UNITED ARAB EMIRATES
MINISTRY OF ECONOMY & TOURISM

الإمارات العربية المتحدة
وزارة الاقتصاد والسياحة

Countering Money Laundering, Terrorism Financing and Proliferation Financing

Guidelines for Designated Non-Financial Businesses and Professions

المستشار / سالم أحمد الطنيجي

مدير إدارة مواجهة غسل الأموال وتمويل الإرهاب

Counselor / Salem Ahmed AlTeneiji

Director of the Anti-Money Laundering & Terrorist Financing Department

March 2026

Table of Contents

Part I Overview 3
1. Introduction 3
1.1. Purpose and Scope 3
1.2. Applicability 4
1.3. Legal Status 4
1.4. Structure of Guidelines 5
2. UAE's AML/CFT/CPF Legislative, Regulatory and National Strategy Overview 6
2.1. National Legislative and Regulatory Framework 6
2.2. DNFBP Supervisory Authorities[1] 7
2.3. International Legislative and Regulatory Framework 7
2.4. AML/CFT/CPF National Strategy Framework 8
3. Highlights of Key Provisions Affecting DNFBPs 8
3.1. Summary of Minimum Statutory Obligations of Regulated Entities 9
3.2. Statutory Prohibitions 9
3.3. Confidentiality and Data Protection 9
3.4. Protection against Liability for Reporting Persons 10
4. Key Concepts 10
4.1. Money Laundering (ML) 10
4.2. Terrorist Financing (TF) 13
4.3. Proliferation Financing (PF) 14
5. Overview of Applicable Sanctions for AML/CFT/CPF Violations 16
6. Risk Assessments 17
Part II Compliance Administration 18
7. Governance 18
7.1. Compliance Officer 18
7.2. Staff Training and Screening 22
7.3. Group Oversight 22
7.4. Independent Audit Function 23
7.5. Senior Management Responsibilities 24
7.6. Managing Compliance Challenges in Resource-Limited DNFBPs 25
Part III ML/TF/PF Risk Assessment 27
8. Identification and Assessment of ML/TF/PF Risks 27
8.1. Key Legal Requirements 27

8.2. Risk Based Approach (RBA) 27
8.3. Business-wide Risk Assessment (BRA) 28
Part IV Mitigation of ML/TF/PF Risks 35
9. Elements of a Solid AML/CFT/CPF Program 35
9.1. Internal Policies, Controls and Procedures 35
9.2. Customer Due Diligence (CDD) 36
9.3. Customer Due Diligence (CDD) Measures 40
Part V AML/CFT/CPF Reporting and Record Keeping 57
10. Suspicious Transaction Reporting 57
10.1. UAE Financial Intelligence Unit (FIU) 57
10.2. Processing of STRs by the FIU 58
10.3. Meaning of Suspicious Transaction 58
10.4. Identification of Suspicious Transactions 59
10.5. Requirement to Report 60
10.6. Specific Exemption from the Reporting Requirement 61
10.7. Procedures for the Reporting of Suspicious Transactions / Activities 61
10.8. Timing of Suspicious Transaction / Activity Reports (STRs/SARs) 61
10.9. Basic Structure of and STR or SAR 62
10.10. Confidentiality and Prohibition against "Tipping Off" 63
10.11. Protection against Liability for Reporting Persons 64
10.12. Handling of Transactions and Business Relationships after Filing of STRs 64
11. Record Keeping 67
11.1. Obligations and Retention Timeframes 67
11.2. Required Record Types 67
Part VI Appendices 70
12. Glossary of Terms 70
13. Useful Links 75

Part I Overview

1. Introduction

As an international commercial, financial, and technological hub that is characterized by a growing reputation for innovative advancements, the United Arab Emirates (UAE) faces considerable risks related to (ML), Terrorism Financing (TF), and Proliferation Financing (PF) risks. Criminals attempt to take advantage of the UAE's open economy, advanced financial systems, and robust business infrastructure to launder illegal funds and finance illicit activities.

The landscape of the UAE's framework for Anti-Money Laundering (AML), Combatting Financing of Terrorism (CFT) and Countering Proliferation Financing (CPF) is influenced by a constantly changing global context, characterized by evolving geopolitical factors, macroeconomic trends, and technological advancements that add layers of complexity in the deterrence of ML, TF, and PF. Thus, in light of the intricate nature of ML, TF and PF risks posed, a proactive and vigilant stance is crucial in implementing an adaptive AML/CFT/CPF framework to effectively tackle escalating threats.

The UAE's National Risk Assessment (NRA) is key in providing a comprehensive understanding of the ML, TF and PF threats, vulnerabilities and risks posed to the UAE. It offers a thorough analysis of primary sectors at risk, such as Designated Non-Financial Businesses and Professions (DNFBPs). In addition to the NRA, various sector-specific studies, strategic analysis reports, and risk assessments provide essential insights into the changing threats and trends, aiding in recognizing sector-specific vulnerabilities and risks.

The UAE's AML/CFT/CPF legislation and regulatory measures are fundamental to the nation's comprehensive AML/CFT/CPF framework. In conjunction with the strategic analyses and findings emanating from risk assessments, these legislations, regulatory measures and other applicable guidelines issued by competent authorities, constitute the foundation of the country's efforts to combat financial crime effectively.

To support the UAE's ongoing commitment to combating financial crime, the Ministry of Economy and Tourism (MoET) has developed comprehensive AML/CFT/CPF Guidelines for DNFBPs as means of providing a structured approach to enhance compliance programmes, strengthen governance, ensure effective reporting, and mitigate identified risks. These Guidelines are designed to complement existing laws and regulations and, when adhered to, will assist DNFBPs in upholding the integrity of the UAE's financial and economic sectors while ensuring alignment with international standards.

1.1. Purpose and Scope

The purpose of these Guidelines is to provide guidance and assistance to regulated DNFBP entities that fall under the supervisory purview of the Ministry of Economy and Tourism's (MoET), in order to provide better understanding and effective performance of applicable statutory obligations under the legal and regulatory framework in force in the UAE.

These Guidelines have been prepared MoET and set out minimum expectations regarding the factors that should be taken into consideration by each supervised DNFBP, when identifying, assessing and mitigating the risks of money laundering, terrorism financing and proliferation financing. These expectations align with, and are intended to complement, the existing legal and regulatory framework in force.

These Guidelines are not intended to limit, replace or otherwise affect the applicability of additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback (whether direct or indirect) that may be published periodically by any relevant authority in relation to regulated entities within the respective jurisdictions, or to any specific regulated entity.

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, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolutions* is outside of the scope of these Guidelines.

While full TFS-related procedures remain under the purview of the EOCN, these Guidelines do include supplementary PF-related risk insights in order to support DNFBPs incorporate PF considerations into their risk assessments. These additions, however, do not replace official EOCN mandates. DNFBPs should refer to the full TFS guidelines issued by the Executive Office for Control and Non-Proliferation

(EOCN), which detail obligations under *Cabinet Decision No. (74) of 2020*, including requirements for screening, freezing, and reporting in relation to designated persons or entities.

Additionally, DNFBPs should also refer to the *Guidance on Conter Proliferation Financing Institutions (FIs), Designated Non-financial Businesses and Professions (DNFBPs) and Virtual Assets Services Providers (VASPs)* and the *Guidance on Proliferation Financing Institutional Risk Assessment (PF IRA)* issued by EOCN to gain understanding of obligations pertinent to CPF measures and to the incorporation of PF risk in their Business Risk Assessment (BRA). When undertaking the BRA, it is recommended that DNFBPs consider PF-inherent risk factors and score PF risk separately from ML/TF considering dual-use goods and services, opaque corporate structures, high-risk jurisdictions, etc. in accordance with the guidance on PF IRA.

DNFBPs must fully comply with all TFS obligations related to TF and PF under *Cabinet Decision No. (74) of 2020* and all relevant EOCN guidance, inclusive of screening, freezing without delay and reporting obligations.

Furthermore, DNFBPs should note that MoET has developed dedicated supplemental guidance for each DNFBP sector falling under its supervisory purview. These publications, along with other guidance documents published by MoET, serve as practical extensions to the national AML/CFT/CPF framework and these present Guidelines with the intention to support regulated entities in the effective implementation of their statutory obligations through case studies which reflect sector-specific typologies and sector-specific red flag indicators to enhance detection capabilities. These materials should be read alongside these Guidelines to ensure a comprehensive and context-appropriate approach to governance, risk assessment and understanding, due diligence, ongoing monitoring and reporting.

1.2. Applicability

Unless otherwise noted, these Guidelines apply to all Designated Non-Financial Businesses and Professions (DNFBPs), and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and Commercial Free Zone, 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 Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing*.

Specifically, and without prejudice to the definition of a DNFBP as provided for in the relevant legislative and regulatory framework of the UAE (see Section 2.1, National Legislative and Regulatory Framework), these Guidelines are applicable to all such persons subject to the Ministry of Economy and Tourism's supervision, as listed below:

- Real Estate Agents and Brokers (REAB)
- Dealers in Precious Metals and Precious Stones (DPMS)
- Independent Accountants and Auditors (IAA)
- Trust and Corporate Service Providers (TCSP)

1.3. Legal Status

Pursuant to Article (49) of *Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing*, Supervisory Authorities are tasked with *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.*

Accordingly, these Guidelines serve as a practical tool to assist regulated entities in effectively implementing the relevant crime-combatting measures and are intended to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE. However, these Guidelines do not constitute additional legislation or regulation, and are not intended to set legal, regulatory, or judicial precedent. Regulated entities 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 regulated entities to meet 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. Regulated entities should perform their own assessments of the manner in which they should meet statutory obligations and should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to circumstances.

1.4. Structure of Guidelines

These Guidelines are organized into six (6) parts, corresponding to the following major themes:

- Part I - Overview
- Part II - Compliance Administration
- Part III - Risk Assessment
- Part IV - Mitigation Measures
- Part V - Reporting and Record Keeping
- Part VI - 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/CPF Law and/or the Executive Regulations to which it pertains. While it has been kept to a minimum, 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 regarding the statutory obligations of regulated entities such that no additional guidance on those sections is provided for in these Guidelines. In other cases, practical guidance is provided on subjects which are not explicitly addressed in the AML/CFT/CPF Law or the Executive Regulations, but which are nevertheless addressed either implicitly or by reference to recognized 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, regulated entities seeking further clarification on matters related to those sections are encouraged to contact their relevant Supervisory Authority through the established channels.

It is the Supervisory Authority's intention to update or amend these Guidelines from time to time, as and when it is deemed appropriate. Regulated entities are reminded that these Guidelines are not the only source of guidance on the assessment and management of ML, TF and PF risks, and that other bodies, including international organisations such as FATF, MENAFATF and other FATF-style regional bodies (FSRBs), and others also publish information that may be helpful in carrying out statutory obligations. It is the sole responsibility of regulated entities to keep apprised and always updated regarding the ML, TF and PF risks to which they are exposed, and to maintain appropriate risk identification, assessment, and mitigation programmes, and to ensure responsible officers, managers and employees are adequately informed and trained on all relevant policies, processes, and procedures.

Text from the AML/CFT/CPF Law and the Executive Regulations 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 section 12, Glossary of Terms). However, in the event of any inconsistency or discrepancy between the text or definitions provided for in the Law and/or the Executive Regulations and such quotations, summaries or paraphrases, or such defined terms, the former shall prevail.

2. UAE's AML/CFT/CPF Legislative, Regulatory and National Strategy Framework Overview

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 UAE, including the financial and commercial free zones, the crimes of money laundering, financing of terrorism, and proliferation financing 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/CPF legislation within the UAE is *Federal Decree-Law No. (10) of 2025 On Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Financing* (the "AML/CFT/CPF Law" or "the Law") and implementing regulation, *Cabinet Resolution No. (134) of 2025 Regarding the Executive Regulations of Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing* (the "Executive Regulations").

The UAE has further strengthened its regulatory framework through the issuance of *Cabinet Decision No. (109) of 2023 Regulating the Real Beneficiary Procedures*, reaffirming its commitment to enhancing transparency, combating financial crime, and promoting accountability within corporate ownership structures. It applies to all company registrars and corporate entities in the UAE, including those in the mainland and non-financial free zones, and mandates the establishment and maintenance of registers detailing Real Beneficiaries, Partners or Shareholders, and Nominee Management Members for corporate entities incorporated in these jurisdictions. Exemptions apply to entities wholly owned by the Federal or Local Government, their subsidiaries, companies incorporated in financial free zones (Abu Dhabi Global Market – ADGM and Dubai International Financial Centre – DIFC), and entities in which a Government Partner (Federal or Local Government) is a shareholder. Entities incorporated in ADGM and DIFC, including DNFBPs, are subject to the beneficial ownership regulations issued by their respective free zone authorities.

The foundation of the UAE's AML/CFT/CPF institutional framework is structured on the basis of a coordinated network of federal and local authorities. The Higher Committee Overseeing National Strategy on Anti-Money Laundering and Countering Financing of Terrorism, established in 2020, provides strategic oversight through the monitoring and evaluation of policies, supervision of mutual evaluations and proposal of legislative reforms. In support of this endeavour, the General Secretariat of the National Committee serves as the national coordinator overseeing the implementation and regular update of national strategies, risk assessment and ensures alignment with international standards under a risk-based and multi-agency approach. The National Committee for Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing (the National Committee) is the primary body for policy making and issuing of regulations to combat financial crime in the UAE in co-ordination with competent authorities. The National Committee determines and assesses the risks of crime on a national level and facilitates the exchange of information and co-ordination among the various agencies. The National Committee's sub-committees include[1]:

- Sub-Committee for National Risk Assessment of ML/TF/PF Risks
- Sub-Committee for Technical Compliance
- Sub-Committee of Companies Registrars
- Sub-Committee for Supervisory Authorities
- Sub-Committee for Money Laundering Crimes Investigative Authorities
- Sub-Committee for Combatting the Financing of Terrorism and the Financing of Illegal Organizations and the Financing of Proliferation
- Sub-Committee for Managing and Follow-up of International Cooperation Requests Related to Money Laundering
- Sub-Committee on Public-Private Partnership for Counter Money Laundering, Terrorism Financing and Proliferation Financing

[1] https://www.namlctfc.gov.ae/media/jvejlwgq/nra-annual-report-eng-r13.pdf

2.2. DNFBP Supervisory Authorities[1]

- The Ministry of Economy and Tourism (MoET) licenses and regulates accountants and auditors in the mainland UAE and Commercial Free Zones (CFZs). In addition, pursuant to executive decrees following the provisions of the AML/CFT/CPF Law and Decision, MoET is the DNFBP supervisor for auditors and accountants, trust and company service providers, dealers in precious metals and stones, and real estate agents and brokers in the mainland and CFZs.
- The Ministry of Justice (MoJ) is the designated supervisor for law firms and other legal professionals, in accordance with Cabinet Decision No. 54/1 of 2019 passed on 8 January 2019 and amended by Cabinet Decision No. 28/4 of 2019 on 21 April 2019. Recently, legal consultancy has been placed under the supervision of MoJ in accordance with Federal Decree Law No. (34) of 2022. This law has been in effect since January 2, 2023.
- The Dubai Financial Services Authority (DFSA) licenses and supervises the DNFBPs that operate within the DIFC for AML/CFT/CPF compliance.
- The Financial Services Regulatory Authority (FSRA) licenses and supervises the DNFBPs that operate within the ADGM for AML/CFT/CPF compliance.

It is imperative that DNFBPs align their AML/CFT/CPF programmes with the pertinent national legislative and regulatory mandates as well as specific requirements as stipulated by the authority under which they are licensed or operating.

2.3. International Legislative and Regulatory Framework

The AML/CFT/CPF legislative and regulatory framework of the UAE forms part of a broader global framework composed of intergovernmental legislative bodies and international and regional regulatory organisations. Grounded in international treaties and conventions aimed at combating money laundering, terrorism financing and the prevention and suppression of the proliferation of weapons of mass destruction, intergovernmental legislative bodies develop laws at the international level. Participating member countries, including the UAE, are then responsible for transposing these laws into their respective national legal and regulatory framework. In parallel, international and regional regulatory organisations formulate policies and provide recommendations, while also assessing and monitoring the implementation of international regulatory standards related to AML/CFT/CPF by participating member countries.

Among the principal intergovernmental legislative bodies, as well as international and regional regulatory organisations, with which the Government and Competent Authorities of the UAE actively collaborate within the international AML/CFT framework, include:

The United Nations (UN)[2]

The Unite Nations (UN), founded in October 1945, is the international organisation with the largest membership, currently comprising of 193 member states. The UN actively combats money laundering through its Global Programme against Money Laundering (GPML), which is headquartered in Vienna, Austria, and is part of the UN Office of Drugs and Crime (UNODC). The GPML is tasked with assisting member states – through their legal, financial, law enforcement and judicial authorities – to develop robust and comprehensive domestic AML/CFT legal and regulatory frameworks as well as the institutional infrastructures and practitioner skills needed to implement them, in accordance with UN instruments and international standards.

The Financial Action Task Force (FATF)[3]

The Financial Action Task Force (FATF), established in 1989 and based in Paris, France, is an intergovernmental body established that sets international standards for combating money laundering, terrorist financing and proliferation financing. It promotes the effective implementation of legal, regulatory and operational measures to address financial crimes and related threats to the integrity of the global financial system. FATF monitors the implementation of its standards, the 40 FATF Recommendations and 11 Immediate Outcomes, by its members and members of FSRBs. It also ensures the consistent and proper application of the 'FATF Methodology' for assessing technical compliance with FATF Recommendations and the overall effectiveness of national AML/CFT/CPF frameworks.

The Middle East and North Africa Financial Action Task Force (MENAFATF)[4]

[2] https://www.unodc.org/unodc/en/money-laundering/global-programme-against-money-laundering/.html
[3] https://www.fatf-gafi.org/en/the-fatf.html
[4] https://www.menafatf.org/about

MENAFATF, a FATF Style Regional Body (FSRB) headquartered in Bahrain, was established in 2004 to foster cooperation and coordination among countries in the MENA region and implement the FATF's 40 Recommendations and related international standards against money laundering, terrorist financing, and proliferation financing. The UAE is one of the founding members; one of the 14 Arab nations that agreed to establish MENAFATF.

The Egmont Group of Financial Intelligence Units (EGFIU)[5]

In 1995, the Egmont Group of Financial Intelligence Units (Egmont Group) was formed by a number of Financial Intelligence Units (FIUs) working together. The Egmont Group, named after the location of its first meeting in Brussels, serves as a forum for FIUs to enhance their national anti-money laundering and counter-terrorism financing (AML/CFT) programmes. Its main goal is to facilitate the exchange of information and expertise among FIUs to combat money laundering, terrorist financing, and other related crimes.

2.4. AML/CFT/CPF National Strategy Framework

The Higher Committee Overseeing National Strategy on AML/CFT has ratified the UAE's 2024 – 2027 National Strategy for Anti-Money Laundering, Countering Terrorism Financing and Proliferation Financing which reflects the nation's commitment to upholding the highest international standards in the fight against financial crime and structured around 11 strategic goals, each supported by targeted legislative and regulatory reforms with key focus on risk-based compliance, effectiveness and sustainability. The strategic goals place emphasis on the following primary pillars:

- Strengthening the nation's understanding of risk and promoting the application of risk-based mitigation measures
- Continuously updating the legal and regulatory framework to address emerging risks and uphold transparency and rule of law.
- Enhancing the risk-based supervision of AML, CFT and CPF obligations across the private sector
- Strengthening domestic and international cooperation and information exchange between government agencies, private sector stakeholders and international stakeholders
- Leveraging financial intelligence and data analytics to enhance capabilities for detection, investigation and disruption of illicit financial activities with the support of centralized monitoring systems and adequate technical and human resources

The achievement of the UAE's strategic objectives for AML/CFT/CPF is dependent on several key aspects, one of which includes the critical role DNFBPs play as key enablers. Operating in sectors that are particularly vulnerable to misuse for illicit activity, DNFBPs, as gatekeepers, must ensure that sector-relevant drivers of success for strengthening the overall AML/CFT/CPF framework, such as those listed below, are effectively implemented and embedded into their business practices and reinforced through risk-based compliance.

- Heightened risk awareness among DNFBPs of both the general ML/TF/PF threats facing the UAE and the sector-specific risks they encounter, as informed by the National Risk Assessment (NRA), sectoral risk assessments, internal risk assessments, typologies and other reports coupled with a clear understanding of their statutory obligations in managing and mitigating those risks.
- Strengthened compliance with AML/CFT/CPF obligations as prescribed in the applicable legal and regulatory frameworks, tailored to the specific risks and characteristics of DNFBP activities.
- Effective coordination between DNFBPs, their supervisory authorities, the Financial Intelligence Unit (FIU), law enforcement, and other competent authorities to support risk mitigation and enforcement efforts.

3. Highlights of Key Provisions Affecting DNFBPs

The AML/CFT/CPF Law and the Executive Regulations contain numerous provisions outlining the obligations and responsibilities of regulated DNFBP entities, as well as their senior management and employees. This section highlights key provisions of immediate relevance to DNFBPs. The sole responsibility to adhere to all provisions of the Law, Decision, and all applicable regulatory notices, rulings and circulars issued by the relevant authorities.

[5] https://egmontgroup.org/about/

3.1. Summary of Minimum Statutory Obligations of Regulated Entities

The AML/CFT/CPF Law and the Executive Regulations set out the minimum statutory obligations of regulated entities as follows:

- To identify, understand, manage, assess, document, and continuously update money laundering, terrorism financing and proliferation financing risks within their business scope, taking into consideration the risk-based approach, while retaining the risk assessment study and related information, and providing the same to the relevant Supervisory Authority upon request.
- To define the scope of and take necessary due diligence measures
- To appoint a compliance officer, with relevant qualification and expertise and in line with the requirements of the relevant Supervisory Authority to execute the stipulated duties
- To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation
- To put in place indicators to identify suspicious transactions
- To report suspicious activity and cooperate with Competent Authorities
- To promptly apply directives of the Executive Office for Control and Non-Proliferation (EOCN) or any other Competent Authorities concerning Targeted Financial Sanctions (TFS)
- To maintain adequate and updated records

Specific guidance on the above and other provisions of the AML/CFT/CPF Law and the Executive Regulations is provided in subsequent sections.

3.2. Statutory Prohibitions

DNFBPs are prohibited from engaging in the following activities:

- Establishing or maintaining any Business Relationship, conducting any financial or commercial transactions, maintaining any Business Relationship under an anonymous or fictitious name or pseudonym or number.
- Establishing or maintaining a Business Relationship or executing any business dealing without completing risk-based Customer Due Diligence (CDD) measures for any reason.
- Engaging in any capacity with Shell Banks, whether to open accounts with such banks on behalf of Customers or facilitate any banking transactions through such banks for themselves or on behalf of their customers.
- Invoking banking, professional, or contractual secrecy as pretext for refusing and/or failing to meet statutory reporting obligation to the relevant authorities

3.3. Confidentiality and Data Protection

DNFBPs 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 10, Suspicious Transaction Reporting). In reporting their suspicions, they must maintain confidentiality regarding 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 DNFBP 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 DNFBPs, or their managers or employees, permitted to inform a customer or the representative of a Business Relationship, or any other third party either directly or indirectly, of the intention to report or that a report has been made, nor disclose any information or data contained in the report or that an investigation is being conducted in that regard is known as the prohibition against "tipping off" and applies not only to the act of reporting a suspicious transaction but also to any related information provided to the FIU or information being requested by the FIU. The prohibition against "tipping off" is subject to enforcement measures; violations of this prohibition result in sanctions (see Section 5, Overview of Applicable Sanctions for AML/CFT/CPF Violations).

