes that do not make economic sense.
- Transaction involves Free Trade Zones/Special Economic Zones. To make the jurisdiction attractive for business, zone authorities may implement separate company formation services from those that exist in the rest of the jurisdiction. Companies established in Free Trade Zones may therefore provide little-to-no ownership information and profit from other non-transparent practices. Goods introduced into Free Trade Zones are generally not subject to the usual customs controls.[30]
- Payments are routed in a circle; funds are sent out from one country and received back in the same country, after passing through another country or countries.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns of the jurisdiction (i.e., trade in goods other than goods which are normally exported/imported by a jurisdiction), or which does not make any economic sense (e.g., semi-conductor manufacturing equipment being shipped to a jurisdiction that has no advanced technology manufacturing capabilities).

Red flags relating to goods:

- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.

- The size of the shipment appears inconsistent with the scale of the exporter's or importer's regular business activities.
- The type of commodity being shipped is designated as "high-risk" for money laundering activities (see Section 2.4 for examples of such goods).
- The shipment terms or methods are inconsistent with the type of goods (for example, shipment of frozen foodstuffs in a regular container; the use of a forty-foot container to transport a small amount of relatively low value merchandise).
- Improbable types of goods, origin, quantities, or destination (for example, shipment of oil from a country that has no oil reserves).
- Documentation showing a higher or lower value or cost of goods than that which was declared to customs or paid by the importer (i.e., commodity over-valuation or undervaluation).
- Customers involved in potentially high-risk activities, including trading in items subject to export/import restrictions (e.g., equipment for military or police, weapons, ammunition, chemical mixtures, classified defence articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil or gas).
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Carousel transactions, meaning the repeated importation and exportation of the same high-value commodity.
- Packaging inconsistent with commodity or shipping method.
- A customer or a counterparty without significant industry experience begins trading in sophisticated equipment.

Red flags relating to corporate structures used:

- A transaction involves the use of front (or shell) companies.
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities.
- Previously established customer specializing in one sector that unexpectedly pivots into an entirely unrelated sector (for example, an IT company quickly establishes a foothold in the acquisition and distribution of bulk pharmaceuticals).
- A trade entity is simultaneously involved in more than one unrelated sector.
- Transaction involves newly formed companies in competitive markets that, at the onset, engage in high volume or value transactions.
- A trade entity's identifying information appears inconsistent with the business profile (for example, a company trading in medical equipment is registered at a residential address; a company trading in sophisticated manufacturing equipment is a sole proprietorship).

- A trade entity displays a notable lack of typical business activities (for example, a company lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances).

- Transactions reveal links between representatives of companies exchanging goods (for example, companies exchanging goods are registered to family members).

- Owners or senior managers of a trade entity appear to be nominees acting to conceal the actual beneficial owners (e.g., they lack experience in business management or lack knowledge of transaction details, or they manage multiple companies).

- Due diligence reveals numerous sole proprietorship businesses/private limited companies set up by seemingly unrelated people are in fact controlled by the same group of people.

- A trade entity engaged in trade of highly technical, sophisticated goods, has no online presence and/or use free email domains for business communication.

- A trade entity is registered or has offices in a jurisdiction with weak AML/CFT compliance.

- A trade entity is registered at an address that is likely to be a mass registration address (e.g., high-density residential buildings, post-box addresses, commercial buildings or industrial complexes, especially when there is no reference to a specific unit).

- A trade entity maintains a minimal number of working staff, inconsistent with its volume of traded commodities.