Except for the exemption noted below, DNFBPs 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 for the reporting to the authorities. (see Section 5, Overview of Applicable Sanctions for AML/CFT/CPF Violations).

Under specific circumstances, the AML/CFT/CPF Law and the Executive Regulations provide an exemption to the statutory reporting obligation on the grounds of professional secrecy for DNFBPs that are "*lawyers, notary publics, other legal stakeholders and independent legal auditors*" who have obtained the information during the course of advising or defending their customers against legal or

judicial proceedings. For further guidance, see Section 10.6, Specific Exemptions from the Reporting Requirement.

3.4. Protection against Liability for Reporting Persons

The AML/CFT/CPF Law and the Executive Regulations provide DNFBPs, 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 occurred.

4. Key Concepts

4.1. Money Laundering (ML)

Money laundering refers to the process by which individuals disguise the illicit origin of criminal proceeds in order to make them appear as derived from legitimate sources. These funds can then be used to conduct either lawful or unlawful activities. The process typically involves efforts to obscure the origin, ownership, and intended use of the illicit funds, effectively concealing their true source. This definition also extends to funds intended for use in the financing of terrorism or other criminal acts.

When substantial profits are generated from criminal conduct, those involved often attempt to utilize the proceeds without attracting attention to the underlying illegal activity. To do so, they may seek to alter the form of the funds or move the money to jurisdictions they believe are less likely to raise suspicion.

Under *Article (2)* of the AML/CFT/CPF Law, *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, therefore.

Furthermore, the crime of Money Laundering is considered an independent crime. The punishment of the perpetrator for the Predicate Offence shall not prevent his punishment for the crime of Money Laundering, and proving the illicit source of the proceeds should not constitute a prerequisite to sentencing the perpetrator of the Predicate Offence.

4.1.1. Funds

The AML/CFT/CPF Law defines "funds" broadly as assets of any kind, whether tangible or intangible, movable or immovable, including national and foreign currencies, documents or instruments evidencing ownership or associated rights, in any form, electronic, or digital form or any interest, profits or income originating or earned from these assets. This includes, but is not limited to:

1. Bank or financial accounts, including virtual or crypto assets.
2. Financial instruments or securities such as shares, bonds, notes, commercial paper, promissory notes, IOUs, share warrants, options, land rights, or other transferable securities and bearer negotiable instruments.
3. Contracts, loans, title deeds, claims, insurance policies, or assignments thereof
4. Intellectual property, including patents and trademarks, as well as royalties, licences, or associated rights.
5. Physical assets, such as commodities, land, precious metals or stones, vehicles, vessels, works of art, or any items used as payment-in-kind.

4.1.2. Stages of Money Laundering

Money laundering involves a series of complex transactions; however, it usually progresses through three distinct stages: placement, layering, and integration.

- Placement: This is the initial stage where illicit proceeds are introduced into the financial system, for example, by depositing small amounts of cash into numerous accounts or using the funds to buy foreign currency.
- Layering: At this stage, the funds are distanced from their illegal origin through multiple layers of transactions, often involving various financial institutions across different countries.

- Integration: This final stage involves reintroducing the funds into the economy as legitimate money, such as by purchasing luxury items, services, or making several types of investments to give the proceeds an appearance of legitimacy.

4.1.2.1. Placement

In this phase, criminals attempt to introduce illicit funds or the Proceeds of Crime into the financial system using a variety of techniques or typologies. Criminals tend to exploit DNFBPs in taking advantage of cash intensiveness of pertinent sectors to obscure the origin of funds.

Common placement typologies[6] include:

- Blending illegal funds with legitimate business revenue, such as placing cash from illegal narcotics sales into cash-intensive, locally owned businesses (e.g., jewellery shops, car dealerships)
- Breaking up large sums into smaller transactions and depositing them into numerous bank accounts to avoid attention or reporting requirements
- Purchasing of foreign exchange or buying traveller's cheques using illegal funds
- Depositing illicit funds into accounts via cheques or credit cards
- Purchasing high-value goods using cash
- Repayment of legitimate loans using laundered cash

4.1.2.2. Layering

Once illicit funds enter the financial system, the next step involves obscuring their origin through complex layers of financial transactions. In this stage, the criminal aims to break any audit trail, often leveraging complex financial transactions and movement of funds through multiple accounts, jurisdictions, or legal entities to obscure the source of funds.

Common layering typologies[6] include:

- Concealing beneficial ownership using front persons or layered corporate structures.
- Moving funds between countries or institutions to avoid trails
- Using offshore businesses / trusts to relocate funds in countries with limited transparency
- Using unlicensed remittance systems (informal value transfer systems) to avoid regulatory scrutiny
- Manipulating invoices, under/over-invoicing, or falsifying documentation to move value (i.e. trade-based money laundering)
- Avoiding financial instruments by trading goods directly i.e. commodity exchange / barter (e.g. exchanging drugs for gold)
- Moving value using crypto assets through unregulated platforms. DNFBPs must consider FATF's guidance on risk-based approaches to virtual assets and virtual asset service providers.
- Using new payment technologies such as mobile money or fintech services to layer transactions anonymously
- Investing in insurance products such as life insurance, which allow for cash-out features for layering purposes.

4.1.2.3. Integration

This stage involves the reintroduction of laundered funds into the legitimate economy. At this point, the objective is to make funds appear legally acquired and usable for legitimate purposes or new illicit acts.

Common layering typologies[6] include:

- Investing in high-value goods or services such as the purchasing of art, luxury vehicles, jewellery, or other expensive items through legal channels
- Acquiring property to store value or generate rental income.
- Investing in legitimate businesses to comingle funds
- Buying shares in companies, including those established or managed by DNFBPs (e.g., accountants or lawyers)
- Establishing trusts, foundations and/or nominees to hold assets through such intermediaries with the aim of obscuring ownership

[6] The UAE Financial Intelligence Unit (FIU) releases reports on trends and typologies which is an analysis based on the information extracted from the suspicious transaction reports (STRs) filed by reporting entities. This is a particularly useful resource for DNFBPs for understanding the prevalent typologies of ML/TF/PF crimes as well as getting information on the latest trends on these crimes in the State. This report is released on the FIU's goAML platform for STR reporting and therefore, is accessible to registered users of goAML.

- Utilizing foreign bank accounts to move funds in other jurisdictions and avoid local controls
- Raising, moving, or disguising terrorist funds through charitable entities (Non-Profit Organizations – NPOs)
- Engaging "specialist" facilitators (lawyers, accountants) to assist in legitimizing illicit funds

4.1.3. Predicate Offence

The AML/CFT/CPF Law defines a Predicate Offence as "*any act constituting a felony or misdemeanour 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*."

By definition, a Predicate Offence is a felony or misdemeanour punishable within the UAE, regardless of whether it occurs domestically or abroad, as long as the act is criminalized and punishable in both the UAE and the country where it was committed.

FATF has designated 21 (twenty-one) major categories comprising many individual predicate offenses. All these categories have been criminalized under the UAE's legislative framework. However, supervised entities should note that this categorization is not exhaustive; rather, it serves as a convenient classification. Under the UAE AML/CFT/CPF Law, any crime, whether felony or misdemeanour, which is not explicitly listed may still qualify as a predicate offence for money laundering.

#	Predicate Offence Category	Description
1	Participation in an organised criminal group and racketeering	Involvement in a structured group committing serious crimes for financial or other benefits.
2	Terrorism, including terrorist financing	Acts intended to cause terror or violence and the financing of such acts.
3	Trafficking in human beings and migrant smuggling	Illicit trade and exploitation of persons, including forced labour and smuggling of migrants.
4	Sexual exploitation, including sexual exploitation of children	Exploitation of individuals, especially minors, for sexual purposes.
5	Illicit trafficking in narcotic drugs and psychotropic substances	Illegal production, distribution, and sale of controlled substances.
6	Illicit arms trafficking	Illegal trade, transfer, or possession of firearms and weapons.
7	Illicit trafficking in stolen and other goods	Trafficking of stolen property, goods obtained by criminal means, or other illegal goods.
8	Corruption and bribery	Abuse of entrusted power for private gain, including offering or receiving bribes.
9	Fraud	Deceptive acts intended to result in financial or personal gain unlawfully.
10	Counterfeiting currency	Producing or distributing counterfeit money or similar instruments.
11	Counterfeiting and piracy of products	Unauthorized copying or imitation of products protected by intellectual property rights.
12	Environmental crime	Serious crimes harming the environment, including illegal dumping or trafficking of endangered species.
13	Murder, grievous bodily injury	Homicide and severe bodily harm caused intentionally.
14	Kidnapping, illegal restraint and hostage-taking	Abduction or unlawful detention for ransom or leverage.
15	Robbery or theft	Taking property by force, threat, or unlawful means without consent.
16	Smuggling	Illegal import or export of goods or persons, bypassing customs, or other controls.
17	Extortion	Obtaining property or money through coercion or threats.
18	Forgery	Falsification of documents or signatures to deceive or cause loss.
19	Piracy	Armed robbery or criminal violence at sea or on aircraft.
20	Tax crimes (related to direct taxes and indirect taxes)	Wilful tax evasion involving direct or indirect taxes, committed with intent to defraud tax authorities.

#	Predicate Offence Category	Description
21	Insider trading and market manipulation	Illicit use of confidential information or manipulation of financial markets for gain.

4.2. Terrorist Financing (TF)

The AML/CFT/CPF 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
- 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.

While money laundering is characterized as a circular process wherein the illicit funds that are laundered ultimately end up with the criminal who generated it, terrorist financing is characterized as a linear process wherein funds may not return to the initial source and are utilized to propagate / support terrorist groups and activities.

4.2.1. Stages of Terrorist Financing

The means and strategies deployed by terrorists / terrorist groups to obtain the financial support required to undertake criminal activities endangers both domestic and global security. Such financial support can be derived from a wide range of sources, both legal (such as income from legitimate businesses and non-profits) and illegal (such as drug trafficking, smuggling of weapons, kidnapping for ransom etc.).

Like money laundering, terrorist financing occurs in stages:

4.2.1.1. Raise

The first stage involves raising the funds intended for a terrorist or terror organization that may originate from a variety of sources. Typical sources of financial support include direct donations by individuals and organizations, the use of charities and non-profit organizations, and funds derived from criminal activities. However, as mentioned above, funds may be sourced from legitimate businesses as well.

4.2.1.2. Store

The second stage involves bundling the funds raised to make it easier to manage. Funds can be 'stored' through bank accounts, prepaid cards and high-value commodities such as precious metals and stones, art and antiquities, cryptocurrencies, etc., until the use of these funds are determined and planned for.

4.2.1.3. Move

The third stage involves moving the stored funds for the purpose of concealing the initial placement of funds. The mechanism through which the funds are moved naturally relates to the store. Typical mechanisms include transfers through banking channels, money services businesses, informal remittance networks, transfers to other wallets (in the case of cryptocurrencies), smuggling high-value commodities such as gold, etc.

4.2.1.4. Use

The last stage involves the utilization of funds wherein payments are made for terrorism related activities such as purchase of weapons, materials, equipment, coverage of costs such as overheads, media, messaging, training and salaries. Funds may also be used to support foreign terrorists, pay and organize for travel services etc.

MENAFATF's 2019 report on the assessment of the global threat posed by the financing of terrorism states that "*the number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve … 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 generally 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."

Accordingly, it is imperative that DNFBPs take into account several risk factors when assessing their exposure to the risk of terrorist financing, including those related to geography, customer type channels, products and services (see Section 8.3.2.2, Risk Factors).

4.3. Proliferation Financing (PF)

The AML/CFT/CPF Law classifies Proliferation Financing as a criminal offence. As with the Financing of Terrorism, Proliferation Financing is not subject to the statute of limitations and is subject to severe criminal penalties.

The AML/CFT/CPF Law defines Proliferation as *the illicit and unauthorized trade, as regulated under the applicable legislation in the [UAE], 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 [AML/CFT/CPF] Law*. It further explains Weapons of Mass Destruction (WMD) to mean *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*.

The term WMD Proliferations refers to the manufacturing, acquiring, possessing, developing, exporting, trans-shipping, brokering, transporting, transferring, stockpiling or using nuclear, chemical or biological weapons, along with their delivery systems and related materials (inclusive of dual-use technologies and goods that may be misused). Proliferation Financing (PF), on the other hand, involves the act of raising, moving, or providing funds, assets or other economic resources, or financing, in whole or in part, to individuals or entities in support of activities related to 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).

4.3.1. Stages of Proliferation Financing

Understanding the stages of proliferation financing is critical to identifying how funds and resources are generated, concealed, moved and ultimately used to support illicit development or spread of weapons of mass destruction.

There are 3 stages of proliferation financing:

4.3.1.1. Fund Raising (Acquisition Phase)

During this stage proliferators obtain the financial resources required to support WMD programs, either through illicit activities such trade-based money laundering and other criminal proceeds, or state-sponsored mechanisms.

4.3.1.2. Funds Concealments (Layering / Obfuscation)

During this stage, funds are routed through complex and opaque channers to evade detection by financial institutions and authorities. The use of front companies, shell entities or nominees are often involved to disguise true beneficial owner and obscure the source of funds.

4.3.1.3. Procurement (Utilization Phase)

During this stage the concealed funds are used to acquire dual-use materials, technologies and services required for the development of WMD. Reliance on falsified shipping documents, fraudulent end-use certificates and sophisticated logistics networks deigned to bypass controls and move goods covertly are frequently relied upon during this stage of proliferation financing.

4.3.2. Vulnerabilities Related to Proliferation Financing

Criminals often resort to shell and front companies which are viewed as being ideal vehicles to conduct illicit activities and conceal their true identities. As per FATF's *Concealment of Beneficial Ownership* report published in 2018[7], shell and front companies are defined as follows:

[7] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Egmont-Concealment-beneficial-ownership-Executive-summary.pdf

- 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.

Furthermore, proliferators tend to exploit complex ownership structure in order to disguise their proliferation activities. FATF has highlighted that, designated persons and entities, along with individuals or entities acting on their behalf, often obscure their beneficial ownership through opaque legal structures, complex arrangements and nominee shareholders. Proliferations have similarly been identified operating through intricate ownership networks, including shell and front companies based in multiple jurisdictions to channel funds to designated persons or entities for the financing of WMD-related programs or procurement of dual-use or proliferation-sensitive goods8.

Similarly, the real estate sector can be infiltrated by criminals seeking to obscure the origin of funds, beneficial ownership or support proliferation-related activities by exploiting vulnerabilities of legal persons where they may use shell companies to hide beneficial ownership or multi-jurisdictional corporate vehicles such as trusts or foundations to invest in high-value properties allowing the storing and movement of large sums of funds under the cover of legitimate investment.

Transactions methods may also be exploited such as high-value cash transactions, prevalent mostly in REAB and DPMS sectors. Such transactions pose significant risk due to challenges in tracing origin of funds, thereby facilitating introduction of illicit funds into the financial system by proliferators with relative ease, particularly in absence of strong compliance frameworks.

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[9]

In order to manage and mitigate such associated risks, it is critical to undertake CDD and risk-based EDD measures. It is imperative that DNFBPs identify and verify the identity of beneficial owners of legal entity customers, including the lowering of ownership percentage thresholds on a risk-sensitive and conduct sanctions screening or adverse news checks. Additionally, it is imperative that appropriate measures are taken to identify and further verify the source of funds on a risk-sensitive basis. Understanding the purpose and nature of transactions and applying enhanced scrutiny on complex or unusual transaction patterns that may indicate PF activity is critical to identifying and mitigating PF related risk. Where the trade of high-value goods is involved, i.e. PMS, trade routes, particularly those lined to high-risk or sanctioned jurisdictions (e.g. DPRK), trade documentation, and supply chain due diligence must be undertaken.

Common red flags to look out for include, but are not limited to:

- Customer activity does not match business profile, or end-user information does not match the customer's declared business.
- Customer provides vague, incomplete, or inconsistent information and resists providing additional details.
- Originator or beneficiary is resident in a high-risk proliferation jurisdiction (e.g., DPRK, Iran).
- Transaction involves possible shell companies (low capital, no real operations, red-flag structural features).
- Links between representatives of companies involved in the transaction (same owners/management indicating circular transactions or concealment).
- Ownership structures involving multi-layer companies or jurisdictions known for opacity.
- Wire instructions or payments coming from or going to entities not listed in the original documentation.
- Declared value of goods/transactions inconsistent with supporting financial or commercial documentation (under/over-valuation).
- Inconsistencies in names, addresses, companies, beneficiaries, or destinations across documents.

[8] https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf.coredownload.pdf

[9] https://rulebook.centralbank.ae/en/rulebook/329-dealers-precious-metals-and-stones

- Attempts to mask transaction purpose or counterparties through fragmented or unusual documentation flows.
- Use of cryptocurrencies or digital assets to avoid conventional financial tracing.
- Indicators of crypto-related obfuscation, such as mining-linked funds, mixers, or unclear wallet ownership.

5. Overview of Applicable Sanctions for AML/CFT/CPF Violations[10]

The AML/CFT/CPF Law imposes allows for the following sanctions against any DNFBPs, their managers or their employees for non-compliance to provisions of applicable legislations. The following table outlines the specific sanctions for various violations, including failures to report suspicious activity, breaches of international obligations, and involvement in money laundering, terrorist financing, or related offenses:

#	Offence	Applicable Sanction
1	Money Laundering (Basic Offence)	Temporary imprisonment (up to 10 years) and a fine of no less than AED 100,000 and no more than AED 5,000,000, or either of these two penalties.
2	Aggravated Money Laundering (e.g., abuse of authority, through an NPO, organised crime group, recidivism)	Temporary imprisonment and a fine of no less than AED 300,000 and no more than AED 10,000,000.
3	Financing of Terrorism	Life imprisonment or temporary imprisonment of no less than 10 years, and a fine of no less than AED 300,000 and no more than AED 10,000,000.
4	Using Proceeds for the Financing of Terrorism	Life imprisonment or temporary imprisonment of no less than 10 years, and a fine of no less than AED 300,000 and no more than AED 10,000,000.
5	Proliferation Financing (Providing, collecting, transferring, or making funds/assets available for WMD proliferation or to designated persons/entities)	Temporary imprisonment and a fine of no less than AED 300,000 and no more than AED 10,000,000. Aggravated penalties may apply where linked to designated persons or sanctions evasion.
6	Violation of UN Security Council Implementation Instructions (Chapter VII – Terrorism & Proliferation) including failure to freeze without delay	Imprisonment or a fine of no less than AED 50,000 and no more than AED 5,000,000.
7	Violation of Article (15) Obligations (Internal controls, risk assessment, reporting obligations) if committed intentionally or by gross negligence	Imprisonment and a fine of no less than AED 100,000 and no more than AED 1,000,000, or either of these two penalties.
8	Failure to Declare / Withholding / Providing Incorrect Information (Cross-border declaration obligations)	Imprisonment and a fine, or either of the two penalties. The Court may also order confiscation of seized funds without prejudice to the rights of bona fide third parties.
9	Tipping Off (Notifying or warning a person of an STR/SAR or investigation)	Imprisonment for no less than 6 months and a fine of no less than AED 100,000 and no more than AED 500,000, or either of these two penalties.
10	General Violation of Other Provisions of the Law (where no specific penalty is prescribed)	Imprisonment or a fine of no less than AED 10,000 and no more than AED 100,000.

[10] The sanctions detailed here are based on the AML/CFT/CPF Decree Law. Additional regulations, resolutions, or amendments issued by competent authorities supplementing the AML/CFT/CPF Law may also apply.

#	Offence	Applicable Sanction
11	Corporate (Legal Person) Liability	Criminal fine which may reach up to AED 100,000,000 depending on the offence. The Court may also order confiscation, suspension of activities, closure of premises, dissolution of the legal person, and publication of the judgment. Natural persons remain individually liable.

6. Risk Assessments

Risk Assessments that are conducted at national and sectoral levels are key to gaining comprehensive understanding of existing and evolving threats, vulnerabilities and risks related to money laundering (ML), terrorist financing (TF) and proliferation financing (PF), particularly those that are sector-specific, to allow for:

- Alignment in risk identification through updated internal business-wide risk assessments conducted by DNFBPs.
- Effective implementation of risk-based mitigation measures through the adjustment/update of the AML/CFT/CPF framework of DNFBPs in line with specific vulnerabilities and risks identified.
- Adherence to statutory obligations as set out in applicable laws and regulations thereby enhancing confidence during supervisory inspections and reducing the likelihood of enforcement measures.
- Reinforcement of UAE's commitment to combating ML/TF/PF crimes, ensuring adherence to global standards

DNFBPs are obliged to take into account findings of the UAE National Risk Assessments (NRA) and Sectoral Risk Assessment (SRA) in enhancing their AML/CFT/CPF programme. Doing so allows for the implementation of proportionate and risk-based controls to effectively mitigate ML/TF/PF risks such as targeted due diligence measures and improved transaction monitoring. The alignment of NRA and SRA findings with internal policies and procedures not only strengthens DNFBPs' ability to detect and prevent financial crime but also ensures compliance with regulatory obligations and further supports national efforts to combat money laundering, terrorist financing, and proliferation financing.

It is imperative that DNFBPs remain vigilant and implement strengthened due diligence and monitoring measures to effectively address the evolving and multi-faceted nature of ML/TF/PF risks. Irrespective of the assessed risk levels of each individual DNFBP sector in the NRA and SRA, all DNFBPs are mandated to apply proportional, risk-based measures by (non-exhaustive):

- Reviewing risk assessments, understanding and evaluating findings, and determining its relevance to the DNFBP's operations and risk profile.
- Updating the DNFBP's internal risk assessment methodology to reflect the latest risk assessment factors and ensure appropriate risk levels are applied.
- Implementing appropriate mitigating controls and maintaining documentation on how these controls address identified risks.

Part II Compliance Administration

7. Governance

A successful AML/CFT/CPF programme should be established on a robust governance framework and a compliance culture that is integrated throughout all tiers of the entity. The designated non-financial business or profession (DNFBP) are required to guarantee that their governance structure is appropriate for its objectives, sensitive to risks, and explicitly aligned with the stipulations of the AML/CFT/CPF Law and Decisions and international standards.

The governance framework must include, at the very least, the following essential components:

- Accountability and Oversight: DNFBPs are required to create distinct lines of accountability and allocate AML/CFT/CPF responsibilities throughout the entity. This includes appointing a qualified Compliance Officer who possesses adequate knowledge, authority, independence, and direct access to senior management or the board. Continuous oversight must be exercised over all personnel and business units whose operations could potentially expose the entity to risks associated with money laundering, terrorist financing or proliferation financing (ML/TF/PF).
- Board and Senior Management Involvement: Senior management, along with the board of directors or the equivalent governing body when relevant, must be kept regularly updated on significant developments related to AML/CFT/CPF. This includes compliance initiatives, internal shortcomings, submitted Suspicious Transaction Reports (STRs), audit results, and the corrective measures implemented. Furthermore, senior management is responsible for approving the DNFBP's AML/CFT/CPF policies and procedures, approving the DNFBP's Business Risk Assessment (BRA), ensuring that the Compliance Officer and the AML/CFT/CPF function receive sufficient resources (human, technical, or financial) to effectively perform their responsibilities.
- Effective Internal Reporting: DNFBPs are required to establish internal reporting systems that guarantee prompt and precise reporting mechanism regarding the status of the AML/CFT/CPF programme. This includes, but is not limited to, data on monitored transactions, alerts generated by the system, ongoing investigations, and details about the filings of Suspicious Transaction Reports (STRs).
- Ongoing Monitoring and Quality Assurance: Governance frameworks must include mechanisms for regular testing, quality assurance reviews, and independent audits of the AML/CFT/CPF programme. These controls help assess the effectiveness of implementation and ensure continuous improvement.
- Group-Wide Consistency and Oversight: DNFBPs belonging to a corporate group or an international network are required to ensure the consistent application of AML/CFT/CPF policies and controls across the entire group. This includes the sharing of compliance information and the supervision of foreign branches or subsidiaries. Additionally, the Compliance Officer must possess adequate oversight regarding the design and implementation of controls at the group level.
- Escalation Mechanisms: In situations where the Compliance Officer detects inappropriate influence, interference, or threats to their independency, it is imperative that they report the issue to the appropriate Supervisory Authority via formal channels, in line with national rules and regulations.

DNFBPs are expected to demonstrate a governance culture that supports proactive risk identification, promotes accountability, and allocates adequate resources for the AML/CFT/CPF programme. Additional guidance on these requirements is set out in the subsections that follow.

7.1. Compliance Officer

The Compliance Officer (CO), also referred to as the Money Laundering Reporting Officer (MLRO), plays a central role in ensuring the effectiveness of a DNFBPs AML/CFT/CPF compliance programme. The MLRO must be appointed at a management level and empowered with the authority, independence, and resources necessary to discharge duties effectively. The function must remain independent from operational and revenue-generating roles such as customer onboarding, transaction processing, product delivery, or other business execution functions to the extent practicable. Where dual roles may be unavoidable considering the size and nature of the DNFBP entity, adequate controls should be put in place which include, but are not limited to, establishing clear reporting lines, oversight by senior management / board and segregation of duties in high-risk processes. Furthermore, the Compliance Officer must have unrestricted access to data, systems, and decision-making forums relevant to AML/CFT/CPF risk management.

7.1.1. Appointment and Approval

In accordance with the AML/CFT/CPF laws and Executive Regulations, DNFBPs are required to appoint a qualified Compliance Officer to oversee the implementation and ongoing effectiveness of their AML/CFT/CPF programme. The appointment must receive the prior written approval of the relevant Supervisory Authority. The Compliance Officer (CO) should be appointed at a management level and granted the necessary authority, independence, and resources to fulfil their responsibilities. The Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Decision specifies that the CO executes duties "under his or her own responsibility," highlighting the necessity for independent judgment and freedom from inappropriate influence.

In selecting the suitable candidate, DNFBPs are required to perform a fit and proper evaluation of the individual's qualifications, background, and integrity. This process involves confirming the candidate's experience in AML/CFT/CPF, their professional reputation, and ensuring there are no criminal or regulatory infractions. If necessary, an Alternate or Deputy CO/MLRO should also be designated, subjected to the same rigorous examination, to maintain compliance continuity in the primary MLRO absence.

DNFBPs are advised to have the role of the CO devoid of any conflicts of interest that may arise between:

- The DNFBP, its staff (which includes the CO), or any person directly or indirectly linked to the entity, and its customers.
- The CO and senior management, which encompasses the Board of Directors or owners.

To maintain objectivity and safeguard the entity against possible ML/TF/PF exploitation, the Compliance Officer (CO) must occupy a role of adequate seniority and autonomy to carry out their functions effectively, including exercising independent judgment and escalating matters to Senior management / board where business decisions may give rise to ML/TF/PF risks or other compliance concerns. Should the CO face inappropriate pressure or interference, they are required to report these concerns to the appropriate Supervisory Authority through official means.

The Compliance Officer (CO) must possess direct and unrestricted access to senior management and/or the board and should actively participate in internal committees or forums that impact business strategy, product offerings, or AML/CFT/CPF risk exposure. This involvement includes discussions regarding:

- Modifications in customer segments, markets, or products.
- The selection and adjustment of transaction monitoring or sanctions screening systems.
- Approval of new vendors or outsourcing arrangements.
- Organizational or governance changes that influence AML/CFT/CPF compliance.

When assessing the competencies, qualifications, and reporting lines for a Compliance Officer (CO), DNFBPs should consider a range of factors, including the organisation's exposure to ML/TF/PF risks—particularly as identified in risk assessments (NRA/SRA). Consideration should also be given to the size, complexity, and nature of the business, as well as the governance framework and the effectiveness of internal controls. Additionally, DNFBPs should ensure that the appointed CO can fulfil the specific responsibilities of the role, which include oversight of the AML/CFT/CPF framework, internal reporting processes, the filing of suspicious transaction / activity reports (STRs/SARs), communication with regulatory authorities, and the implementation of remedial actions.

When deemed necessary, DNFBPs are advised to seek guidance from their Supervisory Authority or professional associations in establishing the suitable qualifications and governance frameworks for their Compliance Officer.

Where DNFBPs cannot appoint a suitably qualified and independent CO internally, the appointment of a third-party Compliance Officer may be permitted under the following conditions:

- The appointed third-party CO must have the necessary qualifications, experience, and understanding of the DNFBP's business model, risk profile, and regulatory mandates.
- DNFBPs are required to perform a fit and proper evaluation of the individual's qualifications, background, and integrity. This process involves confirming the individual's experience in AML/CFT/CPF, professional reputation along with ensuring there are no criminal associations or regulatory infractions.
- DNFBPs must ensure CO independence from operational and revenue-generating roles.
- DNFBPs must ensure that the third-party CO has unrestricted access to all relevant information, records, systems, and staff required to discharge their compliance responsibilities effectively.

- The ultimate accountability for compliance remains with the DNFBP's Senior management and board. Appointment of a third-party CO does not absolve the DNFBP of its regulatory obligations
- Contractual agreements must be clearly and comprehensively drafted to outline the third-party CO's responsibilities, scope of work, reporting lines, and confidentiality requirements.

DNFBPs must periodically review the performance of the third-party CO to ensure continued adequacy, effectiveness, and alignment with regulatory requirements.

7.1.2. Responsibilities of the Compliance Officer

The Compliance Officer (CO), also known as the Money Laundering Reporting Officer (MLRO), plays a critical role in ensuring the DNFBPs adherence to the UAE's AML/CFT/CPF legal and regulatory framework. Appointed at a management level, the CO must act independently and carry out their duties with professional diligence. The CO's responsibilities must be thoroughly documented, approved by senior management, and periodically assessed to guarantee ongoing conformity with the entity's risk profile and legal requirements. Responsibilities fall under the following key categories:

ML/TF/PF Reporting and Cooperation with Authorities

The Compliance Officer is tasked with the review, analysis, and submission of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs). The CO acts as the main liaison for the Financial Intelligence Unit (FIU) and the Supervisory Authority and is required to fully cooperate with all requests for information, audits, or inquiries.

The CO holds ultimate responsibility for identifying and escalating activities that may be associated with money laundering, terrorism financing, or the funding of illegal organizations. All STRs must be filed in a timely, complete, and accurate fashion, and the confidentiality of these reports must be rigorously maintained. Tipping-off constitutes a criminal offense under the AML/CFT/CPF Law. No individual, including senior management, is permitted to interfere with or influence the CO's decision to submit a report.

AML/CFT/CPF Programme Oversight

The Compliance Officer (CO) must guarantee the adequacy, effectiveness, and execution of the Designated Non-Financial Businesses and Professions (DNFBP) Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT/CPF) framework. This includes:

- Oversight of the AML/CFT/CPF Business Risk Assessment.
- Assessment and upkeep of the DNFBPs policies, controls, and procedures concerning Customer Due Diligence (CDD), record-keeping, transaction monitoring, sanctions screening, AML/CFT/CPF training.
- Oversight of regulatory compliance, detection of deficiencies, and reporting of breaches or risk exposures to senior management.
- Ensuring the execution of corrective measures and following up on any feedback, observations, or findings provided by Supervisory Authorities.
- Guaranteeing the quality and precision of data submitted in obligatory AML/CFT/CPF returns and supervisory interactions.
- Filing of all applicable reports to the applicable authority (STRs/SARs/CNMRs/PNMRs/DPMSRs/REARs)

In instances where any component of the AML/CFT/CPF programme is delegated or involves third-party systems (such as screening tools or consultants), the CO retains responsibility for oversight, performance monitoring, and ensuring adherence to regulatory requirements.

Internal Reporting and Escalation

The Compliance Officer (CO) is tasked with the duty of consistently providing updates to senior management and/or the Board of Directors or Owners regarding the status of AML/CFT/CPF compliance. Reports should include, at a minimum:

- The quantity and nature of Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs) submitted.
- Essential compliance metrics along with any violations of the DNFBP risk appetite.
- Progress on remediation efforts for previously identified gaps or deficiencies.
- Alterations in Money Laundering (ML), Financing of Terrorism (FT), and Proliferation Financing (PF) risk exposures and the corresponding control measures.
- All regulatory reporting and any information request from Authorities

- All regulatory updates

Should the CO perceive that undue influence, or pressure is being applied that jeopardizes their independence, it is imperative that they promptly report the issue to the Supervisory Authority through official channels.

Training and Compliance Culture

The CO plays a central role in ensuring that the DNFBPs AML/CFT/CPF training and awareness programmes are robust, up to date, and aligned with emerging risks. This includes oversight of the design and delivery of training tailored to the institution's risk profile, sectoral characteristics, and staff roles. Training should encompass not only regulatory obligations and internal policies, but also practical guidance on recognising and escalating suspicious activities.

Record-Keeping and Audit

The CO must ensure that the DNFBP complies with all record-keeping requirements under the AML/CFT/CPF Law and Executive Regulations, including maintaining customer files, risk assessments, internal reports, and STRs for at least five years. The CO should support internal or independent audits of the AML/CFT/CPF framework and ensure that all findings are addressed through documented remediation plans.

7.1.3. Qualifications of the Compliance Officer

DNFBPs are required to ensure that the designated Compliance Officer (CO) or Money Laundering Reporting Officer (MLRO) has the appropriate qualifications, experience, and skills to fulfil their duties independently and effectively. The CO must function at a management level and hold a sufficiently senior position to impact decisions, question behaviours, and raise risks without facing undue pressure or conflicts of interest.

In evaluating the appropriateness of a candidate for the CO/MLRO role, DNFBPs should perform a fit-and-proper assessment that considers the following criteria, at a minimum:

Knowledge and Competence

- Demonstrated understanding of UAE AML/CFT/CPF laws, Executive Regulations, cabinet decisions, Supervisory Authority guidance, and FATF Recommendations.
- Familiarity with typologies, red flags, and methods of money laundering, terrorist financing, and proliferation financing.
- Competence in overseeing risk-based compliance programmes, STR processes, and internal controls.

Professional Experience

- Practical experience in compliance, AML/CFT/CPF, internal audit, legal, or risk management roles, particularly within the same or comparable industry.
- Experience working with Supervisory Authorities and the UAE Financial Intelligence Unit (FIU), especially in regulatory communication and reporting obligations.

Organisational Positioning

- The Compliance Officer (CO) should be situated at a level that guarantees unobstructed access to senior management, the Board (or its equivalent), as well as to all essential data, systems, and personnel needed to carry out their responsibilities.
- In accordance with the size, nature, and risk profile of the DNFBP, the CO may receive support from a suitably qualified third-party compliance service provider, provided such delegation does not exempt the DNFBP from fulfilling its statutory AML/CFT/CPF obligations. The support received from the qualifies third-party compliance service provider should be governed by stringent oversight and proper controls of standards by the DNFBP.

Personal and Ethical Attributes

- High integrity, sound judgment, and ethical behaviour.
- Ability to operate autonomously and without any conflicts of interest.
- Strong leadership, analytical and communication skills to influence internal stakeholders and ensure compliance effectiveness.

Continuous Development

DNFBPs are required to ensure that their Compliance Officers (COs) consistently keep abreast of the latest developments in ML/TF/PF risks, regulatory changes, and best practices in compliance. This

continuous development should encompass active involvement in both internal and external training programmes, regulatory discussions, and pertinent industry forums or sector-specific activities, inclusive of outreach programs organized by relevant Authorities.

Moreover, when DNFBPs utilize third-party consultants or vendors to assist with any component of the AML/CFT/CPF program, the CO remains fully accountable for comprehending, validating, and supervising the sufficiency and effectiveness of those external solutions.

DNFBPs must maintain records of the qualification assessments and background verification of appointed individuals as the Compliance Officer and notify the relevant Supervisory Authority of any changes to the role or reporting lines.

7.2. Staff Training and Screening

An effective AML/CFT/CPF program relies on the skills, integrity, and awareness of the personnel within a DNFBP. Therefore, it is essential for DNFBPs to create explicit policies, procedures, and controls regarding staff screening and training. Such measures facilitate the effective execution of ML/TF/PF risk mitigation and empower employees to exercise sound judgment when identifying and addressing suspicious transactions.

Employees are required to comprehend the ML/TF/PF risks that the DNFBP faces, as well as how to implement internal controls within their respective roles. Considering the dynamic nature of criminal typologies, it is essential for employees to remain updated on the emerging ML/TF/PF risks continuously.

When applicable, these measures should also encompass foreign branches and subsidiaries.

DNFBPs must guarantee that the screening and training of staff are risk based and customized according to the size, nature, and complexity of their operations. This includes, but is not limited to:

- Screening new employees
- Continuously evaluating AML/CFT/CPF proficiency and recognizing individual training requirements
- Designing and delivering tailored AML/CFT/CPF training based on role-specific requirements and ML/TF/PF risk exposure.

A successful and effective training program must cover, at a minimum:

- Relevant AML/CFT/CPF laws, regulations, and supervisory expectations.
- Internal policies, procedures, and control measures aimed at risk mitigation.
- ML/TF/PF typologies and red flags pertinent to the DNFBPs business model.
- Case studies-based learning and practical escalation scenarios.
- Process for raising internal STRs/SARs to the Compliance Officer, in keeping with "Tipping Off" requirements.
- PF-specific training covering, at a minimum, dual-use goods, front-company patterns, high-risk jurisdictions, PF-related red flags, reporting obligations.

AML/CFT/CPF training must be delivered to all pertinent personnel within the DNFBP, which includes frontline and customer-facing employees, specialized AML/CFT/CPF compliance teams, as well as senior management and board members. This guarantees that every tier of the entity is prepared to facilitate effective governance, oversight, and the execution of strong AML/CFT/CPF controls.

When developing a training framework, several factors must be taken into consideration, including but not limited to:

- The UAE NRA and relevant sectoral or thematic risk assessments
- The complexity of the business, its products, customer demographics, and delivery methods.
- The quality, frequency, and delivery format of training sessions
- The sufficiency of both internal and external training resources
- Mechanisms for monitoring to evaluate the effectiveness of training and the outcomes of learning

Ultimately, the Compliance Officer is responsible for overseeing the effectiveness of these measures, ensuring that all staff remain well-informed, and that training supports a culture of compliance across all levels of the entity.

7.3. Group Oversight

Where a DNFBP operates as part of a group or owns majority-controlled subsidiaries, it is required to implement a comprehensive and group-wide AML/CFT/CPF programme that is consistently applied

across all its branches and subsidiaries, whether located within or outside the UAE. This requirement applies irrespective of whether the DNFBP is part of a local, regional, or international financial group.

The AML/CFT/CPF programme must include a uniformed standards for all branches and subsidiaries for:

- Risk assessment and mitigation measures
- Policies and procedures for customer due diligence (CDD), record keeping, transaction monitoring, and suspicious transaction reporting (STR)
- Internal controls and compliance oversight
- Information sharing mechanisms between all branches
- Staff screening and training protocols and procedures

To ensure the effectiveness of group-level compliance, DNFBPs must also:

- Appoint a qualified and independent CO/MLRO with oversight of all domestic and foreign operations
- Establish clear channels for timely and confidential reporting of AML/CFT/CPF issues from foreign branches and subsidiaries to head office compliance functions
- Maintain the ability to monitor and assess the adequacy and effectiveness of foreign operations AML/CFT/CPF controls on an ongoing basis

Where a foreign branch or subsidiary operates in a jurisdiction with less stringent AML/CFT/CPF requirements than those mandated by UAE law, DNFBPs must ensure—to the extent permitted by local law—that the UAE's standards are adopted. If this is not possible due to host country legal restrictions, the DNFBP must implement additional risk-mitigating controls and immediately inform its UAE Supervisory Authority. Examples of additional measures include but are not limited to:

- Conducting gap analyses comparing local AML/CFT/CPF requirements with UAE standards
- Setting up formal compliance protocols with foreign branches or subsidiaries to ensure consistent implementation
- Restricting customer onboarding or product access until adequate CDD standards are met
- Limiting reliance on third-party CDD conducted abroad unless appropriately verified and certified
- Applying enhanced due diligence (EDD) measures for higher-risk jurisdictions
- Including group entities in centralized compliance reporting, transaction monitoring, and system alerts review
- Regularly training foreign-based staff on UAE compliance expectations

In all instances, DNFBPs are obligated to keep accurate records of any control failures, legal limitations, or operational shortcomings experienced in their foreign branches or subsidiaries. If substantial gaps, legal barriers, or significant ML/TF/PF risk exposures are discovered, these must be communicated to the appropriate Supervisory Authority promptly and transparently.

Additionally, DNFBPs must adhere to any further supervisory measures that may be enforced consequently, which could involve suggestions to reorganize their operations or, if necessary, to withdraw from high-risk foreign markets where AML/CFT/CPF compliance cannot be sufficiently guaranteed.

7.4. Independent Audit Function

A robust and independent audit function is an essential element of a comprehensive AML/CFT/CPF governance framework. DNFBPs are mandated to create an effective audit function to evaluate and assess the sufficiency and efficacy of their internal policies, controls, and procedures in relation to the prevention of money laundering, financing of terrorism, and the funding of illegal organizations.

This function is crucial for pinpointing vulnerabilities and facilitating ongoing enhancements within the AML/CFT/CPF compliance program. The audit function should be properly organized and adequately staffed with individuals who have the necessary expertise, experience, and comprehension of ML/TF/PF risks, and the function should be tailored to the nature, scale, and complexity of the DNFBPs operations.

DNFBPs are required to guarantee that audit arrangements— whether internal or external—maintain genuine independence from compliance and operational functions, ensuring they are devoid of any conflicts of interest.

Although larger DNFBPs might have their own internal audit functions, smaller or resource-limited DNFBPs may opt to hire qualified external auditors. In these instances, DNFBPs are still responsible for verifying that the external auditors possess the necessary competence, are regulated by the relevant authorities, and are subject to adequate internal oversight and coordination.

The engagement of third-party audit services must be formalized through written contracts, and DNFBPs should ensure that the requirements for confidentiality, data protection, and the scope of the audit are explicitly defined and upheld.

Audit activities must be carried out on a regular basis and should be a fundamental component of the organisation's governance and risk management framework. The frequency and thoroughness of audits ought to be established using a risk-based methodology, considering the following factors:

- The overall ML/TF/PF risk exposure of the DNFBP, as indicated by the UAE National Risk Assessment (NRA) and any other relevant sectoral risk assessments
- The nature, size, and geographical scope of the entity
- Insights and feedback received from supervisory authorities' inspections, including noted deficiencies and administrative measures
- Internal occurrences (for instance, significant modifications in operations, products, or customer demographics)
- The results and findings of the DNFBPs internal ML/TF/PF risk assessment

The independent audit's scope must encompass, at a minimum, the following areas:

- An assessment of the design and operational effectiveness of AML/CFT/CPF related policies, procedures, and systems, ensuring their compliance with UAE AML/CFT/CPF legal and regulatory standards.
- An evaluation of the adequacy of staff training, which includes the quality of the materials, frequency of training sessions, attendance of staff, and mechanisms for escalating non-compliance.
- A review of outsourcing arrangements concerning AML/CFT/CPF functions, which involves assessing the qualifications of third-party personnel, terms of contracts, monitoring processes, and the overall risk profile of the service provider.
- A review of transaction monitoring and case management systems, focusing on alert management, the quality of investigations, and the escalation procedures for suspicious activities.
- An assessment of the effectiveness of remediation plans resulting from prior audit findings, supervisory reviews, or internal control evaluations.
- An evaluation of the adequacy of record-keeping practices in accordance with AML/CFT/CPF regulations, as well as the entity's capability to provide information promptly to Competent Authorities.

All audit findings must be officially recorded and communicated to senior management and the board (or an equivalent governance body). Audit reports should encompass clearly articulated observations, gap analysis, risk ratings, timelines for remediation, and designated responsibilities for follow-up.

In instances where significant deficiencies are detected, DNFBPs are required to notify their Supervisory Authority, particularly when risks cannot be mitigated within an acceptable timeframe.

The audit function must function independently of the CO/MLRO and report directly to the highest level of governance within the DNFBP (for example, the Board of Directors or Owners), and when necessary, DNFBPs should establish audit committees or similar oversight entities to ensure appropriate governance and follow-up.

7.5. Senior Management Responsibilities

An effective and robust AML/CFT/CPF framework requires a strong and visible leadership from the highest levels. Senior management—and, when relevant, the board of directors or owners—hold the ultimate responsibility for guaranteeing that the governance structures, systems, and controls of the DNFBP are resilient, risk-oriented, and appropriate for their intended purpose. This includes establishing a suitable risk appetite, promoting a culture of compliance, and ensuring that the AML/CFT/CPF program functions with independence, expertise, and adequate resources.

Senior management is required to show active involvement in the AML/CFT/CPF program and cannot transfer accountability for its effectiveness. Their duties go beyond merely approving policies; they must also include direct oversight, regular evaluations, and prompt actions regarding significant compliance matters.

Key Responsibilities of senior management includes the following:

Governance and Control Environment

- Designate a competent Compliance Officer (CO/MLRO) at the management level, ensuring they possess adequate independence, seniority, and authority to effectively execute their responsibilities and report directly to senior management and/or the Board of Directors.
- Authorize the appointment of a Deputy or Alternate CO/MLRO where applicable, while considering the nature, size, and ML/TF/PF risk profile of the DNFBP.
- Ensure that the CO/MLRO has access to timely information, sufficient human and technological resources, and the authority to supervise AML/CFT/CPF controls, including instances where consultants or external vendors are engaged.
- Appoint an independent auditor / audit function.
- Establish clear lines of accountability, free from undue influence or conflicts of interest, particularly concerning STR/SAR decision-making.

Policy Approval and Risk Appetite

- Authorize and approve the entity's AML/CFT/CPF policy framework, which includes policies for:
  - Risk identification and mitigation
  - Customer Due Diligence (including Enhanced Due Diligence, Simplified Due Diligence, and ongoing monitoring)
  - Indicators of suspicious transactions and reporting procedures
  - Sanctions screening and compliance with targeted financial sanctions
  - Employee screening and AML/CFT/CPF training
  - Recordkeeping and data privacy
- Establish and periodically reassess the entity's risk appetite with respect to ML/TF/PF risks, ensuring it is consistent with the DNFBPs business model and regulatory responsibilities.