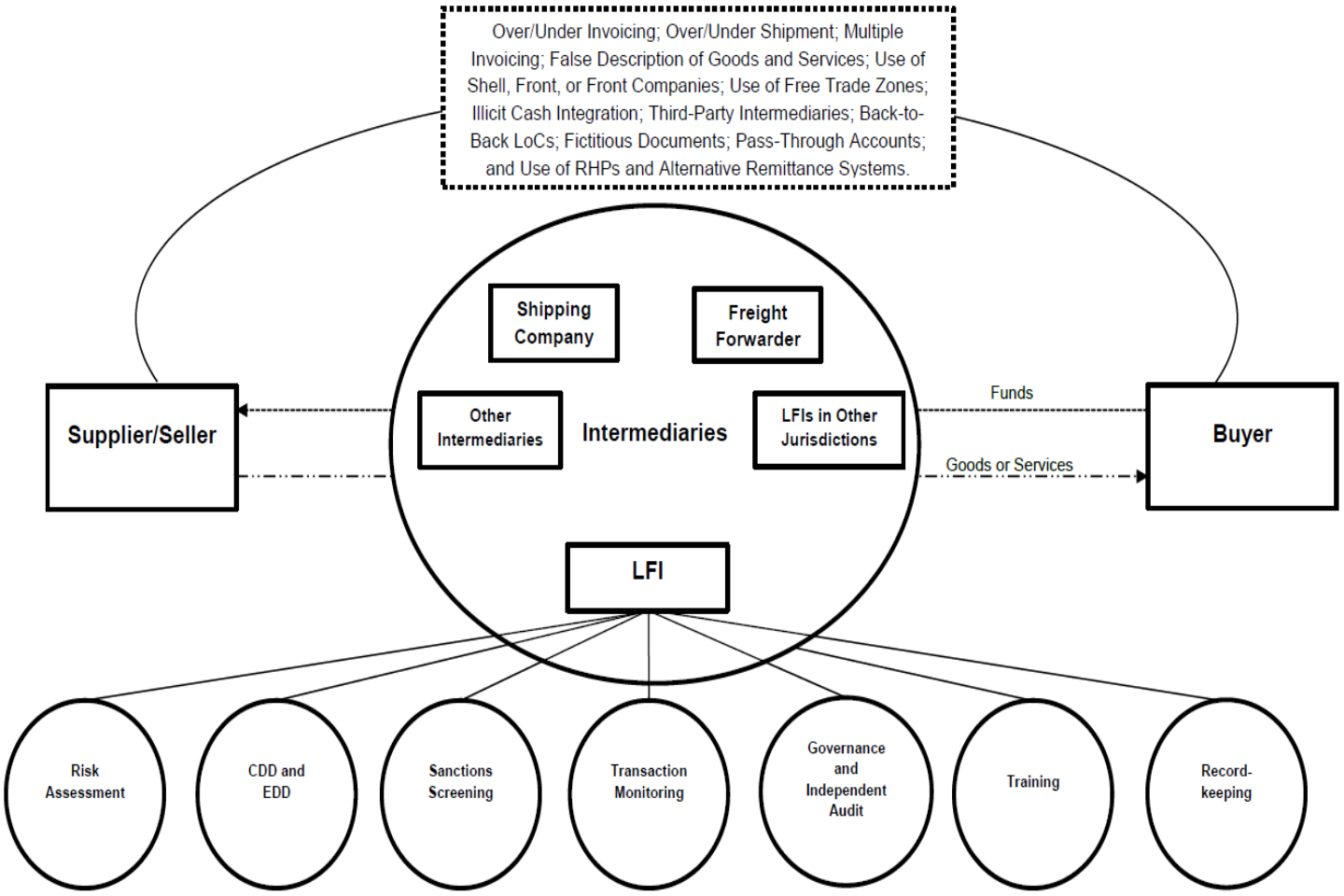
- The name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it, potentially in an effort to appear as part of the corporation, even though it is not actually connected to it.

- Use of fiduciary companies established in FTZ.

---

[25] Dubai Financial Services Authority, *Trade Finance Report*, 2016, https://www.dfsa.ae/application/files/1015/8425/3351/TF-Report-FINAL_Eng_12_october_2016_mid-res.pdf
[26] FATF, *Guidance on Trade-Based Money Laundering*, 2006, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf
[27] FATF, *Trade-Based Money Laundering Risk Indicators*, 2021, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Risk-Indicators.pdf
[28] BAFT, *Combating Trade Based Money Laundering: Rethinking the Approach*, 2017, https://www.amlc.nl/wp-content/uploads/2018/11/baft17_tmbl_paper.pdf
[29] Asia/Pacific Group on Money Laundering, *APG Typology Report on Trade Based Money Laundering*, 2012, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade_Based_ML_APGReport.pdf.coredownload.pdf
[30] For more information about how Free Trade Zones could be exploited in TBML, see: Money Laundering vulnerabilities of Free Trade Zones, Financial Action Task Force, March 2010, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingvulnerabilitiesoffreetradezones.html

Annex 2. Visual Synopsis



Annex 3. Synopsis of the Guidance

Introduction	Purpose and Scope of the Guidance	The purpose of this Guidance is to assist the understanding and effective performance by CBUAE licensed financial institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	This Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories: national banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers; and insurance and re-insurance companies, agencies, and brokers.
	Legal Basis	▪ Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments; ▪ Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations and its amendments; ▪ Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution and its amendments; ▪ CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

	Definitions and Acronyms	▪ Several frequently used terms and phrase are defined, and a list of acronyms used in the Guidance is provided.
Understanding and Assessing TBML	Background of International Trade System and Trade Finance	▪ Background on global trade and the role of the UAE in it. ▪ Overview of a wide range of commonly used trade finance products including letters of credits, factoring, etc. ▪ Overview of trade transactions particularly vulnerable to TBML, such as settlements on an open account or non-documentary trade finance
	TBML Typologies	▪ 12 typologies of TBML are identified and explained in detail along with relevant examples (e.g., Over- and Under-Invoicing of Goods and Services; Falsely Described Goods and Services; Use of Shell, Front, or Shelf Companies; Illicit Cash Integration; etc.).
	Service-Based Money Laundering	A brief introduction section to service-based money laundering (SBML) highlighting the risks SBML schemes represent.
	Economic Sectors and Products Vulnerable to TBML	▪ A section dedicated to seven economic sectors and types of products that are particularly vulnerable to the risk of TBML (e.g., Gold, Precious Metals, and Minerals; Car Parts and Vehicles; Clothing and Second-hand Textiles; etc.), with detailed explanations of each and relevant examples.
Understanding and Assessing Illicit Transshipment Risks	Illicit Transshipment	▪ Definition of transshipment is provided ▪ The risk of dealing with sanctioned countries using transshipment is discussed. ▪ Six illicit transshipment techniques that are relevant to the UAE are discussed in detail.
Mitigating TBML and Illicit Transshipment Risks	Enterprise-wide Risk Assessment and Risk-based Approach	▪ Per Article 4 of the AML-CFT Decision, LFIs are required to identify, assess, and understand the ML/TF risks to which they are exposed in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. ▪ This section provides information about how LFIs may approach their risk when implementing enterprise-wide risk assessments.
	CDD and EDD Measures	▪ This section provides points to be considered when conducing CDD (e.g., different pieces of information to be considered). ▪ The EDD sections lays down when EDD measures are warranted in line with the UAE regulations. Furthermore, it provides some best practices for conducting EDD.
	Targeted Financial Sanctions Obligations	▪ This section explains sanctions-specific obligations of LFIs under relevant authorities in the UAE and provides several best practices for sanctions screening in trade-related transactions. ▪ The section also includes guidance on how to adjudicate "hits" generated during the sanctions screening process.
	Transaction Monitoring and Reporting	▪ This section reminds LFIs of their obligations under Article 7 and 16 of the AML-CFT Decision concerning monitoring clients' activities; ▪ It offers best practices in transaction monitoring concerning trade-related transactions; and ▪ It explains the obligation to report suspicious activities or transactions.
	Governance and Independent Audit	▪ This section explains the three lines of defence model and specifies the role of senior management in a successful compliance program. ▪ It also discusses the importance of regular independent audits and, when necessary, remediation following each audit exercise.
	Training	▪ This section discusses the importance of training to manage the TBML and illicit transshipment risks and outlines points LFIs should

		consider when developing and implementing a successful training program.
	Record-keeping	▪ This section reminds LFIs of their obligations under Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision regarding record-keeping.
Annexes	TBML and Illicit Transshipment Red Flags	More than 50 red flags associated with TBML and illicit transshipment are listed for the LFIs. They are grouped in four categories: ▪ Red flags relating to payments and trade transactions; ▪ Red flags relating to jurisdictions; ▪ Red flags relating to goods; and ▪ Red flags relating to corporate structures used.
	Visual Synopsis	A visual synopsis of the Guidance has been provided that illustrates the parties to trade transactions, various intermediaries including LFIs, and the controls measures they can implement.