Oversight of AML/CFT/CPF Compliance

- Examine and assess the periodic reports from the CO/MLRO, which includes findings, corrective measures, emerging risks, and updates regarding the effectiveness of the AML/CFT/CPF program.
- Authorize or escalate:
  - Business Relationships with High-Risk Customers (including PEPs)
  - Transactions and relationships associated with High-Risk Countries
  - Significant modifications to AML/CFT/CPF systems, controls, and vendor solutions
- Supervise the execution of recommendations derived from independent audits or supervisory inspections.

Implementation of Competent Authority Directives

- Apply directives from the UAE Cabinet, the National Committee, and the Supervisory Authorities related to search, freeze, or unfreeze orders received.
- Ensure compliance with guidance issued regarding High-Risk Jurisdictions and targeted financial sanctions.

Strategic Integration and Continuous Improvement

- Ensure that AML/CFT/CPF controls are integrated into the business strategy and that the Compliance Officer participates in:
  - Product or service development decisions.
  - Market expansion strategies.
  - Third-party selection or system acquisition that has AML/CFT/CPF implications.
- Examine lessons learned from internal incidents or enforcement actions, both at the domestic and global levels, to enhance the program and prevent future occurrences.

Senior management is essential in creating and sustaining a robust AML/CFT/CPF compliance framework. Their continuous dedication, supervision, and proactive involvement are vital for protecting the DNFBP from being exploited for ML/TF/PF related activities. By setting the tone at the top and enabling the CO, senior management guarantees that the entity not only meets regulatory requirements but also plays a significant role in advancing the UAE's wider AML/CFT/CPF goals.

7.6. Managing Compliance Challenges in Resource-Limited DNFBPs

Although the size and operational complexity of a DNFBP can differ, all DNFBPs—irrespective of their structure or personnel—are uniformly required to adhere to the stipulations of Federal Decree-Law No. (10) of 2025 and Cabinet Resolution No. (134) of 2025. Smaller and mid-sized DNFBPs, which

frequently function with limited personnel and resources, may encounter difficulties in segregating responsibilities or forming dedicated compliance teams. Nevertheless, these difficulties do not exempt them from meeting their legal AML/CFT/CPF responsibilities.

In instances where staffing is constrained and a single employee or manager takes on various roles and complete separation of duties is not feasible, DNFBPs are required to ensure that their policies and procedures—especially those pertaining to CDD, the identification and reporting of suspicious transactions, and Sanctions List screening—are thoroughly documented, consistently enforced, and regularly reviewed. Any deviations from these policies or procedures must be explicitly justified based on a risk-based rationale, sanctioned by the appropriate personnel, and accompanied by additional mitigating controls when necessary. All such documentation must be maintained in accordance with statutory record-keeping obligations, and any notable exceptions should be included in the Compliance Officer's periodic reports to the relevant Supervisory Authority.

To compensate for operational limitations, small and mid-sized DNFBPs must strengthen their independent audit arrangements. Where applicable, this may include:

- Incorporating audits of key controls, such as CDD measures, STR procedures, and sanctions screening, into the internal or outsourced audit plan.
- Increasing the frequency and scope of audit reviews, including random sampling, retrospective transaction reviews, or setting lower transaction-value thresholds for review.
- Documenting audit findings and corrective actions and ensuring they are addressed within defined timelines and reviewed by senior management.

When internal resources are inadequate, DNFBPs may engage in the assistance of a qualified third party to aid in compliance or audit activities. Nevertheless, the DNFBP—through its senior management and Compliance Officer—remains completely responsible for the oversight, quality assurance, and regulatory compliance of these services.

Part III ML/TF/PF Risk Assessment

8. Identification and Assessment of ML/TF/PF Risks

8.1. Key Legal Requirements

As per the AML/CFT/CPF Law and Decision, when identifying, assessing and mitigating ML/TF/PF risks, DNFBPs are required to:

- Identify, assess, and understand risks
- Consider relevant risk factors such as customers, countries/geographies, products, services, transactions, and delivery channels
- Document and update risk assessments regularly and make them available to supervisory authorities upon request
- Define the scope of and take necessary due diligence measures
- Develop and implement internal policies, controls, and procedures to manage and mitigate identified risks, with senior management approval, and apply these across majority-owned subsidiaries and affiliates
- Monitor the implementation of internal controls and continuously enhance them as needed
- To immediately implement directives related to UNSC resolutions concerning terrorism financing and WMD proliferation
- Apply Enhanced Due Diligence (EDD) measures when elevated risk is identified, including:
    - Obtaining more customer and beneficial owner information
    - Systematically updating CDD data
    - Identifying the source of funds
    - Enhancing ongoing monitoring and transaction checks
    - Obtaining senior management approval to commence the business relationship
- Apply Simplified Due Diligence (SDD) when low risk is identified and no suspicion exists, including:
    - Updating data based on less frequent intervals
    - Reducing the rate of ongoing monitoring and transaction checks
    - Inferring the purpose of the business relationship from transaction behaviour or business relationship that has been established
- Refrain from applying SDD where a suspicion of crime exists
- Maintain complete and updated records and data for all transactions (local and international) and due diligence measures and provide them promptly to competent authorities upon request

8.2. Risk Based Approach (RBA)

In line with the AML/CFT/CPF Law and its implementing Decision along with international standards, DNFBPs are required to adopt a Risk-Based Approach (RBA) in identifying, assessing, and mitigating ML/TF/PF risks.

As per Article (19) of the AML/CFT/CPF Law, every DNFBPs shall *identify, understand, manage, assess, document, and continuously update the risks of [money laundering, terrorism financing and proliferation financing] within their business scope, taking into consideration the risk-based approach and the multiple aspects of risks as defined by the Executive Regulations of the [AML/CFT/CPF] Law, while retaining the risk assessment study and related information, and providing the same to the Supervisory Authority upon request.*

In identifying, assessing and understanding the ML/TF/PF risks that are commensurate with the size and nature of business of the DNFBP, the Executive Regulations mandates the assessment of "*all the relevant risk factors such as customers, countries or geographic areas; and products, services, transactions and delivery channels, before determining the level of overall risk and the appropriate level of mitigation to be applied*" and *"documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."*

Contrary to a 'one-size fits all' approach, the application of a Risk-Based Approach in identifying, assessing, and mitigating ML/TF/PF risks allows for the efficient and proportionate allocation of resources, application of stronger measures that is commensurate with the risk identified whereby enhanced measures are applied to higher risks scenarios and, where permitted, simplified measures in lower-risk scenarios. Thus, the Risk-Based Approach is not merely a statutory mandate, it is a practical necessity in order to have a robust AML/CFT/CPF program that is adaptive to the evolving risk and regulatory landscape.

While there are limits to any risk-management approach, and no RBA can be considered as completely failsafe; there may be occasions where a DNFBP has taken all reasonable measures to

identify and mitigate ML/TF/PF risks, but it is still used for ML/TF/PF in isolated instances. Nonetheless, it is imperative for DNFBPs to understand that a risk-based approach is not a justification for ignoring certain ML/TF/PF 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 the type of their customers, products and services, transactions, geographic areas and delivery channels, and to be in a position to always apply sufficient AML/CFT/CPF mitigation measures on a risk-appropriate basis.

Conducting an ML/TF/PF business-wide risk assessment can assist DNFBPs in understanding their risk exposure and the areas that should be prioritized in combating ML/TF/PF. It is an essential component to the deployment of a Risk-Based Approach and the foundation of an effective AML/CFT/CPF program. The understanding of national and sectoral level threats, vulnerabilities and risks related to ML/TF/PF primarily stems from the UAE NRA and SRA, in addition to other sources of information as highlighted in Section 8.3.1.3, Risk Factors.

The risk exposure of the DNFBP is assessed on the basis of a variety of inherent risk factors, some of which are related to the nature, size, complexity and operational environment of their businesses, while others are customer or relationship-specific (see Section 8.3.1.3, Risk Factors). With the inherent risks as a basis, the DNFBP can determine the nature and intensity of risk mitigating controls to apply to the inherent risks. The level of inherent ML/TF/PF risks influence the kinds and levels of AML/CFT/CPF resources and mitigation strategies which DNFBPs require to put in place. The assessment of inherent ML/TF/PF 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 DNFBP, additional control measures will need to be implemented to ensure that the level of ML/TF/PF risk is acceptable to the DNFBP.

8.3. Business-wide Risk Assessment (BRA)

The purpose of a Business-wide Risk Assessment (BRA) is to improve the effectiveness of ML/TF/PF risk management, through the identification of inherent ML/TF/PF risks faced by the DNFBP as a whole, determining how these risks are effectively mitigated through internal policies, procedures and mitigating measures, and establishing the residual ML/TF/PF risks and any gaps in the controls that should be addressed. Thus, an effective BRA can allow DNFBPs to identify gaps and opportunities for improvement in their AML/CFT/CPF framework and make informed management decisions about risk appetite, allocation of AML/CFT/CPF resources, and ML/TF/PF risk-mitigation strategies that are appropriately aligned with residual risks.

DNFBPs may utilise a variety of models or methodologies to assess risks, in keeping with the nature and size of their businesses. DNFBPs should decide on both the frequency and methodology of a BRA, including baseline review (which is a critical starting point to ensuring risk awareness and compliance) and (follow-up reviews involving the reassessment and update of risk understanding based on changes or new developments). The BRA methodology should be appropriate to the DNFBPs circumstances, taking into consideration the nature of the inherent and residual ML/TF/PF risks to which it is exposed, as well as the results of the NRA and any Sectoral Risk Assessment.

In cases where DNFBPs engage third-party vendors to undertake risk assessments, caution must be exercised to ensure that the assessment is not treated as a 'black box' exercise. DNFBPs must understand the methodology, data sources, assumptions, and analytical tools used by the vendor, and ensure these are appropriate for their specific business model, customer base, and product and service offerings. DNFBPs must also verify that all relevant risk factors, as specified in section 8.3.1.3, Risk Factors have been properly considered and weighted. The output of a third-party assessment should be critically reviewed by the DNFBP's Senior Management and appropriate controls are to be adapted. DNFBPs are accountable for the adequacy and effectiveness of the risk assessment despite having the exercise outsourced.

In most cases, DNFBPs should consider performing the BRA at least annually; however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. DNFBPs should also decide on policies and procedures related to the periodic review of their BRA methodology, taking into consideration changes in internal or external factors. These decisions should be documented, approved by senior management, and communicated to appropriate levels of the entity.

As part of the model or methodology, DNFBPs should consider including in their ML/TF/PF 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 BRA will be the classification of identified risks into various categories, such as high, medium, low, or some combination of those categories such as medium-high, medium-low. Such classifications may assist DNFBPs to prioritise their ML/TF/PF risk exposures more effectively, so that they may determine the appropriate types and levels of AML/CFT/CPF resources needed and adopt and apply reasonable and risk-proportionate mitigation measures.

In order to have an effective risk management framework, it is imperative that DNFBPs differentiate between a Customer Risk Assessment (CRA) and a Business-Wide Risk Assessment (BRA). While both assessments are essential components of a comprehensive framework, they serve different purposes. A CRA focuses on evaluating the risk that individual or corporate customers present in relation to ML/TF/PF and includes the identification of high-risk customers coupled with a subsequent adjustment of monitoring and due diligence procedures to mitigate associated risks. This involves analysing the customer's characteristics, behaviours, transaction patterns, and geographic elements to assess the likelihood of involvement in financial crimes. This assessment helps determine the appropriate level of due diligence and monitoring required, especially during customer onboarding and periodic reviews. On the other hand, a BRA focuses on assessing the DNFBP's overall risk of exposure to ML/TF/PF at an entity level by taking into consideration a wide range of internal and external factors that may impact the DNFBP's overall risk management framework. DNFBPs should refer to the *CRA Guideline* issued by MOET for detailed guidance.

8.3.1. Risk Assessment Methodology and Documentation

A well-documented assessment of the identified inherent risk factors (see Section 8.3.1.3, Risk Factors) is fundamental to the adoption and effective application of reasonable and proportionate ML/TF/PF risk-mitigation measures. Thus, the result of such an ML/TF/PF business risk assessment allows for a systematic categorisation and prioritization of inherent and residual ML/TF/PF risks, which in turn allows DNFBPs to determine the types and appropriate levels of AML/CFT/CPF resources needed for mitigation purposes.

An effective ML/TF/PF business risk assessment is not necessarily a complex one. The principle of a risk-based approach means that DNFBPs' risk assessments should be commensurate with the nature and size of their businesses. DNFBPs with smaller or less complex business models may have simpler risk assessments than those of with larger or more complex business models, which may require more sophisticated risk assessments.

8.3.1.1. Risk Assessment Methodology

The Executive Regulations oblige DNFBPs to document their risk assessment operations. DNFBPs may utilise a variety of models or methodologies in assessing their ML/TF/PF risk. DNFBPs 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 DNFBPs management approved AML/CFT/CPF risk appetite and strategy.
- Takes into consideration input from relevant internal sources, including input and views from the designated AML/CFT/CPF compliance officer and other relevant units like risk management and internal control.
- Takes into consideration relevant information (such as ML/TF/PF trends and sectoral risks) from external sources, including the NRA or any Sectoral 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/TF/PF risks and determining their timing and impact on the organisation.
- Considers whether the AML/CFT/CPF 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/CPF 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.

8.3.1.2. Documentation and Updating

a) Documentation

DNFBPs are obliged to document their ML/TF/PF business risk assessment, including methodology, analysis, and supporting data, and to make them available to Supervisory Authorities upon request. DNFBPs should incorporate into their documentation, the information used to conduct the ML/TF/PF business risk assessment in order to demonstrate the effectiveness of their risk assessment processes. Examples of such information include, but are not limited to:

- Entity's overall risk policies (for example, risk appetite statement, customer onboarding policy, and others, where applicable).
- ML/TF/PF risk assessment model, methodology and procedures, including such information as organisational 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/CPF compliance officer.
- Details of the inherent and residual risk factor analysis that constitutes the risk assessment

The documentation measures taken by DNFBPs should be reasonable and commensurate with the nature and size of their businesses.

Senior Management must formally certify that the BRA undertaken by the entity is an accurate reflection of its risk exposure, is supported by appropriate mitigation measures and is readily available for review by the Supervisory Authority.

b) Updating

DNFBPs are obliged to keep their ML/TF/PF business risk assessment up to date on an ongoing basis. In fulfilling this obligation, they should review and evaluate their ML/TF/PF risk assessment processes, models, and methodologies periodically, in keeping with the nature and size of their businesses. DNFBPs should also update their ML/TF/PF 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, changes in products and services, technological developments, legislative or regulatory developments, or the identification of material new ML/TF/PF threats or risk factors. In this regard, DNFBPs should take into consideration the results of the most recent NRA or any Sectoral 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 Section 13, Useful Links.

8.3.1.3. Risk Factors

A DNFBPs' first step in conducting a BRA is to identify, assess and understand the inherent ML/TF/PF risks (i.e., the risks that a DNFBP 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, transactions, delivery channels, geographic locations, and any other risk factors. A proper identification of risk factors is crucial to the effective assessment of ML/TF/PF risk.

Identified risk factors are used for the accurate categorisation of inherent risks, as well as for the application of appropriate mitigation measures. At the entity level, this includes adopting and applying adequate policies, procedures, and controls to business processes. 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 9.3, Customer Due Diligence (CDD) Measures).

The Executive Regulations outline several risk factors which DNFBPs must take into consideration *"pertaining to customers' risks, States or geographical regions, products, services, operations and their implementation channels before identifying the total risk level and the adequate risk reduction measures to be adopted."* DNFBPs may also consider a wide array of additional risk factors, that stem from various sources, such as:

Category	Source	Description
Internal Sources	AML/CFT/CPF Compliance Officer Input	Observations, alerts, and input from the designated compliance officer.
	Internal Audits and Compliance Reviews	Findings from audits and periodic reviews of internal controls.
National Sources	National Risk Assessment (NRA) Results	Assessment of national ML/TF/PF threats, vulnerabilities, and risks.
	Sectoral Risk Assessments (SRA)	Reports on sector-specific risks
	Public-Private Partnership Information Sharing Forums / Roundtables	Typology exercises or joint information exchanges between relevant authorities and private sector.
	Supervisory Guidance / Typology Reports	Guidance, case studies, red flags, strategic analysis reports from relevant authorities.
International Sources	FATF Mutual Evaluation Reports (MERs)	Country-level AML/CFT/CPF effectiveness evaluations.
	FATF / FSRB / Egmont Group, UNODC Publications	Reports focused on global, regional, and sector-specific threats, vulnerabilities, and risks.

In keeping with the ever-evolving nature of ML/TF/PF risks, and to ensure that DNFBPs implement a model for conducting a BRA that is appropriate to the nature and size of their businesses, DNFBPs should continuously update the risk factors which they consider, to reflect new and emerging ML/TF/PF risks and typologies.

A good practice to assess the inherent risk factors, is for DNFBPs 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 DNFBP can determine the inherent risks of a risk factor.

When assessing the inherent risks, a DNFBP 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, a DNFBP 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 regarding some of the major risk factors that should be considered by DNFBPs when conducting the BRA 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 BRA, DNFBPs are reminded that they should take a holistic view when evaluating exposure to these categories of customers.

8.3.1.3.1. Customer Risk

The customer risk factors refer to types or categories of customers or business relationships that posed increased or decreased ML/TF/PF risk exposure. These factors should be assessed when undertaking the DNFBPs business-wide ML/TF/PF risk assessment and reflected in customer-specific risk ratings.

Certain customer types or relationship categories may present inherently higher ML/TF/PF risks and when identifying such categories, DNFBPs should consider the sources mentioned in Section 8.3.1.3, Risk Factors.

DNFBPs should consider the following, among others, when assessing the customer risk factors:

- 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: DNFBPs with small, homogenous customer bases may face different risks from those with larger, more diverse customer bases. Similarly, DNFBPs targeting growing or emerging markets may face different customer risks than those with more established customer bases.
- Maturity of relationships: DNFBPs 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.
- Specific high-risk customer factors that DNFBPs should consider, include:
- Categories of business relationships with complex legal, ownership, or direct or indirect group or network structures, or with less transparency regarding Beneficial Ownership, effective control, or tax residency, may pose different ML/TF/PF 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/TF/PF risks.
- Non-resident entities particularly those with connections to offshore and high-risk jurisdictions.
- Persons 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 whose wealth structure or financial flows are opaque or not well established

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.

8.3.1.3.2. Geographic Risk

DNFBPs should consider geographic ML/TF/PF risk factors both from domestically and cross-border sources. These risks may arise from:

- Locations where the DNFBP has offices, branches and subsidiaries and
- Locations in which the customers reside or conduct their activities.

DNFBPs should consider the following, among others, when assessing the geographic risk factors:

- Regulatory/supervisory framework: Countries with stronger AML/CFT/CPF 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/CPF measures. DNFBPs should monitor these official lists and advisories regularly.
- International Sanctions: DNFBPs should consider whether the countries or jurisdictions they deal with are the subject of international sanctions, such as targeted financial sanctions (TFS) or broader restrictive measures imposed by the United Nations Security Council (UNSC), UAE authorities, Office of Foreign Assets Control (OFAC), European Union (EU) or other relevant bodies that could impact their ML/TF/PF risk exposure and mitigation requirements.
- Reputation: DNFBPs should consider whether the countries or jurisdictions they deal with are associated with higher or lower levels of ML/TF/PF, 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). Sources such as Transparency International, FATF, MENAFATF, Basel AML Index, Global Corruption Indices may support these assessments.
- Combination with customers' inherent risk factors: DNFBPs should consider the countries risk in combination with customers risks, including principal residential or operating locations of customers. For instance, a foreign PEP residing or associated with a high-risk jurisdiction may present significantly higher overall ML/TF/PF risk. Similarly, customer conducting business activities across multiple jurisdictions considered high-risk warrant for a closer assessment.

8.3.1.3.3. Products, Services and Transaction Risk

When assessing the inherent ML/TF/PF risks associated with products, services, and transaction types, a DNFBP should take stock of its lines of business, products and services that are more vulnerable to ML/TF/PF abuse. DNFBPs should assess the inherent ML/TF/PF risks of abuse of the products and services by their customers considering several factors such as their ease for holding and transferring value or their complexity and transparency, links to known ML/TF/PF typologies. Some of the risk factors that DNFBPs should consider, among others, are:

- Typologies: DNFBPs should consider whether the product, service, or transaction type is associated with any established ML/TF/PF typologies or red flags identified by national authorities or international bodies such as, but not limited to, the use of legal structures for asset layering, purchase of real estate with untraceable funds and involvement of complex cross-border fund flows.
- 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, financing of terrorism and/or proliferation financing. DNFBPs 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 DNFBPs to different types and levels of ML/TF/PF 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/TF/PF
- DNFBPs 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/TF/PF risks particularly when the volume and frequency is inconsistent with a customer's profile, value can be easily split or layered to avoid detection.

8.3.1.3.4. Delivery Channel 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/TF/PF risk. Some delivery channels may limit visibility over the customer / business relationship or transaction, thereby increasing the potential for abuse.

When evaluating delivery channel-related risk, DNFBPs 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, reduce the DNFBPs direct oversight or involves third-parties or technologies that involve complicated verification and monitoring. Among others, delivery channels that are potentially high-risk may include customer onboarding or servicing through 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 which can expose DNFBPs to risks arising from inadequate due diligence performed by the third party or limited control over the customer interaction (DNFBPs should ensure that such third parties are supervised and adhere to AML/CFT/CPF obligations); and the use of third-party payment, or other transaction intermediaries that limit transparency or impair transaction monitoring such as external payment processors, virtual assets service providers (VASPs).

8.3.1.3.5. Other Risk Factors

Given the ever-evolving nature of ML/TF/PF 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.

To ensure their risk-based approach remains effective, DNFBPs should monitor their risk environment and ensure that their ML/TF/PF risk assessment and corresponding risk mitigation measures are reviewed and updated in response to regulatory updates, guidance issuance by supervisory authorities, national and sectoral risk assessment results, developments in products, services, delivery models and global publications from international bodies such as FATF, Egmont Group, UNODC, etc. Links to some of these sources may be found in Appendix 11.2.

Examples of some of the types of additional risk factors which DNFBPs may consider in identifying and assessing their ML/TF/PF risk exposure include:

- Novelty/innovation: DNFBPs 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 business may not be as well understood as and may therefore pose a different level of ML/TF/PF 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/TF/PF risk exposure than would more traditional or expected product, service, transaction, or channel types regarding that same type of customer.
- Cyber security/distributed networks: DNFBPs 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 terrorism financing or proliferation financing, 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 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.
- Organisational expansion: new branches, subsidiaries, or affiliates, whether domestically or globally introduces additional ML/TF/PF risk exposure particularly if operations take place in higher-risk jurisdictions.

8.3.2. Assessing New Product and New Technologies Risks

As part of their obligation to update their ML/TF/PF risk assessments on an ongoing basis, the Executive Regulations, in Article (24), specifically requires DNFBPs to *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*. Additionally, DNFBPs *shall assess risks prior to the launch or use of products, practices, or technologies, and shall take appropriate measures to manage and mitigate those risks.*

DNFBPs 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/TF/PF risk assessment and mitigation requirements into their new product, service, channel, or technology development processes.

For assessing the ML/TF/PF risks associated with new products, services, practices, techniques, or technologies, DNFBPs may consider utilising the same or similar risk assessment models or methodologies as those utilised for their ML/TF/PF business risk assessments, updated as necessary for the 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 8.3.2.1, Documentation and Updating).

DNFBPs should be particularly vigilant when assessing the ML/TF/PF risks of the different types of innovations, which may either introduce new vulnerabilities or amplify existing risks such as digital assets and blockchain-based solutions which may entail the use of virtual assets (cryptocurrencies, NFTs, stablecoins) for transactions or investment, adoption of blockchain-based smart contracts, tokenization for settlements, involvement of virtual asset service providers (VASPs) as customers or partners as these allow for anonymity, rapid transaction processing and pose difficulty in tracing beneficial ownership etc. Other innovative methods include the incorporation of artificial intelligence and machine learning in onboarding or monitoring activities inclusive of automated customer interaction and self-service tools where there is minimal human oversight; these may lead to

incomplete or inaccurate data collection, weak document validation and impersonation if appropriate measures are not in place.

Part IV Mitigation of ML/TF/PF Risks

9. Elements of a Solid AML/CFT/CPF Program

An effective and successful AML/CFT/CPF program must be founded on the globally acknowledged three lines of defence framework. These elements, which should be customized to the size, nature, and complexity of the DNFBPs operations, are crucial for reducing the risks associated with money laundering, terrorist financing, and proliferation financing (ML/TF/PF)

- A system of internal policies, procedures and controls, including an ongoing employee training program (first line of defence)
- A designated Compliance Function, led by a competent and knowledgeable CO / MLRO responsible for oversight of the policies, procedures and controls (second line of defence).
- An independent audit function that assesses the overall effectiveness of the AML program (third line of defence)

DNFBPs are required to implement measures that effectively manage and mitigate any ML/TF/PF risks using a risk-based approach (RBA), as prescribed under the AML/CFT/CPF Law and Decision.

9.1. Internal Policies, Controls and Procedures

To support the risk mitigation initiatives, DNFBPs must create a framework of internal policies, controls, and procedures that are in alignment with their risk profile and business model.

Policies

A detailed high-level declaration and statement that establishes the organizational tone and framework for AML/CFT/CPF. These policies must be approved by the entity's senior management.

Procedures

A detailed step by step guide that will clearly translate the policies into actionable items and ensure clear responsibilities are assigned to the relevant stakeholders and staff.

Controls

The internal systems, technologies, and tools employed by DNFBPs to monitor, support, and guarantee the effective execution of their AML/CFT/CPF program in accordance with established parameters, regulatory expectations, and local and international laws and regulations.

In accordance with Article (19) of the UAE AML/CFT/CPF Law and Articles (5) to (20) of Executive Regulations, DNFBPs are mandated to establish and implement comprehensive internal policies, procedures, and controls to effectively manage and mitigate risks associated with ML/TF/PF. These measures must be formulated based on the results of the DNFBPs business-wide ML/TF/PF risk assessment and should be aligned with the nature, size, and complexity of the business operations.

These internal frameworks shall:

- Be documented, approved by senior management, and communicated clearly throughout the entity
- Be applied to all branches, subsidiaries, and affiliates where the DNFBP holds a controlling interest, both within and outside the UAE
- Reflect the conclusions of the UAE NRA, SRA any relevant sectoral risk assessments, and the entity's own ML/TF/PF risk assessment.
- Be subject to regular review, effectiveness testing, and periodic updates in response to changing risk in the market or shifts in regulatory expectations.

To ensure a risk-based and effective implementation, the policies, controls, and procedures must be:

- Reasonable and proportionate to the assessed ML/TF/PF risks
- Integrated into day-to-day operations, encompassing front-line business processes and compliance oversight
- Adapted to reflect the specific customer base, product/service offerings, delivery channels, and geographic footprint of the DNFBP

9.1.1. Technology and Infrastructure Considerations

DNFBPs are required to evaluate the sufficiency of their Information Technology (IT) infrastructure and Management Information Systems (MIS) while developing and executing AML/CFT/CPF controls. This evaluation includes:

- The capability to produce timely and precise risk reports
- Facilitating automated transaction monitoring and customer due diligence systems
- Guaranteeing secure data storage and audit trail functionalities
- Aligning MIS capacity with the scale and intricacy of operations, especially in high-risk or swiftly growing business sectors

Internal AML/CFT/CPF policies and procedures must cover the following functional areas:

- Risk Identification and Assessment: Establishing mechanisms to identify, assess, and document ML/TF/PF risks at a business wide level.
- Customer Due Diligence (CDD): Implementing Customer Due Diligence, which includes Simplified Due Diligence (SDD) and Enhanced Due Diligence (EDD), periodic reviews, and protocols for third-party reliance.
- Monitoring and Suspicious Activity Reporting: Continuous monitoring of customers and transactions, escalation processes, and prompt reporting of suspicious transactions to the Financial Intelligence Unit (FIU).
- AML/CFT/CPF Governance and Training: Assigning compliance responsibilities, ensuring sufficient resources, staff training, and conducting independent internal audits to evaluate the program's effectiveness.
- Record-Keeping: Ensuring the proper retention and accessibility of customer and transactional records in compliance with legal timeframes.

The establishment of such internal systems demonstrates the DNFBPs commitment to fulfilling its AML/CFT/CPF obligations under UAE law and regulations and aligns with key FATF Recommendations.

9.2. Customer Due Diligence (CDD)

A comprehensive CDD program must include the following key elements, in accordance with the UAE AML/CFT/CPF Law and Decision, and in line with FATF Recommendations:

- Customer and Beneficial Owner identification and verification
- Customer risk profiling and risk rating
- Customer acceptance procedures
- Understanding the purpose and intended nature of the business relationship
- Ongoing monitoring of the business relationship
- Investigation and escalation of unusual transactions
- Record-keeping and documentation

These components constitute the basis of a robust AML/CFT/CPF compliance framework. Their implementation allows DNFBPs to recognize and comprehend their customers, evaluate the related ML/TF/PF risks, and enforce suitable controls. An effectively organized CDD program aids in averting the exploitation of DNFBPs for unlawful activities, facilitates the prompt identification of suspicious activities, and showcases adherence to both national legal obligations and international benchmarks.

9.2.1. Risk-Based Application of Customer Due Diligence Measures

DNFBPs are required to apply a risk-based approach to their CDD measures. This means that DNFBPs must assess the risks of money laundering, terrorist financing, and proliferation financing posed by each of their customers and business relationships and tailor the scope, depth, and frequency of CDD measures accordingly. This risk assessment must take into consideration the results of the NRA, SRA and any other relevant risk factors identified through the DNFBPs own ML/TF/PF risk assessments.

DNFBPs are required to apply a risk-based approach to customer due diligence, including:

- Enhanced Due Diligence (EDD): for situations presenting higher risks of money laundering, terrorist financing, or proliferation financing (see Section 9.3.6, Enhanced Due Diligence Measures).
- Simplified Due Diligence (SDD): for lower-risk customers, business relationships, and scenarios where no suspicion of ML/TF/PF is present (see Section 9.3.5, Simplified or Delayed Due Diligence).

DNFBPs must also consider multiple risk factors when determining their customers risk profiles, including but not limited to:

- Geographic risk factors.
- The customer's type, activities, and ownership structure.
- Products, services, transactions, or delivery channels that may present increased risk.

In addition, DNFBPs should also consider the customer's source of funds and wealth, source of funds, the use of complex ownership structures or intermediaries, involvement in cash-intensive activities, reputational concerns such as adverse media or regulatory sanctions, the duration and nature of the business relationship, and any unusual behaviour or transaction patterns that deviate from the customer's expected profile. These factors help ensure a comprehensive assessment of ML/TF/PF risk in line with the UAE AML/CFT/CPF framework and FATF standards and recommendations.

Each customer's ML/TF/PF risk profile is dynamic and must be reviewed and updated regularly to reflect changes in circumstances, new information, or behaviours that may affect their risk levels. DNFBPs are required to increase or decrease the intensity and frequency of CDD measures in line with changes in the assessed risk level.

CDD measures must never be considered a static or one-time exercise. DNFBPs must remain vigilant and apply enhanced scrutiny whenever there are doubts regarding the accuracy or adequacy of the previously established risk categorization or CDD information.

Supervisory authorities shall evaluate the effectiveness of DNFBPs' implementation of a risk-based CDD framework as part of their ongoing supervision and inspection activities.

9.2.2. Assessing Customer and Business Relationship Risk

A customer refers to any individual or entity that either engages in a one-off or occasional financial activity or transaction or establishes an ongoing commercial or financial relationship with the DNFBP.

The accurate assessment of the ML/TF/PF risks associated with a customer or business relationship is fundamental to determining the appropriate level of Customer Due Diligence (CDD) to apply. This assessment forms the basis for customer risk classification and underpins the risk-based approach to AML/CFT compliance.

DNFBPs may adopt different approaches to customers and business relationships risk classifications, depending on the nature, size, and complexity of their operations and customer base. These may include simplified or profile-based approaches for smaller DNFBPs or those with homogenous customer types, generic profiles may be applied for similar categories of customers. For larger or more complex DNFBPs, a scoring system approach or weighted risk scoring models may be adopted which will be based on multiple risk factors (e.g. customer type, jurisdiction, service type, delivery channel).

Regardless of the methodology employed, DNFBPs must ensure that the risk assessment model is comprehensively documented, with a clear explanation of the rationale and the assumptions which it is based on. The methodology must be formally approved by senior management and communicated across all relevant departments within the organisation. In addition, DNFBPs are required to establish and maintain policies and procedures for the periodic review and timely updating of both individual customer risk classifications and the risk assessment framework, particularly in response to changes in internal operations or external risk factors. It is essential that the outcomes of the risk classification process directly inform the application of appropriate customer due diligence measures, whether simplified, standard, or enhanced in full accordance with the risk-based approach and the expectations set forth by UAE regulatory authorities and international standards.

9.2.3. Establishing Customer Risk Profile

DNFBPs are required to establish a customer risk profile that reflects the types and levels of risk associated with each customer. This risk profile enables DNFBPs to compare actual customer activity with expected behaviour, thereby enhancing their ability to detect unusual or potentially suspicious transactions.

For customers that are legal persons or legal arrangements, DNFBPs must identify any natural person owning or controlling 25% or more of the entity. In certain cases, DNFBPs should consider identifying beneficial owners below the 25% threshold mandated by the Executive Regulations. 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. Additionally, DNFBPs may choose to consider identifying beneficial owners below the 25% threshold, in line with their internal policy.

To effectively understand the ownership and control structure, DNFBPs should obtain and incorporate into the risk profile:

- A detailed explanation or company structure chart showing ownership interests of 25% or more, tracing through intermediate entities or nominee stakeholders to the natural persons who ultimately own or control the entity.
- Information on the entity's internal management structure, identifying senior management or persons exercising control over the entity.
- Details of majority-owned or controlled operating subsidiaries, including the nature of their business and their operating locations.

Additionally, DNFBPs must comprehend the intended purpose and nature of the business relationship. This includes gaining a comprehensive understanding of the customer's business activities, ownership structure, and control mechanisms. Depending on the risk profile, DNFBPs are required to perform ongoing due diligence to ensure that transactional activities align with the customer's anticipated behaviour and overall risk characteristics. For customers deemed higher-risk or more complex, DNFBPs are expected to gather and regularly update supplementary information, which includes but is not limited to:

- The projected size, value, and transaction volumes
- The anticipated types, frequency, and purpose of transactions
- Known or expected counterparties, beneficiaries, and third-party intermediaries involved in transactions
- Geographic regions or countries linked to the customer's operations, transactions, or counterparties
- The timing and patterns of the customer's transactional activity
- The customer's source of funds and source of wealth, especially in cases involving high-risk profiles or Politically Exposed Persons (PEPs)

In addition, DNFBPs need to factor in sanctions risk as component of the customer risk profile, which include the determination whether customers or transactions may have links with jurisdictions, individuals or entities that are included in sanction lists (mandatory lists include UNSC and UAE Terrorist Lists; other lists may be considered depending on the DNFBP's internal policy).

Consideration should also be given to the risks of the delivery channel, particularly where the onboarding is not face-to-face, where digital platforms are used, or third-party service providers are involved, which can increase the vulnerability to identity theft, anonymity and other forms of money laundering, terrorist financing, or proliferation financing abuses.

Considerations relating to customer behaviour risk, including but not limited to unusual transaction patterns, reluctance or evasion, high-risk association, unusual requests, post-onboarding / relationship establishment behaviour, should be incorporated into a comprehensive risk-based monitoring framework as part of the DNFBP's RBA and that departures from the expected behaviour of the customer should signal a reassessment of the risk as well as escalation, review or STR where appropriate. Reviews need to be done on a periodic basis commensurate with level of risk of the customer.

For lower-risk customers, DNFBPs may adopt more generic risk profiles to compare actual and expected activity levels, while ensuring these remain sufficient to detect deviations that could indicate ML/TF/PF risks.

9.2.4. Circumstances and Timing for Undertaking CDD Measures

Under normal circumstances, DNFBPs are required to conduct Customer Due Diligence (CDD) measures, including the identification and verification of customers, beneficial owners, beneficiaries, and controlling persons, prior to or at the time of establishing a Business Relationship. Similarly, for customers with whom there is no ongoing Business Relationship, CDD must be completed before the execution of any transaction. DNFBPs must apply a comprehensive risk-based approach to their CDD measures, considering all relevant risk factors such as customer profile, ownership and control structures, delivery channels including remote or non-face-to-face onboarding, and exposure to sanctions risks in accordance with UAE regulations. The timing and scope of CDD measures must ensure full compliance with AML/CFT/CPF legal obligations and international standards. Additional guidance on the application of these requirements, including specific provisions for exceptional circumstances, is set out in the following sub-sections.

9.2.5. Establishment of a Business Relationship

A Business Relationship is formed when a DNFBP agrees to provide services or perform transactions for, at the behest of, or on behalf of, or on direction of a customer, knowing or having reasonable grounds to believe that the relationship is an ongoing and/or periodic in nature, even if it is on a permanent or on temporary basis. The establishment of a Business Relationship initiates the need to apply full CDD according to the ML, TF, and PF risk of the customer.

Such a relationship is deemed to exist when any - but not limited to – of the following actions occur:

- Engaging or agreeing to engage in any kind of dealing, transaction, or activity with the customer on an ongoing or periodic basis, or as a single transaction.
- Carrying out transactions or providing services on behalf of or on the instruction of the customer, including transactions carried out for the benefit of a third party.
- The supply of professional, business or other services under a contract, a power of attorney, an engagement letter or similar document.
- Receiving compensation, including fees, commissions, or any form of remuneration for a service that indicates a continuing relationship.
- Interacting with the customer to establish regulatory, professional or contractual obligations for ongoing monitoring or due diligence.

Irrespective of form or nature of business relationship or transaction, when a business relationship is established, DNFBPs shall carry out CDD measures commensurate with the risk level they have identified for the type of customer designated and the nature and purpose of the business relationship between the entity and the customers. These measures include, but are not limited to:

- Know and verify the identity of the customer, beneficial owner and beneficiary owner and controlling person.
- Understanding the nature and purpose of the business relationship.
- Evaluating the customer's risk according to their profile to establish the correct level of due diligence – simplified, standard, or enhanced.

CDD must also be conducted or updated when:

- There is a suspicion of money laundering or terrorist financing
- There are doubts about the accuracy, completeness, or validity of previously obtained customer identification data.

By conducting CDD measures upon the commencement of a Business Relationship and maintaining the process throughout the life of the Business Relationship, DNFBPs would not only meet the objectives of laws and regulations, as required under the UAE's AML/CFT/CPF regime, but also closely adhere to the risk-based approach principles. The sooner CDD is started the earlier DNFBPs can develop a complete understanding of the identity, including profile of customers and nature of their activities in relation to its risk and will safeguard the entity before any substantial business impact takes place. Documentation and Verification of CDD throughout the Business Relationship allows DNFBPs to monitor changes in customer behaviour, detect emerging risks, and act accordingly to unusually activities and suspicious transactions. This continuous and ongoing process ensures that risk assessments are current and that controls are adjusted to reflect changes in the risk level.

In doing so, DNFBPs can show a commitment to protect against the misuse of their services for money laundering, terrorist financing, or other illicit uses, with the result that they are able to preserve the integrity of their operations and contribute to the wider national and international fight against financial crime.

9.2.6. Occasional Transactions

Occasional Transactions refer to a one-time transactions or short-term transactions undertaken by the DNFBP for a customer without an existing Business Relationship with the entity. While these are not ongoing business relationships, they may still result in DNFBPs being exposed to risks of money laundering or terrorist financing and therefore must be subject to appropriate customer due diligence (CDD) measures under certain circumstances.

Examples of Occasional Transactions may include, but are not limited to:

- The one-time sale or purchase of high-value goods such as precious metals, precious stones, jewellery, or collectible coins.
- Acceptance of a deposit or payment in relation to a single real estate transaction from a buyer with no ongoing relationship with the DNFBP.

- Assisting a customer in a one-time company formation.

DNFBPs are required to undertake CDD measures, including customer identification and verification, in the following situations:

- When the occasional transaction is equal to or exceeds AED 55,000 (or its equivalent in any other currency), whether conducted as a single transaction or as multiple transactions that appear to be linked.
- When there is a suspicion of money laundering, terrorist financing, or proliferation financing, regardless of the value of the transaction
- When there are doubts regarding the accuracy, authenticity, or completeness of identification data previously obtained.

In all applicable cases, DNFBPs must identify and verify the identity of the customer and, where relevant, the beneficial owner(s), beneficiaries, and controlling persons. They are also required to develop an understanding of the nature and purpose of the transaction being conducted. Based on the information obtained and the inherent risk, DNFBPs must apply a risk-based approach to determine the appropriate measures of customer due diligence measures.

Occasional transactions must not be treated as exempt from AML/CFT/CPF obligations simply because they do not involve an ongoing relationship. The same level of vigilance and professional judgment must be exercised as would be expected in the case of Business Relationships, particularly in sectors where the value or anonymity of transactions can mask illicit activity.

9.3. Customer Due Diligence (CDD) Measures

DNFBPs must implement robust and risk-sensitive customer due diligence (CDD) measures in accordance with the customer's money laundering, terrorism financing, and proliferation financing (ML/TF/PF) risks classifications. The level and complexity of CDD deployed should be commensurate with the risk associated to the customer or Business Relationship and should be based on superior principles of a risk-based approach, as prescribed by UAE law and global standards.

As part of the CDD process, DNFBPs must, at a minimum, undertake the following key components:

- Identification and verification of customer and beneficial owner(s), beneficiaries, and controlling persons. Verification should be based on documentation, records, or information from an independent and reliable source.
- Sanctions and adverse media screening of the customer and of all beneficial owners to determine exposure to TFS obligations and to identify possible legal or reputational risks, mainly in a high risks' situation.
- Understanding and knowing the intended purpose and nature of the business relationship. For legal persons and arrangements, this includes a clear understanding of the customer's business activities along with its ownership and control structure.
- Obtaining clarity on the source of funds/wealth.
- Creating a customer risk profile against which real behaviour can be compared, checked, and assessed.
- Continued monitoring of the Business Relationship, through analysis of the transactions occurring during the course of the relationship. This ensures consistency with the customer's known profile and the expected level and type of activity and facilitates the detection of potentially suspicious transactions.
- Adequately documenting accurate and current customer information, especially for high-risk customers. DNFBPs must establish procedures for the periodic review and update of documents, data, and other information collected during the CDD process.

For customers assessed as higher risk, DNFBPs are required to conduct enhanced due diligence (EDD), which may include establishing the source of funds and wealth and applying a stricter verification or monitoring measures.

DNFBPs must also incorporate a documented internal policies, procedures, and controls that reflect a risk-based approach to their CDD procedures. These internal frameworks should be designed while taking into consideration the following:

- The results of the DNFBPs business-wide ML/TF/PF risk assessment
- The timing, sequencing, and conditions under which CDD measures must be applied
- The frequency and triggers for updating CDD information
- The required level of ongoing monitoring based on the customer's risk profile

These internal controls must be proportionate to the size, nature, and complexity of the DNFBPs business. They should be approved by senior management, aligned with the outcomes of the UAE NRA, SRA and any relevant sectoral risk assessments, and communicated clearly across all relevant levels of the organisation.

9.3.1. Customer and Beneficial Owner Identification and Verification of the Identity

The identification and verification of customers (including the Beneficial Owner, beneficiaries and controlling persons) is an essential element of an effective Customer Due Diligence (CDD) process, and a key foundation to a sound AML/CFT/CPF programme. Such measures must be taken prior to entering a Business Relationship or carrying out an occasional transaction, following the risk-based approach and the obligations established in the Executive Regulations as well as Cabinet Resolution No. 58 of 2020 Concerning the Regulation of Procedures Related to Real Beneficiary (the UBO Resolution).

DNFBPs must identify and verify the identity of all natural and legal persons or legal arrangements involved in the relationship or transaction, including any person acting on their behalf. The verification must be based on reliable, independent source documents, data, or information. The extent and method of identification and verification should be determined by the level of risk presented by the customer and be commensurate with the nature and size of the DNFBPs business.

Identification and Verification of Natural Persons

DNFBPs are required to take the following steps in order to acquire and verify at least the following information:

- Personal identification details including full name, nationality, date of birth, place of birth and number of national identification document or passport, country of issue, date of issue and expiry date.
- Proof of residential address, in the form of a utility bill, government issued documents, lease agreement, or an account statement issued by a government regulated financial institution.
- The identification data should include the name, nationality, date of birth and place of birth, and national identification number of a natural person.

When official documents are unavailable, alternative documentation may be accepted where reasonable and supported by a documented risk assessment. Acceptable alternatives may include:

- Letters from reputable employers, educational institutions, or state authorities.
- Documentation proving receipt of government assistance or subsidies.

In such cases, DNFBPs must record the rationale for accepting alternative documents and apply appropriate risk mitigation measures.

Where digital identity systems are used, DNFBPs must ensure the system meets standards of reliability, independence, and security, as outlined in FATF's Guidance on Digital ID (2020).

Identification and Verification of Foreign Nationals

For foreign nationals, DNFBPs must ensure that identification documents are valid and recognized under the laws of the issuing country. In higher-risk scenarios, DNFBPs should authenticate the validity of such documents through means such as:

- Confirmation from the issuing authority or relevant embassy/consulate
- Use of commercial software to validate MRZs (machine-readable zones) or biometric chips

Identification and Verification of Legal Persons and Legal Arrangements

In addition to identifying the legal entity, DNFBPs must identify and verify:

- The Ultimate Beneficial Owner, being the natural persons who have ultimate ownership or control of the legal entity.
- The authorized representative(s) of the customer (including explanation of both authority of signatories, guardians, attorneys or legal representatives, and court appointed or act of court).

Acceptable evidence of authority includes items such as notarized powers of attorney, corporate board resolutions, official registry extracts, and court orders.

Information of legal persons and arrangements to be obtained and verified comprises:

- Official legal name, registration number, date and place of incorporation or establishment.
- Registered address and principal place of business.
- Legal form and ownership structure.

Where nominee shareholding or directorship is identified, DNFBPs must identify and verify both the nominee and ultimate beneficial owner, obtain nominee arrangement documentation, assess the legitimacy and purpose of the nominee structure and apply enhanced scrutiny where opacity or complexity is eminent.

Documentation and Certification

DNFBPs must establish robust procedures for authenticating and certifying customer identification documents. Certification may be performed by:

- DNFBP employees (e.g., certified true copy notation, with name, position, date, and signature).
- Reputable external parties (e.g., legal professionals, notaries public, regulated institutions), including, where applicable, documents certified with an Apostille under The Hague Convention.

Risk-Based Measures and Internal Controls

DNFBPs must apply enhanced measures in higher-risk scenarios, such as politically exposed persons (PEPs), complex legal structures, or cross-border relationships. Conversely, simplified measures may be applied where lower risks are identified.
Internal policies and procedures for CDD should incorporate:

- A "four-eyes" review mechanism for high-risk cases.
- Documentation standards for identity verification.
- Defined escalation procedures where verification cannot be completed.

All identification and verification data must be kept up-to-date, and DNFBPs must conduct periodic reviews to ensure continued compliance, particularly for high-risk customers or where red flags arise during ongoing monitoring.

9.3.2. CDD Measures Concerning Legal Persons and Arrangements

DNFBPs must apply appropriate Customer Due Diligence (CDD) measures to legal persons and legal arrangements, in line with the Executive Regulations and consistent with a risk-based approach. This includes identifying and verifying the identity of the Beneficial Owners, beneficiaries, and other controlling persons before establishing a Business Relationship or carrying out a transaction. The following principles apply when conducting CDD on entities such as:

Legal Persons with Layered Ownership Structures

When the customer is a legal person that is owned or controlled by other legal persons or legal arrangements—such as a subsidiary of a parent company or a structure involving trusts—DNFBPs must:

- Take reasonable steps to identify the natural persons who ultimately own or control the customer through direct or indirect ownership of 25% or more of the shares or voting rights, or through other means of control.
- Look through each layer of ownership and control until natural persons are identified. This may require tracing ownership across multiple entities and jurisdictions.
- Consider cumulative ownership or control across entities that may appear separate but are effectively controlled by the same parties. Even if individual stakes are below 25%, DNFBPs must assess whether common ownership or control meets or exceeds the 25% threshold in the aggregate.

Where no natural person meets the ownership or control threshold, DNFBPs must identify and verify the identity of the natural person(s) holding the position of senior managing official, as per Article (10) of the Executive Regulations.

Legal Arrangements (e.g., Trusts, Foundations)

For customers that are legal arrangements—including trusts and similar structures—DNFBPs must identify and verify the identity of all relevant parties, including *Trustee, Settlor, Trust Protector, Beneficiaries, or classes of Beneficiaries, and the powers and authorities granted* ultimate effective control over the arrangement.

Where a beneficiary is designated by category or class, DNFBPs must obtain sufficient information to satisfy themselves that they can identify the beneficiary at the time of distribution or when the beneficiary exercises vested rights.

If the arrangement allows for contributions from persons other than the initial settlor(s), DNFBPs must take steps to understand the identity and role of those contributors and assess any resulting changes to the Beneficial Ownership structure.

Understanding the Control Structure and Associated Parties

DNFBPs are required to obtain and document information on individuals or entities involved in the management or administration of a legal arrangement. This includes:

- Trustees or equivalent managing persons.
- Service providers such as legal advisors, accountants, tax consultants, investment managers, or directors.
- Intermediaries subject to regulatory supervision.

Such information must be obtained from the trustees or relevant representatives and retained as part of the customer's CDD file. DNFBPs must also apply these same principles to other types of legal arrangements such as foundations, religious institutions, charitable organizations, or membership clubs, ensuring that founders, administrators, and governing persons are identified and verified.

In all cases, DNFBPs must apply a risk-based approach to determine the depth of CDD measures and extent of verification required. Higher-risk structures (e.g., multi-jurisdictional arrangements or opaque control layers) should be subject to Enhanced Due Diligence (EDD). The information gathered must be adequately documented, up-to-date, and made available to competent authorities upon request.

9.3.3. Ongoing Monitoring of the Business Relationship

DNFBPs must conduct ongoing monitoring of business relationships to ensure that the transactions and activities carried out over time are consistent with the customer's risk profile, the nature of their business, and the information obtained through Customer Due Diligence (CDD).

Ongoing monitoring forms a critical part of the risk-based approach to the entity AML/CFT/CPF farmwork and is essential for detecting and reporting suspicious activity.

Principles of Ongoing Monitoring

DNFBPs must implement measures to monitor transactions conducted throughout the course of the relationship and ensure that these transactions are consistent with the customer's known profile, including their business activities, risk level, source of funds, and expected transaction patterns. They must also identify transactions that deviate from expected behaviour and assess whether further inquiry or reporting is required. The frequency and intensity of ongoing monitoring must be proportionate to the level of risk associated with the customer or relationship.

Risk-Based Monitoring and Escalation

DNFBPs shall adopt a risk-based approach (RBA) to decide on the extent and frequency of monitoring. This includes:

- High-risk customers and relationships: Require enhanced monitoring, deeper analysis of transaction purpose and origin, and more frequent reviews of CDD information. Suspicious or abnormal transaction patterns should be investigated and where necessary reported to the FIU.
- Low-risk customers and relationships: May be subject to simple or occasional monitoring, where justified by the customer risk assessment results and in accordance with section 9.3.5 on Simplified or Delayed Due Diligence.

All decisions related to monitoring thresholds and methods should be documented, periodically reviewed and agreed by the senior management.

Monitoring Techniques and Controls

DNFBPs may adopt one or a combination of the following monitoring methodologies, depending on the nature, size, and complexity of their business.

- Threshold-based monitoring: Threshold-based monitoring involves the establishment of predefined monetary values, transaction volumes, or frequencies that, when exceeded, automatically trigger a review or further investigation. Ideally, such monitoring allows DNFBPs to spot what could be unusual or suspicious by establishing where your customer's normal profile (or Type of business) will be. Thresholds should be risk rated to the customer and regularly reviewed to consider changes in the customer's activities, or way of conducting their business.
- Transaction-type monitoring: Transaction-type surveillance is directed at certain types of transactions that are deemed to be inherently higher risk or vulnerable to being abused for ML/TF/PF. Such transactions include, but not limited to, cash-based transactions, money transfers payable to third parties, and cross-border wire transfers. In respect of the interpretation of such parameters including the risk profile of the customer and the circumstances in which transactions are executed, DNFBPs should set rules and alerts based on such types of transaction within its transaction-monitoring system.
- Geographic monitoring: Geographic tracking includes monitoring transactions involving jurisdictions or geographic areas with a higher risk of money laundering, terrorist financing, or other illicit financing. These include jurisdictions against which international sanctions are in force, countries on the Financial Action Task Force's (FATF) list of jurisdictions with strategic AML/CFT/CPF deficiencies, and those jurisdictions with which there is a reputation for high levels of corruption, secrecy, and limited regulatory controls. DNFBPs are to determine the risks of the geographical location where the funds are coming from or going to, the location of the customer, counterparty or beneficiary. These transactions with high-risk countries should be flagged for requiring enhanced due diligence and for justifying what these transactions are for. Geographic tracking should also integrate up-to-date information to consider alterations in international sanction lists or FATF advisories so that risk is as current as possible.
- Customer-based monitoring: Customer-based monitoring is the ongoing scrutiny of transactions for a person or an entity which has been identified as presenting a high ML/TF/PF risk. This includes customers that receive a high-risk rating due to their profession, origin of wealth, corporate ownership structure or earlier detected suspicious activities. This is particularly relevant for those working in high-risk sectors, where exploitation of financial systems is more likely. DNFBPs need to adapt their monitoring procedures to the actual risk associated with each high-risk customer, which requires them to apply enhanced scrutiny to the transactional activity, especially the nature, volume and frequency, and reason of such transaction.

Such approaches allow for more effective identification of suspicious activity and support timely reporting to the relevant authorities when necessary.

Monitoring systems may be automated, semi-automated, or manual. Regardless of the method used, DNFBPs must:

- Document their systems and procedures
- Conduct periodic reviews to ensure the effectiveness of the deployed systems.

- Ensure that senior management approves the systems and that responsibilities for oversight and action are clearly assigned.

Updating CDD Information and Detecting Irregularities

Ongoing monitoring must be supported by periodic reviews of the customer's profile and CDD data. DNFBPs must:

- Update CDD information when new risks or inconsistencies has been identified.
- Reverify the customer identity and beneficial ownership when needed.
- Examine the economic rationale of the transactions that appear to be unusual or not in line with the customer's known profile.

Where necessary, DNFBPs should collect additional information about the transactions or counterparties involved such as legal names, regulatory status, and publicly available records to be able to establish whether the activity is:

- Normal: in line with the customer's usual behaviour.
- Reasonable: Clearly justified and supported by business context and documents in hand.
- Legitimate: Conducted within the legal and regulatory framework applicable to the customer and the counterparty.

Monitoring of Customers and Reporting to the FIU

DNFBPs must report a customer to the Financial Intelligence Unit (FIU) via an STR/SAR once they know, suspect, or have reasonable grounds to suspect that the funds, transaction, or proposed transaction is connected to the commission of a crime or to money laundering or terrorist financing. Prompt reporting, as well as the ability to appropriately monitor post reporting, is necessary to satisfy legal obligations and to protect the DNFBP from becoming embroiled in money laundering.

If a DNFBP reports a Suspicious Transaction Report (STR) on a customer or transaction, then the entity must conduct heightened monitoring of the customer and take risk-based action accordingly. This would also involve a comprehensive review and where necessary, reassessment of the business relationship in all its aspects in order to establish if the business relationship is still with the DNFBP risk appetite. If the review shows that the risk is unacceptable or that the continued Business Relationship could involve the DNFBP in regulatory, legal or reputational trouble, it may be appropriate to limit, suspend or even end the business relationship.

All actions taken following the filing of an STR must be clearly documented in accordance with the requirements set out in the Executive Regulations and the DNFBPs internal policies and procedures. Documentation should include the rationale for continued engagement or termination, any enhanced due diligence measures applied, and records of internal deliberations or approvals.

9.3.4. Reviewing and Updating the Customer Due Diligence Information

Regular review and timely update of Customer Due Diligence (CDD) information is an essential part of any AML/CFT/CPF program. DNFBPs are required to ensure that the CDD records, data, and information for customers and Beneficial Owners is accurate, up to date and maintained during the course of Business Relationship.

Risk-Based Update of CDD Information

DNFBPs shall adopt a risk-based approach (RBA) to determine the frequency, scope, and method of CDD reviews. This includes:

- High-risk customers: CDD information must be reviewed and updated more frequently. The specific review cycle (e.g., every 6 or 12 months) should be defined in internal policies and justified based on the customer's risk classification and on the DNFBP risk appetite.
- Low-risk customers: DNFBPs may conduct less frequent reviews (e.g. every 24 months), if there is no suspicion of Money Laundering, Terrorism Financing, or other financial crimes or any alerted or triggered event which may cause to initiate the review.

These periodic reviews must be documented, approved by management, and aligned with the entity's broader AML/CFT/CPF risk management program.

Event-Driven and Interim Reviews

In addition to scheduled periodic reviews, DNFBPs must conduct interim or event-driven reviews when material changes or risk triggers arise. These include, but are not limited to:

- Discovery of contradictory or outdated CDD information.
- Change in ownership, legal structure, or control of a customer that is a legal person or arrangement.
- New legal or judicial proceedings involving the customer or a Beneficial Owner.
- Adverse media reports or intelligence suggesting involvement in financial crimes.
- Qualified audit opinions or concerns raised by third-party advisors.
- Transactions inconsistent with the customer's known profile, or suggestive of unusual or suspicious activity.

Event driven reviews must assess whether to update the customer's risk rating, escalate to senior management, file a Suspicious Transaction Report (STR), or consider suspending or terminating the relationship.

Scope and Components of the CDD Review:

Each periodic or event driven CDD review should be proportionate to the customer's risk level and may include:

- Verification of identification documents and expiry checks
- Review of the purpose and intended nature of the relationship
- Re-assessment of the source of funds and source of wealth
- Confirmation or revision of the customer's beneficial ownership and control structure
- Examination of the customer's recent transactional activity
- Re-evaluation of the customer's business operations, sector, and jurisdictional exposure

DNFBPs are encouraged to use structured tools, such as risk-based review checklists or workflow templates, to ensure consistency and effectiveness across all CDD updates.

Internal Policies and Procedures

DNFBPs must establish and implement clear internal policies and controls that address:

- The maximum allowed time between reviews as per the customer risk category
- The circumstances that trigger interim reviews
- The level of documentation required for each type of review
- Procedures for escalating findings to Compliance Officers or Senior Management
- The approval processes for PEPs, high-risk customers, or adverse findings
- Guidance on how to remediate incomplete or outdated CDD files

Such policies must be proportionate to the nature and size of the DNFBP and should be reviewed periodically to ensure continued relevance.

Organizational Responsibilities:

DNFBPs should allocate specific roles and responsibilities for the CDD review and update process, including:

- Front-line staff or relationship managers conducting the initial review
- Compliance teams reviewing updates and verifying that they align with AML/CFT/CPF guidelines
- Senior management oversight of CDD decisions, especially for high-risk customers and PEPs
- Internal audit or quality assurance teams performing periodic reviews of CDD update quality
- Recordkeeping teams maintaining logs of review dates, findings, and actions taken (see Section 11, Record Keeping)

Responsibility and accountability should be indicated in the DNFBPs compliance management framework.

9.3.5. Simplified or Delayed Due Diligence Measures

In accordance with the risk-based approach set out in the AML/CFT/CPF Law and Decision, DNFBPs may apply Simplified Due Diligence (SDD) or delay certain aspects of the CDD process in limited circumstances where there is no suspicion of money laundering (ML), terrorist financing (TF), or other criminal activity, and where the risk of ML/TF/PF is demonstrably low. These measures must be proportionate, justified by documented risk assessments, and subject to appropriate controls and oversight.

9.3.5.1. Permissible Conditions

DNFBPs may apply SDD or defer verification of identity under the following conditions:

- Low-Risk Customers or Beneficial Owners: Where, following documented risk analysis, the customer or Beneficial Owner is assessed as posing a low risk of ML/TF/PF, and no suspicion exists, DNFBPs may establish a business relationship prior to completing identity verification. In such cases, DNFBPs must:
    - Obtain basic identification information before onboarding
    - Complete full verification in a timely manner
    - Implement mitigating measures to manage residual risk, such as delayed execution of transaction until verification is finalized
- Listed Companies: DNFBPs are exempt from verifying the identity of shareholders or Beneficial Owners when:
    - The customer or controlling entity is listed on a regulated stock exchange with disclosure requirements equivalent to those in the UAE
    - Appropriate source of ownership information (e.g. stock exchange websites, annual reports, public registers)
    - The DNFBP still verifies the identity and authority of any individual acting on behalf of the customer
- Legal Arrangements with Unnamed Beneficiaries: In cases such as trusts with unnamed or contingent beneficiaries, DNFBPs must:
    - Obtain sufficient information on the class of beneficiaries to enable identification at payout where a DNFBP administers customer funds, assets or arrangements that result in distributions to beneficiaries. Even in cases where DNFBPs provide purely administrate or corporate services (without handling funds) obtaining UBO information is a critical element of CDD.
    - Verify beneficiary identities prior to settlement, payout, or exercise of legal rights in cases where a DNFBP is responsible for administering customer assets or facilitating transactions that benefit third parties. Even in cases where DNFBPs provide purely administrate or corporate services (without handling funds) verifying UBO information is a critical element of CDD.
    - Monitor the relationship for changes that may trigger earlier identification
- Exceptional Operational Constraints: DNFBPs may delay verification in exceptional cases where immediate identification is operationally infeasible, provided:
    - There is no suspicion of ML/TF/PF
    - Justification is documented
    - Verification occurs as soon as practicable and appropriate controls are in place to prevent misuse
- Listed Company Subsidiaries: DNFBPs may rely on the listing status of a parent entity when the customer is a majority-owned subsidiary, provided equivalent transparency requirements are met.

9.3.5.2. Residual Risk Controls

Whenever SDD or delayed CDD has been applied, DNFBPs must implement controls to manage associated risks, including but not limited to:

- Holding or delaying transactions until verification is completed
- Limiting the scope or value of transactions
- Flagging the relationship for enhanced post-verification monitoring

All exceptions must be recorded, justified, and subject to compliance oversight. Risk classifications and decisions to defer verification must be approved by senior management or the CO/MLRO and reviewed periodically.

It is imperative for DNFBPs to understand that SDD does not imply standard CDD is omitted, rather it implies that the same core standard CDD measures such as those prescribed in previous sections (identifying and verifying the customer and beneficial owner, understanding the nature of the

business relationship, and conducting ongoing monitoring) is applied but with reduced intensity or frequency; in a manner that is less intrusive.

9.3.6. Enhanced Due Diligence (EDD) Measures

Enhanced Due Diligence (EDD) measures shall be applied by the DNFBPs in respect of any Customer or Business Relationship determined as presenting a high risk of ML/TF/PF in accordance with the Risk-Based approach established under the Executive Regulations.

Higher-risk EDD is seen as the next level up from straightforward CDD, comprising more detailed scrutiny, a fuller range of information collection and more intense monitoring matched to the perceived level of risk.

Note: While elements of EDD are discussed across various sections of these Guidelines, this section serves as the central reference for EDD obligations.

Applicability of Enhanced Due Diligence

EDD measures are considered mandatory – but not limited to - the following circumstances:

- When a customer or transaction is classified as high risk based on the DNFBPs internal ML/TF/PF risk assessment.
- When a customer falls under specific statutory categories requiring EDD (e.g., Politically Exposed Persons, and customers from high-risk countries).
- When there are doubts about the adequacy, accuracy, or consistency of previously obtained CDD information.
- When red flag indicators of suspicious or unusual transactions are observed.

EDD may also be applied as a precautionary measure when the customer's risk classification is unclear or pending further review.

Core EDD Measures

When applying EDD, DNFBPs must implement the following additional due diligence measures to obtain further assurance about the identity, activities, and legitimacy of the customer:

- More robust identification and verification of the customer and Beneficial Owner(s), including reliance on independent and reliable documentation.
- In-depth understanding of the nature of the customer’s business, the purpose and intended nature of the Business Relationship, and expected account activity.
- Verification of source of funds and source of wealth, including substantiating documents.
- Review of financial records, such as audited financial statements or bank references.
- Collection of supplementary information, such as major counterparties, international exposure, expected transaction volumes, and geographic footprint.
- Higher levels of management approval before the initiation or continuation of a high-risk relationship.
- Increased frequency and scope of transaction monitoring and CDD reviews.
- Verification of the legitimacy of product end-use, identification of supply-chain vulnerabilities and scrutiny of high-risk jurisdictions, dual-use goods or opaque corporate structures, specifically where PF risk is identified.

All such information must be evaluated against the customer’s risk profile and assessed for plausibility and legitimacy.

Practical Risk Factors and Indicators

When assessing whether to apply EDD, DNFBPs should consider the presence of the following non-exhaustive risk factors:

- Customers engaged in cash intensive or high value transactions which are inconsistent with stated business purpose.
- Customers based in or transacting with jurisdictions identified by the FATF as high risk or under increased monitoring.
- Customers using complex legal structures or nominee arrangements without a clear business rationale.
- Transactions inconsistent with the customer’s risk profile, business model, or sector norms.

- Adverse media, litigation, or enforcement history involving the customer or related parties.

Where one or more risk indicators are present, the DNFBP must either apply EDD or justify the decision not to do so, with such justifications retained in accordance with recordkeeping obligations. It is imperative to note that DNFBPs must not engage in transactions which involve anonymity-enhancing technologies, mixers or privacy coins wherein beneficial ownership cannot be determined.

EDD Policy Development and Implementation

DNFBPs should create and maintain, written internal policies, procedures and control mechanisms to address how they will implement EDD. Such mechanisms should:

- Be proportionate to the size, nature, and complexity of the DNFBPs operations.
- Documented on a risk-based approach referring to the firm's ML/TF/PF Business Risk Assessment, UAE National Risk Assessment (NRA) and relevant or Sectoral Risk Assessment.
- The timing, content, and escalation process for applying EDD measures.
- Event driven triggers to review.
- Documented approval from a senior manager should be mandatory for accepting new or retaining existing high-risk Business Relationships.
- Be supported by continued education and awareness raising with relevant staff.

These EDD policies must be documented, periodically reviewed, and subject to internal audit to ensure continued relevance and effectiveness.

The implementation of EDD measures should be monitored by the Compliance Officer and subject to a periodic review by senior management to ensure higher risk business relationships are identified, rated and managed accordingly. DNFBPs should have written policies and procedures that identify the responsibilities for performing a customer risk assessment, seeking approval as required, and the factors to consider in determining the level of due diligence necessary. All EDD conclusions and along with the underlying rationale must be recorded in a comprehensive audit trail to facilitate transparency and accountability. Where the level of risk of ML/TF/PF is assessed as unmitigable, DNFBP should follow formal escalation procedures, including the refusal to enter into, or termination of the business relationship. EDD should be considered as a process, rather than a box ticking exercise, a process that is incorporated into the risk-based approach, both on a rolling basis as new information or new risk factors are identified.

9.3.6.1. Requirements for Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEP) who hold or have held a prominent public function and by virtue of that position can manage public assets and state-owned enterprises. The increased ML/TF/PF risks attributed to PEPs is because they may have access to state funds, procurement systems and decision-making. Therefore, PEPs must always be considered high risk from an AML/CFT/CPF perspective.

Definition and Scope of PEP's

AML/CFT/CPF Law and the Executive Regulations define PEP's as:

Natural persons entrusted with, or have been previously entrusted with, prominent public functions in the [UAE] 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 position.

The definition also includes the following:

- *Immediate family members of the politically exposed person, such as spouses, children and their spouses, and parents.*
- *Persons known to be close associates of the politically exposed person, including:*
    - *Persons having joint beneficial ownership of a legal person or Legal Arrangement, or any other close professional or social relationships with a PEP.*
    - *Persons having sole beneficial ownership of a legal person or Legal Arrangement that*

Identification and Risk Management of PEPs

DNFBPs are required to establish and maintain effective internal systems to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP. These systems must be proportionate to the nature and size of the DNFBPs operations and may include:

- Automated screening tools to check customers and transactions against known PEP databases.
- Manual and digital background checks, which may include:
  - Internet and media searches
  - Subscription or publicly available databases
  - Background investigation services

Identification should occur at onboarding and throughout the business relationship as part of ongoing monitoring. DNFBPs must ensure their screening systems are updated and capable of identifying new or emerging PEP relationships.

Enhanced Measures for PEP

When a PEP is identified, the DNFBP must apply Enhanced Due Diligence measures, including but not limited to:

- Obtaining senior management approval before initiating or continuing a business relationship with the PEP.
- Establishing the source of wealth and source of funds, which must be supported by reliable documentation.
- Assessing the legitimacy of the customer's financial background, including cross-checking professional history and public disclosures.
- Conducting more frequent monitoring of transactions and periodic reviews of the relationship.

These measures also apply where the PEP is a Beneficial Owner, beneficiary, or controlling person.

Ongoing Obligations and Escalation Triggers

Senior management approval must also be obtained in the following situations:

- A non-PEP customer becomes or is identified as a PEP during the course of the relationship.
- A routine or event-driven CDD review identifies changes in the customer's risk profile.
- A material transaction that is unusual or inconsistent with the known profile of the PEP is detected.

Where risk remains high or suspicious activity is detected, a Suspicious Transaction Report (STR) must be considered.

Domestic and Former PEP

For Domestic PEP's and individuals no longer in prominent public functions, DNFBPs are not required to automatically apply full EDD measures. However, they must assess whether the relationship nonetheless presents a high ML/TF risk due to:

- The individual's remaining influence or connections, even if informal.
- The seniority of the previous public function.
- Whether the former and current roles are substantively linked, such as ongoing engagement with government functions or decision-making processes.

Where such risk factors are present, DNFBPs must treat the individual as a high-risk customer and apply EDD measures accordingly. These decisions must be documented and subject to periodic review.

All Politically Exposed Persons (PEP's) should be identified, classified, risk assessed and where applicable the application or exemption of Enhanced Due Diligence (EDD) measures must be thoroughly documented and well justified. This includes documentation of the basis of consideration, decision-making process, and supporting evidence and must be in a form that is maintained with other required records as specified recordkeeping requirements. Such decisions must be formally approved by senior management, with the rationale clearly articulated to ensure transparency and accountability. Furthermore, these categorizations and decisions should be revisited periodically,

taking into consideration any changes to the customer's profile, status or risk position to decide if the PEP consideration and related risk level are still appropriate.

The Compliance Officer is responsible for ensuring the effective implementation and ongoing oversight of the institution's PEP policy. This also involves ensuring the necessary training of all relevant staff in how to identify PEPs, consider risk levels, apply appropriate due diligence and, escalating concerns when necessary. Regular training and awareness programs should be held in order to arm employees with applicable knowledge to identify and manage PEP-related risks, consistent with changes to both regulatory expectations but also internal policies.

9.3.6.2. Requirements for High-Risk Customers or Transactions

Where a customer, Beneficial Owner, or transaction presents a high risk of Money Laundering or Terrorism Financing, DNFBPs must apply Enhanced Due Diligence (EDD) measures commensurate with the nature and severity of the risks identified. These measures form a critical component of the DNFBPs risk-based approach and are aimed at mitigating the exposure of the business to illicit financing.

High-risk customers and transactions are those that exhibit characteristics which may obscure the origin of funds, the identity of the parties involved, or the purpose of the relationship. The Executive Regulations recognises high-risk factors such as:

- Customers from high-risk jurisdictions.
- Non-resident customers lacking recognised forms of identification.
- Complex legal structures or ownership chains.
- Business Relationships or transactions lacking clear economic rationale.
- Cash-intensive operations or dealings with unknown third parties.

Risk-Based Determination and Triggering of EDD

DNFBPs must apply EDD measures when it is based on a documented and evidenced on the results of the risk assessment. EDD should not be implemented by default, rather, it must be triggered by a clear identification of elevated risk factors. High-risk ratings will be derived from the results of both the DNFBPs Business Risk Assessment and customer risk profiling and rating, as well as red flags noted during customer on-boarding, periodic reviews or transactions initiated. Sectoral and geographic risk factors, as referenced from the UAE National Risk Assessment or any applicable Sectoral Risk Assessments should also be taken into consideration when determining customer risk rating.

Where a customer is assessed as high-risk, DNFBPs must evidence the basis on which that assessment was made and the risk characteristics that resulted in the customer being categorised as high risk. Such documentation should then serve as the basis for the application of proportionate EDD measures, which are commensurate with the nature and level of risk identified. The approach must be risk-based and show that the DNFBP is effectively acting in accordance with national AML/CFT/CPF obligations and standards.

EDD for Suspicious, Unusual, or Illogical Circumstances

EDD must also be applied in any - but not limited to - the following scenarios:

- The customer provides illogical reasons for operating in or through the UAE, without a clear business, personal, or professional connection to the country.
- There is a disconnect between the customer's business profile and their stated employment or professional background.
- Transactions are unusual in size, frequency, or counterparties when compared with the customer's known economic activity.
- The transaction or legal structure is more complex than anticipated based upon the individual's levels of education, experience, and understanding of general industry practices.
- The transaction involves counterparties, jurisdictions, or structures that do not align with the stated business model, raising concerns of obfuscation or evasion.

Enhanced Due Diligence Measures

Once a customer or transaction is identified as high-risk, DNFBPs must apply more intensive measures to understand the relationship, transaction, and verify the provided information. These may include:

- Verifying of identity of the Customer and Beneficial Owner from independent and reliable sources, in particular, non-residents and customers with complex structures.
- Understanding the identity and business of the customer, including the customer's business activities, the purpose of the business relationship, the anticipated pattern of transactions.
- Assessing the legitimacy of the customer's financial profile, such as reviewing Vs, corporate records, or other material evidence supporting the stated business model.
- Investigating the customer's legal structure to identify ownership and control, as well as discover the existence of parent entities, trusts or offshore holding companies.
- Cross- referencing information using open-source tools, such as:
    - ✓ Public media searches
    - ✓ Public registries and databases.
    - ✓ Subscription services offering adverse media and sanctions screening.

The information and data should be tested for internal consistency, credibility, and plausibility. Inconsistencies or unverified claims should provoke more inquires or escalations.

9.3.6.3. Requirements for High-Risk Countries

Business Relationships and transactions with countries identified as high-risk by DNFBPs must be subjected to Enhanced Due Diligence (EDD) procedures and where necessary countermeasures. This obligation applies not only to the customers themselves, but also under Beneficial Owners, lead that deal with Legal Persons and Arrangements of these countries. High-risk countries are those:

- Call for Action or Jurisdictions under Increased Monitoring by Financial Acton Task Force (FATF).
- Designated by the UAE National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations (NAMLCFTC).
- Identified by the UAE Regulators or the FIU to have strategic AML/CFT/CPF deficiencies or such that are subject to increased risk.

DNFBPs should have internal systems and controls that help identify, record and report such risks as part of their risk-based approach.

Identification of High-Risk Countries

DNFBPs shall establish and periodically update an inventory of countries classified at high risk from credible and reliable sources. This list would be a vital input to their risk assessment frameworks and would help identify heightened geographic risks during customer due diligence and as part of ongoing monitoring. Primary sources should be listed as public statements and high-risk jurisdiction lists released by the FATF, designations published by the NAMLCFTC, or the any of the notices, circulars, directives issued by the relevant UAE Supervisory Authority or the FIU. In addition, risk indicators as identified in the UAE's NRA, should be included to reflect the national priorities and threat landscape

Supplemental tools such as THE BASSEL AML INDEX, OECD list of non-cooperative tax jurisdictions, and other independent risk indices can be used to increase awareness of risks, however they cannot replace or override lists provided by FATF, UN Security Council or from authorities within the UAE. Such external means should clearly be secondary and supportive. DNFBPs should also ensure that such high-risk country lists are incorporated into their internal risk assessment procedures and, where appropriate, embedded within automated monitoring systems to facilitate real time alert and increased scrutiny of any transactions or relationships, as appropriate.

Enhanced Due Diligence Obligations

Enhanced measures must be applied for any Business Relationship, customer or transaction that is related to a high-risk country. DNFBPs shall Apply enhanced measures to manage and mitigate the risk of money laundering and terrorism financing and proliferation financing. Such measures include but not limited to:

- Stricter verification of identity using documentation from independent and reliable sources.

- Detailed inquiry into the purpose and economic rationale of the relationship or transaction.
- Assessment of the legitimacy of the customer's source of wealth and funds.
- Evaluation of the business activities and counterparties, especially where the activity involves sectors vulnerable to abuse.
- Identification and risk assessment of foreign Politically Exposed Persons (PEPs) among the customer, Beneficial Owners, or other controlling persons.
- Regularly reviewing and updating their customer information, and more stringent internal reporting and approval measures.

These measures should be commensurate with the size and complexity of the business and the level of risks involved and the entities risk appetite.

Countermeasures and Supervisory Expectations

In cases of extreme risk—especially where a country is subject to an FATF Call for Action or similar UN Security Council resolutions—DNFBPs must apply risk-mitigation measures and countermeasures as directed by the relevant UAE authorities. These may include:

- Restricting or terminating specific products or services.
- Applying transaction limits, enhanced controls, or delayed settlement mechanisms.
- Requiring senior management approval for any dealings with the country or its nationals.
- Intensifying transaction monitoring with a focus on detecting patterns associated with high-risk jurisdictions.
- Refusing or exiting relationships, where the risks cannot be effectively mitigated.

Countermeasures should not be implemented in a vacuum but must follow clear directives from the NAMLCFTC, FIU, and Supervisory Authority. DNFBPs must remain alert to public notices and supervisory circulars that announce new designations or changes to existing risk classifications

Internal Policies, Procedures, and Controls

To ensure the compliance with the requirements referred to above, DNFBPs are required to have in place and maintain internal policies and procedures which cover:

- Organisation's risk appetite for high-risk country exposures.
- Definitions and process on how country risk is calculated, including integration into customer risk scoring model.
- Role descriptions and escalation metrics in relation to onboarding, checking and maintaining customers from high-risk jurisdictions.
- Continued staff education of geopolitical and jurisdictional threats.
- Periodic audit and assurance reviews of EDD and countermeasure processes involving high-risk countries.

The policies should be developed to fit the DNFBPs business model, risk profile, and customer profile, with a need to periodically be reviewed and updated, so that they are responsive to changes in the international and domestic risk environment.

9.3.6.4. Requirements for Money or Value Transfer Services

DNFBPs must exercise enhanced diligence when establishing or maintaining Business Relationships with Money or Value Transfer Services (MVTSs), particularly due to the inherent ML/TF/PF risks associated with fast, cross-border movement of funds and frequently informal agent networks. The due diligence required must be commensurate with the nature of the relationship and the level of exposure to ML/TF risk, and form part of the DNFBP broader risk-based AML/CFT/CPF program.

- Licensing and Legal Status: Before entering into a Business Relationship with an MVTS provider, DNFBPs must verify that the MVTS is duly licensed or registered and regulated in the UAE or its home jurisdiction and is subject to effective AML/CFT/CPF regulation and supervision. Evidence of licensing should be obtained and recorded as part of the onboarding process.
- Assessment of AML/CFT/CPF Controls and Risk Profile: DNFBPs must collect sufficient information necessary to make a risk-based judgment of the level of integrity and control environment. This includes but not limited to:

- Reviewing the MVTS's AML/CFT/CPF policies, procedures and internal controls including those with respect to CDD, recordkeeping, and STR filing.
- Reviewing the compliance of the MVTS with the provisions of the wire transfers.
- Identifying the MVTS's ownership, structure, and control effectiveness, including any relations with Politically Exposed Persons (PEP's), and the presence of any conflict of interests or lack of transparency in its management structure.
- Assessing who the MVTS's customers are and its exposure to different geographic regions (particularly high-risk jurisdictions) or sectors that may be subject to ML/TF/PF risks.
- Obtaining a list of agents or sub-agents where applicable and evaluating whether the MVTS exercises effective control over these agents, including through compliance training and periodic monitoring.

- Internal Controls and Documentation: DNFBPs must develop internal policies and procedures that address the specific risks associated with MVTS relationships, including criteria for onboarding and maintaining relationships, methodologies for assessing risks, obtaining management approvals, and ongoing monitoring of the MTVS's transactions.

All CDD/EDD and monitoring requirements on relationships involving services of Money or Value Transfer Service Providers (MVTSs) must be proportionate with the size, nature, and complexity of the business, and the related risk exposure of the DNFBP. A one-size-fits-all measures are not applicable, and DNFBPs are expected to customize their controls to mitigate the risk associated with a specific MVTS relationship.

Where elevated-risk factors are established – including transactions with unregulated or unlicensed MVTS operators, associations with high-risk jurisdictions, or beneficial ownership by Politically Exposed Persons (PEPs), the DNFBPs should take additional measures. These could involve stronger verification processes, more analysis of the source of the funds, and more regular checks and continues transactions monitoring. Where the risks of the MVTS relationship cannot be adequately reduced or mitigated through appropriate controls, DNFBPs should be prepared to decline the business or terminate the relationship. Decisions should be made based on a justified risk assessment and in a manner consistent with risk-based approach and compliance duties of the DNFBP to the UAE AML/CFT/CPF laws.

9.3.6.5. Requirements for Non-Profit Organizations

Non-Profit Organisations (NPO) can, in some instances, be abused for terrorist financing or for the financing of other illegal activities, in particular when governance controls are weak, financial flows are crossing borders, or NPO is operating in / raises funds from high-risk or conflict affected areas.

DNFBPs, taking into consideration a Risk-based approach, must while entering into or continuing Business Relationships with NPO's apply additional due diligence measures which are appropriate to the risks identified, and to ensure that those do not present an undue obstacle to the correct activities of charitable Institutions.

Examples of measures that DNFBPs should consider while dealing with an NPO include, but are not limited to:

- Understanding the nature and risk profile of the NPO. DNFBPs must assess the NPO's overall risk exposure by obtaining a detailed understanding of:
  - Its legal status, licensing or registration.
  - The structure of the board and the senior management, and the identification of major shareholders or individuals with controlling interest and any links with Politically Exposed Persons (PEPs).
  - The nature, scope, and extent of its operations and activities.
  - The source and profile of donors and beneficiaries, particularly where funds originate from or are disbursed to individuals or entities in high-risk jurisdictions.
  - The geographic regions where the NPO operates.
- Screening and sanctions compliance. DNFBPs will need to perform checks on NPO, its management, significant donors, and large beneficiaries against the UN Security Council lists, UAE terrorist list, and any other lists from international partners. Once a match is found, the DNFBP is required to initiate appropriate actions to report to Financial Intelligence Unit (FIU) as per applicable policies and procedures.
- Assessment of internal controls and transparency. DNFBPs need to assess whether the NPO's internal AML/CFT/CPF controls are appropriate to its size and complexity of its operations

and its risk profile. Such controls may include the establishment of clear accounting and financial reporting systems that are subject to independent audit, ensuring financial transparency and accountability. NPOs would also need to establish systems on due diligence of donors, vetting of beneficiaries and an ongoing monitoring of programmes to ensure that the money originates from and is distributed to legitimate people and purposes.

- Relationship-based controls by DNFBPs. Where a DNFBP maintains an ongoing relationship with an NPO, additional measures should include enhanced due diligence for NPO's operating in high-risk sectors or transferring funds to jurisdictions with weak governance, periodic reassessment of their risk classification, documented senior management approval for high-risk relationships, and clear procedures for escalation and reporting of suspicious activity.

DNFBPs should incorporate NPO characteristics risks into their internal AML/CFT/CPF program through risk-based customer identification and due diligence checklists, and enhanced screening for high-risk NPO's. Clear roles and responsibilities of the compliance staff managing the NPO exposure, backed by periodic training of front-line staff in NPO terrorism financing typologies, legal obligations, and red flag indicators. Furthermore, the effectiveness of controls related to NPO Business Relationships should also be assessed with the use of an external audit or compliance review. All such measures should be commensurate with the risk, approved by senior management, and consistent with both UAE AML/CFT/CPF Law and FATF requirements.

9.3.7. Reliance on a Third Party

DNFBPs could, under certain circumstances, rely on third parties to perform elements of the Customer Due Diligence (CDD) tasks, such as the identification and verification of customers and Beneficial Owners, and reason and intended nature of the Business Relationship. Such dependency does not excuse the DNFBPs primary responsibility to perform its duties with respect to meeting the CDD obligations under the AML/CFT/CPF Law and its implementing regulations.

Before taking reliance, the DNFBP must confirm that the third party is subject to regulation and supervision for AML/ CFT/CPF purposes and must be required to apply in a law or enforceable measures CDD and record keeping measures equivalent to the ones provided for in the AML/CFT/CPF Law of the UAE. In all cases, DNFBPs remain fully responsible for:

- The quality and adequacy of the CDD conducted.
- Obtaining, without delay, the underlying CDD data and documentation from the third party.
- Assessing the customer's risk level and taking measures to mitigate risks, such as continuous monitoring.

Moreover, DNFBPs are to undertake a documented evaluation of the AML/CFT/CPF framework of the third party, including the adequacy of its policies, the soundness of its internal controls, and the expertise and number of compliance staff, as well as the strength of its record keeping and audit mechanisms. Helpful tools in this regard can include formal due diligence questionnaires, third-party AML attestation letters, site inspections or reliance certification forms. Special caution is warranted where the third party is located outside the UAE. In such cases, DNFBPs must confirm that the foreign jurisdiction applies AML/CFT standards equivalent to those of the UAE, particularly in terms of regulatory oversight and enforcement.

When relying on a third party, DNFBPs must establish clear, enforceable arrangements—such as service-level agreements or reliance contracts—that set out the responsibilities of both parties. These agreements should define the scope of CDD measures to be conducted, the procedures for data retrieval, the format and frequency of information sharing, and the obligation to provide certified copies of identification and verification documents upon request. Third parties should also certify the authenticity of submitted documentation, where appropriate.

DNFBPs must also be able to obtain without delay all relevant CDD documentation—including identification, verification, Beneficial Ownership, source of funds, and ongoing monitoring information—held by the third party. This includes any data used to form the basis of customer risk assessments. Reliance arrangements must not result in delays, gaps, or incomplete records that could hinder timely access by the DNFBP or the relevant Supervisory Authority or the FIU. Even when CDD is initially performed by a third party, DNFBPs are required to maintain continuous oversight of the Business Relationship. This includes conducting transaction monitoring, periodic reviews of CDD information, and escalation of suspicious activity. DNFBPs must ensure that the risk classification of the customer remains current and must document any updates or re-assessments.

DNFBPs should distinguish between formal reliance on a third party and the use of information from independent and reliable sources during their own CDD processes. For example, using government registries, credit bureaus, or commercial databases to verify identity does not constitute third-party reliance. However, if CDD documentation is obtained from another obliged entity, and the DNFBP intends to rely on that for the entity's CDD process, the full reliance framework must be applied—including evaluation of the entity's regulatory status and contractual arrangements.

The degree of dependence and the level of verification and oversight measures should be proportionate with the nature, size and risk of the DNFBPs activities. Internal policies should specify when third-party reliance may be exercised, the conditions under which CDD conducted by third parties is accepted, and the responsibilities of compliance personnel for coordinating and approving those arrangements. High-risk reliance cases should be endorsed by senior management, with periodic independent reviews or audits performed to evaluate the functioning reliance exercises.

9.3.8. Restrictions on Customer Due Diligence in High-Risk and Tipping-Off Scenarios

In some high-risk cases, if a DNFBP knows or suspects that the customer or Beneficial Owner is engaged in ML, TF, or PF related activities and has reasonable grounds that if CDD measures are to be taken, that would result in tipping-off of the customer, the following obligations are applicable:

- Terrorism Financing (TF): If the suspicion relates to terrorism financing or if the DNFBP identifies a match against relevant UN Security Council Resolutions or the UAE's domestic TFS list:
    - The DNFBP must immediately freeze the relevant funds or assets, without prior notice to the customer.
    - A report must also be filed with the FIU without delay.
    - The transaction must not proceed under any circumstances.
- Money Laundering (ML): If the suspicion relates to money laundering, and there is a reasonable belief that performing CDD measures would tip off the customer:
    - The DNFBP must not delay the transaction in a way that could raise suspicion.
    - The DNFBP must decline to proceed with the transaction, if the risk cannot be mitigated without tipping off the customer.
    - A report must also be filed with the FIU without delay.

Required actions in such cases by the DNFBPs includes, but are not limited to, the following:

- Cease CDD procedures only if they are likely to tip off the customer. DNFBPs should not require any additional documentation that may raise suspicion during the CDD process if it would constitute tipping off.
- Do not proceed with the transaction if suspicion of ML or TF exists and can't be mitigated.
- Immediately file a Suspicious Transaction Report (STR) with the FIU. The report should explain the nature of the suspicion, the rationale for not performing further CDD, the red flags noticed, and the basis for declining the transaction.
- Maintaining a clear internal record of the rationale, timing, individuals involved, and actions taken.
- Refrain from informing the customer or any third party that an STR has been or may be filed, or that a decision not to proceed was due to AML/CFT concerns.

In conclusion the use of SDD or deferral of some elements of CDD must be accompanied by evidence to support the fact that there is a low risk of ML, TF, PF or other crime and that an associated risk assessment has been conducted and documented. DNFBPs may only take such measures in clearly defined and permissible circumstances, and only if there are strong in-house controls, continuous monitoring and senior management oversight of this exercise. These exceptions should not be allowed to undermine the AML/CFT/CPF framework of the DNFBP and must be embedded in a wider risk-based methodology. Whereas in the cases of suspicion of ML/TF/PF activities or when CDD might be considered as tipping off, DNFBPs shall stop CDD measures, refrain from proceeding with the transaction, and file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) without delay. Under no circumstances should such measures undermine compliance obligations or hinder timely reporting and effective risk mitigation.

Part V AML/CFT/CPF Reporting and Record Keeping

10. Suspicious Transaction Reporting

Under the UAE's AML/CFT/CPF legal and regulatory framework, all DNFBPs are obliged to promptly report to the Financial Intelligence Unit (FIU) suspicious transactions or attempted 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. DNFBPs are required to put in place and update indicators that can be used to identify possible suspicious transactions.

To fulfil these obligations, DNFBPs 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.

Failure to report a suspicious transaction without delay, whether intentionally or by gross negligence, is a federal crime in the UAE. The AML/CFT/CPF Law provides for sanctions, as outlined in Section 5, Overview of Applicable Sanctions for AML/CFT/CPF Violations, against any person, including the DNFBP, or its 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.

While acting in good faith in accordance with their statutory obligation to report suspicious transaction / activity to the FIU, DNFBPs, their board members, employees and authorized representatives are protected from any administrative, civil, or criminal liability as stipulated in the Executive Regulations. This protection is applicable even if the individual was unaware of the specific underlying criminal activity and irrespective of whether any unlawful conduct ultimately occurred. It also extends to situations wherein an employee files a report, despite their employer's refusal to do so.

Nonetheless, DNFBPs should note 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 / activity, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction / activity.

Note: PF-related TFS obligations, inclusive of screening, freezing without delay and reporting apply under *Cabinet Decision No. (74) of 2020* and EOCN guidance, which DNFBPs must abide by in parallel with present Guidelines.

10.1. UAE Financial Intelligence Unit (FIU)

The UAE FIU gains its legal mandate and powers primarily from the AML/CFT/CPF Law and Articles (44) to (47) of the Executive Regulations as an independent unit established to exclusively receive, analyse, and disseminate Suspicious Transaction / Activity Reports (STRs/SARs) from all Reporting Entities, including Financial Institutions (FIs), Designated Non-Financial Businesses and Professions (DNFBPs), and Virtual Asset Service Providers (VASPs), licenced or registered in the UAE. Additionally, the FIU, as the central national agency is tasked with the sole responsibility for performing the following functions:

- Receiving and analysing reports of suspicious cases from the Federal Customs Authority.
- Requesting additional information and documents relating to STRs/SARs, 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/SARs, to ensure the compliance of FIs and DNFBPs with their statutory AML/CFT obligations.
- Sending data relating to STRs/SARs 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/SARs or any other information to which it has access.

Under the aegis of the NAMLCFTC, 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 applicable reports by all DNFBPs. DNFBPs are mandated to register on the goAML system by following the system registration guide[11] and maintain their registration in an active status. The Compliance Officer of the company is required to register as the user of the system. goAML provides a secure link for each DNFBP to the FIU through their respective supervisory authorities. The system hosts processes for facilitating filing of applicable reports. The guidance documents for filing of STRs are posted on the dashboard of this system. All DNFBPs must register themselves immediately to confirm their readiness for filing of STRs/SARs and all other applicable reports.

The reports 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 reports, performs a trend analysis to understand the prevailing trends in transactions and sectors or Institutions where possibility of ML/TF/PF 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.

10.2. Processing of STRs by the FIU

A core function of the FIU is to conduct operational analysis on reports filed and information received from FIs, DNFBPs, VASPs 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 to determine the linkages between those targets and the possible proceeds of crime, money laundering, predicate offences and terrorist financing.

Upon the receipt of reports 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 DNFBPs 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 reports filed 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/TF. As a result of this analysis, the FIU may from time to time disseminate enhanced due diligence and fraud alerts to DNFBPs as a preventive measure and may also disseminate information to DNFBPs about prevalent or new and emerging ML/TF/PF typologies, or other specific risks which DNFBPs should take into consideration.

10.3. Meaning of Suspicious Transaction

Within the meaning of the AML/CFT/CPF Law and its implementing Executive Regulations, a suspicious transaction refers to any transaction, attempted transaction, or funds which a DNFBP 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 proliferation financing.
- 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 occurred or on proving the illicit source of the proceeds involved. DNFBPs do not need to have knowledge of

[11] https://www.moet.gov.ae/documents/20121/0/goAML+System+Registration+Guide+29102024.pdf/5b7e9a8f-4e82-ea40-e33b-e17b9ba21e18?t=1737006501052

the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; reasonable grounds are sufficient.

DNFBPs should also note that transactions need not be completed, in progress or pending completion 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. Thus, the obligation to report extends to incomplete or partially executed or declined transactions. It is applicable to attempted transactions which were halted due to incomplete documentation, rejected due to sanctions screening alerts, reversed or cancelled by the customer post due diligence inquiries, etc. DNFBPs must ensure that internal policies and procedures clearly outline escalation and reporting mechanisms for attempted transactions.

10.4. Identification of Suspicious Transactions

DNFBPs 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/TF/PF typologies. DNFBPs should also consider the red flag indicators incorporated in these guidelines, results of the NRA, any Sectoral Risk Assessment and their own ML/TF/PF business risk assessments in this regard.

As part of their overall AML/CFT/CPF framework, and commensurate with the nature and size of their businesses, DNFBPs 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.

Note: For the purpose of this guidelines "alerts" and "cases" shall be understood as to include automated transaction monitoring alerts or cases, manual transaction monitoring, internal referrals and law enforcement requests.

DNFBPs should ensure that they have an adequate process and dedicated, experienced staff for the investigation of and dealing with alerts/cases. The investigation of alerts/cases 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/CPF process. This means that DNFBPs 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 DNFBPs expeditiously investigate alerts/cases and possible indications of ML/TF/PF and immediately report the transaction upon determining that the transaction should be reported to the FIU. DNFBPs therefore need to able to show that from the moment of the alert immediate and continuous action has been taken.

In this respect, DNFBPs must have a procedure in place that defines the reporting process, and what steps to take in such cases. When investigating alerts/cases, it is important to examine the customer's earlier and related transactions, and to reconsider the customer's risk profile.

When identifying suspicious transactions, DNFBPs, and their management and employees, should be aware of the facts that, in relation to ML/TF/PF 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, DNFBPs 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, DNFBPs 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 regarding another. For this reason, clear internal policies and procedures regarding alert/case escalation and investigation, and internal suspicious transaction reporting are critical to an effective ML/TF/PF 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 section 13, Useful Links. A few examples of potentially suspicious transaction types that DNFBPs 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 amounts, especially when they are inconsistent with the nature of the customer's business.
- 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 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.

10.5. Requirement to Report

DNFBPs 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 about when the possible crimes or the suspicious transaction took place.

Under federal law and regulations, whether the DNFBP 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. With the exception of the exemption described in section 10.6, Specific Exemption from the Reporting Requirement below, any person, including DNFBPs 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 the applicable penalty.

10.6. Specific Exemption from the Reporting Requirement

While all DNFBPs are generally required to report suspicious transactions, the AML/CFT/CPF Law and Executive Regulations provide specific limited exemption for lawyers, notaries, other legal professions or independent legal auditors on the grounds of professional secrecy only under one specific condition:

When they have obtained information concerning the *transactions 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*.

It is important to note that there are no exemptions from the statutory reporting requirement provided for other DNFBPs under the AML/CFT/CPF Law or Executive Regulations.

10.7. Procedures for the Reporting of Suspicious Transactions / Activities

As the designated Competent Authority for receiving and analysing STRs/SARs from all DNFBPs, it is within the purview of the FIU to determine the procedures for the reporting of suspicious transactions. As stated in the Executive Regulations, DNFBPs 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 Executive Regulations provide for the reporting of STRs to be affected by the designated compliance officer of the DNFBP. Specifically, the Executive Regulations state 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, DNFBPs 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 10.10, 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 regarding reporting to the FIU.
- Other conditions deemed appropriate by the 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 DNFBPs business.

10.8. Timing of Suspicious Transaction / Activity Reports (STRs/SARs)

DNFBPs are obliged to report STRs/SARs to the FIU without delay. Since it is the responsibility of the designated 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 7.1, Compliance Officer) it follows that the STRs/SARs should be immediately reported once the suspicious nature of the transaction becomes clear. This means that the internal reporting of suspicion to the Compliance Officer should be done directly once the suspicion or reasonable grounds for suspicion are established, and immediately the designated Compliance Officer has confirmed that the transaction (whether pending, in progress, or past) is suspicious, it should be reported.

Without prejudice to the above, DNFBPs 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 Compliance Officer. The DNFBP 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, DNFBPs 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 10.4, Identification of Suspicious Transactions). These policies and procedures should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

10.9. Basic Structure of and STR or SAR

Compliance Officers, Money Laundering Reporting Officers (MLROs), and other relevant employees within DNFBP entities who use the goAML platform must be fully familiar with the various report types. It is essential that the DNFBP selects the appropriate report type when submitting information through the goAML platform.

Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) are the primary report types used for submitting new suspicions. In contrast, Additional Information File without Transactions (AIF) and Additional Information File with Transactions (AIFT) are supplementary reports used to provide additional information relating to an already submitted STR or SAR. When filing an AIF or AIFT, the DNFBP must reference the original STR or SAR submission number.

STR

If, during the establishment or course of the business relationship, or when carrying out a transaction for or on behalf of a customer or occasional customer, a DNFBP suspects that the transaction may relate to money laundering, a predicate offence, or the financing of terrorism or illegal organisations, then the DNFBP is required to submit an STR to the FIU within the timeframe outlined in the applicable guidance.

SAR

If a DNFBP suspects that any activity or attempted transaction (i.e., one that was not executed) during the course of a business relationship may be linked to money laundering, predicate offences, or terrorist or illegal financing, a SAR must be submitted to the FIU within the reporting timeline established in the guidance.

AIF (without Transactions)

If the FIU requests further information while reviewing an STR or SAR, the DNFBP that submitted the original report may receive an AIF request through the goAML Message Board. In this case, the DNFBP must submit an AIF report through goAML, containing only non-transactional supplemental details.

AIFT (with Transactions)

If the FIU requests additional information including transactional details while assessing an STR or SAR, the DNFBP will receive an AIFT request via the Message Board. The DNFBP must then submit an AIFT report through goAML, containing the requested transaction information.

RFI (Request for Information) without Transactions

Where the FIU seeks further information from multiple DNFBPs, not just the reporting entity, an RFI request will be sent through the goAML Message Board. DNFBPs receiving such a request are required to submit an RFI report via the platform.

RFI (with Transactions)

This is similar to the standard RFI request but requires the inclusion of transaction data in the submission.

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, a DNFBP entity 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[12].

Then the entity 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)

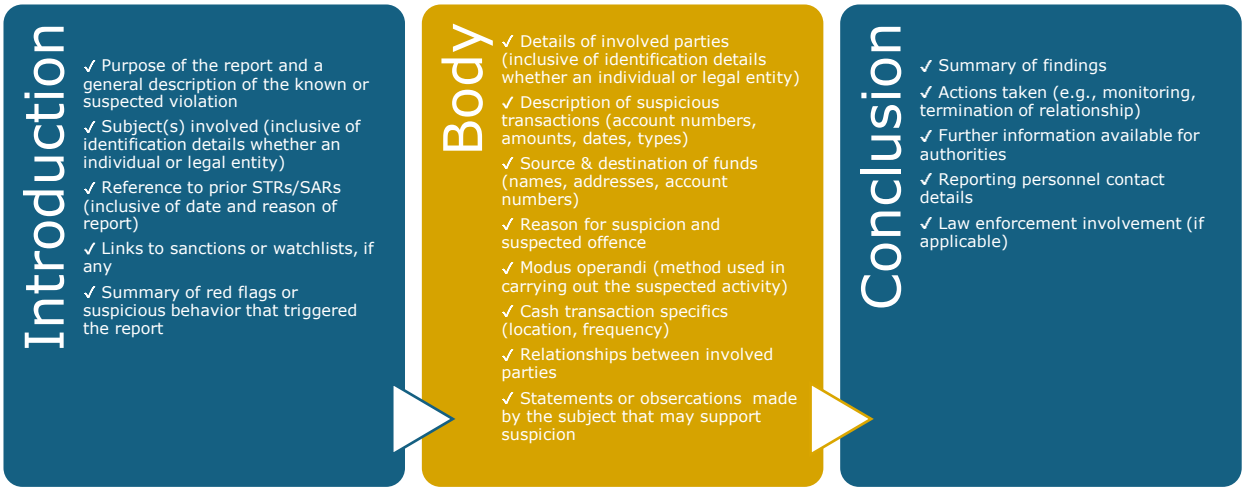
If, during the establishment or course of the customer relationship, or when conducting an activity on behalf of a customer or a potential customer, a DNFBP entity identifies activities related to high-risk countries as defined by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee[12].

The DNFBP 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.

Note: Where a transaction and/or activity involves a high-risk country also triggers suspicion, it imperative that DNFBPs prioritize STR obligations.

10.9.1. STR/SAR Narrative Reporting

When all relevant information has been collected, analysed, and documented, and the DNFBP entity determines that an STR or SAR is warranted, the details must be presented in a concise, chronological format using a similar narrative report template as provided in the diagram below which presents a summary of the required narrative structure. It serves as a guide for formatting purposes but is not a substitute for the complete reporting content. The narrative report serves as a supplement to the goAML submission, addressing any limitations in the standard report description field.



10.10. Confidentiality and Prohibition against "Tipping Off"

When reporting suspicious transactions to the FIU, DNFBPs are obliged to maintain confidentiality regarding 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/CPF framework, and in keeping with the nature and size of their businesses, DNFBPs, 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. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

[12] A comprehensive list of High-Risk Countries can be found on NAMLCFTC website

DNFBPs must ensure that all relevant information relating to STRs/SARs 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. DNFBPs need to ensure that policy and procedures are reflected in for example, appropriate access rights regarding core systems used for case management and notifications, secure information flows and guidance/training to all staff members involved. This guidance and training are 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 / activities, what questions they must 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 DNFBP 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/TF/PF.

It is a federal crime for DNFBPs 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 the applicable penalty.

10.11. Protection against Liability for Reporting Persons

DNFBPs, as well as their board members, employees and authorised representatives, are protected by the relevant articles of the AML/CFT/CPF Law and Executive Regulations from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious transaction / 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 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.

10.12. 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:

- DNFBPs 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 to mitigate the associated ML/TF/PF risks. It is however not required to terminate the relationship.

Further guidance on both topics is provided below.

- **FIU Instructions**

After receiving an STR/SAR from a DNFBP, the FIU may or may not revert to the reporting entity with specific instructions / directives, 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 Compliance Officer of the DNFBP. DNFBPs must maintain strict confidentiality regarding FIU directives and must ensure that appropriate documentation of actions undertaken as a result of those directives is maintained, including but not limited to records of exact time and date of receipt of the FIU directive, the timing and manner of executing the directives, ensuring that records re retained in accordance with the statutory record-keeping obligations.

Confidentiality of FIU's Instructions

The responsibility for coordinating the DNFBPs prompt compliance with the FIU's instructions or requests lies with the designated AML/CFT/CPF 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 DNFBPs 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 DNFBP. Regardless of the circumstances surrounding the FIU's instructions or requests, including whether the compliance officer is permitted

to provide explanations to the staff of the DNFBP, the DNFBP 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/SAR involves an anticipated, pending, or already in-progress transaction, DNFBPs 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, DNFBPs 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 DNFBPs 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 wherein an STR/SAR is anticipated, pending, or in process of being prepared by the DNFBP STR/SAR or an STR/SAR has been reported to the FIU by the DNFBP, any additional suspicions that may arise should also be immediately reported to the FIU as a follow-up to the original STR/SAR. 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 DNFBP 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 DNFBP.
    - 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 DNFBP 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 DNFBP 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, DNFBPs 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, DNFBPs 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, DNFBPs 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), DNFBPs 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.

DNFBPs 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, DNFBPs 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

DNFBPs 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 DNFBPs 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). DNFBPs 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, DNFBPs 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/TF/PF risks associated with the business relationship.

In such cases, beyond the EDD measures described in previous sections (see Sections 9.3.3, Ongoing Monitoring of the Business Relationship and 9.3.6 Enhanced Due Diligence (EDD) Measures), DNFBPs 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).

DNFBPs should also document the specific EDD, ongoing monitoring, and additional control measures to be taken. In this regard, DNFBPs 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/TF/PF risks associated with the business relationship.

11. Record Keeping

11.1. Obligations and Retention Timeframes

Designated Non-Financial Businesses and Professions (DNFBPs) must establish and maintain comprehensive records covering all transactions, customer due diligence (CDD) documentation, business correspondence, and outcomes of any analysis performed. Records must also encompass documentation generated as part of the entity's ML/TF/PF risk assessment and mitigation processes, in accordance with the requirements set out under the Executive Regulations.

Records are to be retained in an orderly manner that allows for effective analysis and the tracing of financial activities. They must be sufficient to reconstruct transactions in a manner that, if required, can support investigations or be used as evidence in legal proceedings. All CDD and transactional records must be readily available to Competent Authorities upon request and without undue delay.

The minimum statutory retention period for such records is five (5) years, calculated from the latest of the following events:

- The termination of a business relationship or closure of a customer account.
- Completion of an occasional transaction where no business relationship exists.
- Completion of a supervisory inspection.
- The issuance of a final judgment by a competent judicial authority.
- Dissolution, liquidation, or termination of a legal person or arrangement.

Competent Authorities may, at their discretion, require DNFBPs to extend record retention beyond the minimum period, either for specific customers, transactions, or broader categories considered of supervisory or investigative interest.

To comply with these requirements, DNFBPs must implement documented record-keeping policies and procedures, proportionate to the nature, size, and scale of their operations. These policies should be formally approved by senior management, regularly reviewed, and communicated across all relevant levels of the organisation. Key considerations should include:

- Allocation of responsibilities for record-keeping, data protection, and contingency planning, including escalation protocols.
- Procedures for cataloguing, archiving, transfer, and eventual destruction of records.
- Measures ensuring the prevention of any unauthorized access to both archived and active data.
- Audit and quality assurance mechanisms to test the adequacy and effectiveness of the record-keeping framework.

11.2. Required Record Types

The AML/CFT/CPF framework requires DNFBPs to maintain records across several categories. These broadly include:

- Transaction Records: All documents and data related to a business transactions weather it was domestic or international transaction.
- Due Diligence Records: Customer identification information, supporting documentation, due diligence results, monitoring records, and internal analysis.
- Company Information: Corporate formation and governance documents, as well as beneficial ownership and senior management details.
- Third Party Reliance Records: Documentation evidencing reliance on third parties for CDD or any other measures, ensuring accessibility and compliance with record-retention obligations.
- Ongoing Monitoring Records: Documentation from the continuous monitoring of business relationships, including reviews, analyses, and related correspondence.
- Suspicious Transaction Report (STR) Records: Internal and external STRs, investigations, correspondence, and related communications with the FIU.

Further details with regards to each category is provided below.

11.2.1. Transaction Records

All DNFBPs are required to retain records for all transactions. Whether domestic or cross-border, occasional or for an ongoing business relationship for no less than five (5) years. Such records should include:

- Customer instructions, correspondence, and order forms.
- Receipts, invoices, billing notifications, statements of account, and any other related financial documentation.
- Escrow or fiduciary account records.
- Agreements involving sales, purchases, leases, or mergers.
- Analytical and statistical data regarding financial flows, values, volumes, and other relevant details.

In addition to the above, DNFBPs should retain and compile any notes or explanations related to unusually complex, large, or atypical transactions.

11.2.2. Customer Information Records

DNFBPs are required to maintain records obtained through their CDD, EDD, or SDD measures on customers, beneficial owners, and other controlling parties. Examples include:

- Customers account information and any related files.
- Customer communications, call logs, or meeting records (including recordings and transcripts where applicable)
- Copies of identification documents, due diligence forms, profiles, and supporting documents.
- Risk classification and assessment records based on the entity risk assessment conducted.

11.2.3. Company Information Records

The Executive Regulations stipulate 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. Records should include, at a minimum:

- Incorporation, registration, dissolution, and governance documentation.
- Amendments to legal form, name, address, or authorised representatives.
- Identification documents of beneficial owners, shareholders, directors, and equivalent controlling parties.

To fulfil their statutory record-keeping obligations in this regard, DNFBPs 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.

11.2.4. Reliance on Third Parties Records

DNFBPs that rely on third parties, whether unaffiliated or members of their own groups, are obliged to ensure that copies of all the necessary documents collected through the performance of CDD measures or any other measures which has been assigned to the third party can be obtained upon request and without delay, and that the third parties adhere to the record-keeping provisions of the AML/CFT/CPF Decision.

To achieve their statutory obligations, and commensurate with the nature and size of their businesses, DNFBPs 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 DNFBPs should give consideration when formulating relevant policies, procedures and controls include, but are not limited to:

- The entity's role and responsibility to assess, monitor, and test the third-party policies, procedures, and controls related to records keeping, and data protection. This should also include appropriate business contingency and escalation procedures.
- Service level agreements addressing accessibility and security.
- 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.

11.2.5. Ongoing Monitoring on Business Relationship Records

DNFBPs are required to retain all customer records and documents obtained through the ongoing monitoring of the Business Relationships. Examples of such records include but are not limited to:

- Transactions reviewed, analysis, and investigation records.
- All customer correspondence and meeting notes related to those transactions or their analysis and investigation. This is inclusive of customer confirmations on end-use/end-user, supply chain counterparties, screening outcomes, rational for due diligence decisions.
- CDD, EDD, and SDD 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 of the transactions.
- Transaction handling decisions, including approval or rejection records, along with related analysis and correspondence.

11.2.6. Suspicious Transaction Reports (STR) Records

DNFBPs are required to retain all records and documents pertaining to STRs or any other reports and the results of all analysis or investigations performed. Such records should include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence.
- Requests for information by competent authorities.
- CDD and Business Relationship monitoring records, documents and information obtained while analysing or investigating potentially suspicious transactions, and all internal or external correspondence or communication records associated with them.
- 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.

Part VI Appendices

12. Glossary of Terms

Term	Definition
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 AML/CFT/CPF Law.
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.
Concerned Authorities	The governmental entities concerned with the implementation of any provision of this Decree by Law within the State.
Crime	The crime of Money Laundering and the predicate offences related thereto, or the financing of terrorism, or the proliferation financing.
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.
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.
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 AML/CFT/CPF Law.
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/TF).
Executive Office	The Executive Office for Control and Non-Proliferation, concerned with the implementation of targeted financial sanctions within the State.
Executive Regulations	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
FATF	The Financial Action Task Force is an inter-governmental 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.
Freezing	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.

Term	Definition
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	Any person engaged in one or more financial activities or operations determined by the Executive Regulations of the AML/CFT/CPF Law, on behalf of or for the benefit of a customer.
Financing of Terrorism	Any of the acts defined in Clause (1) of Article (3) of the AML/CFT/CPF Law.
FIU	Financial Intelligence Unit
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.
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.
Law (or "AML/CFT/CPF Law")	Federal Decree by Law No. (10) of 2025 Regarding Anti-Money Laundering, and Combating the Financing of Terrorism and Proliferation Financing
Law Enforcement Authorities	The federal and local authorities entrusted, pursuant to the provisions of AML/CFT/CPF 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.
Legal Arrangement	Trusts or other similar arrangements.

Term	Definition
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.
Money Laundering	Any of the acts defined in Clause (1) of Article (2) of the AML/CFT/CPF Law, including its commission through digital systems, Virtual Assets, or cryptographic technologies.
Non-Profit Organisations (NPOs)	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.
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 a felony or misdemeanour, 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.
Proceeds	Funds derived, directly or indirectly, from the commission of any felony or misdemeanour, 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.
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.
RBA	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/TF/PF risk in accordance with the nature and degree of the risk.
Registrar	The competent authority responsible for supervising the economic or trade register of the various types of establishments registered in the UAE, as regulated by the legislation in force in the UAE.

Term	Definition
Sanctions Committee	The UN Security Council Committee established as per resolution numbers 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.
Sanctions List	A list wherein individuals and terrorist organisations, 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 management of their own Funds to a Trustee pursuant to a Trust Instrument.
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
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.
Suspicious Transactions	Transactions involving funds for which there are reasonable grounds to suspect that they constitute Proceeds of any felony or misdemeanour, or are related to Money Laundering, Financing of Terrorism, or Proliferation Financing, whether such transactions were executed or merely attempted.
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.
Targeted Financial Sanctions (TFS)	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.
Transaction	Any disposal or utilization involving Funds or Proceeds, including, inter alia, deposit, withdrawal, transfer, sale, purchase, lending, exchange, mortgage, or donation.

Term	Definition
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.
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.
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.
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.
Without Prior Notice	The taking of an action without prior notice or involvement of the owner, Customer, or the affected Party.
Virtual Asset Service Providers (VASPs)	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.
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.

13. 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
Executive Office for Control and Non-Proliferation (EOCN)	https://www.uaeiec.gov.ae/en-us/about-us
Financial Action Tas Force (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/
Ministry of Economy & Tourism	https://www.moet.gov.ae/en/home
UAE National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee (NAMLCFTC)	https://www.namlcftc.gov.ae/en/
Securities and Commodities Authority	http://www.sca.ae/
UAE Financial Intelligence Unit (UAE FIU)	https://www.uaefiu.gov.ae/en/
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/