الإمارات العربية المتحدة
وزارة الإقتصـــــاد

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

Guidelines for Designated Non-Financial Businesses and Professions

April 1, 2019

Contents

Part I—Overview

1. Introduction
   - 1.1 Purpose and Scope
   - 1.2 Applicability
   - 1.3 Legal Status
   - 1.4 Organisation of the Guidelines

2. Overview of the AML/CFT Legal, Regulatory, and National Strategy Frameworks of the United Arab Emirates
   - 2.1 National Legislative and Regulatory Framework
   - 2.2 International Legislative and Regulatory Framework
   - 2.3 AML/CFT National Strategy Framework

3. Highlights of Key Provisions Affecting Supervised Institutions
   - 3.1 Summary of Minimum Statutory Obligations of Supervised Institutions
   - 3.2 Confidentiality and Data Protection
   - 3.3 Protection against Liability for Reporting Persons
   - 3.4 Statutory Prohibitions
   - 3.5 Money Laundering
   - 3.6 Predicate Offences
   - 3.7 Financing of Terrorism
   - 3.8 Financing of Illegal Organisations
   - 3.9 Sanctions against Persons Violating Obligations

Part II—Identification and Assessment of ML/FT Risks

4. Identification and Assessment of ML/FT Risks
   - 4.1 Risk-Based Approach
   - 4.2 The Standard ML Model and Generic ML/FT Risks
   - 4.3 ML/FT Typologies
   - 4.4 Risk Factors
     - 4.4.1 Customer Risk
     - 4.4.2 Geographic Risk
     - 4.4.3 Product-, Service-, Transaction-Related Risk
     - 4.4.4 Channel-Related Risk
     - 4.4.5 Other Risk Factors

Contents

4.5 Risk Assessment
4.5.1 Documentation, Updating, and Analysis
4.5.2 Assessing Enterprise Risk
4.5.3 Assessing Business Relationship Risk
4.5.4 Assessing New Product and New Technologies Risks
4.5.5 Examples of Risk Assessment Operations

Part III—Mitigation of ML/FT Risks

5. Internal Policies, Controls and Procedures

6. Customer Due Diligence (CDD)
6.1 Risk-Based Application of CDD Measures
6.2 Circumstances and Timing for Undertaking CDD Measures
6.2.1 Establishment of a Business Relationship
6.2.2 Occasional Transactions
6.2.3 Exceptional Circumstances
6.3 Customer Due Diligence (CDD) Measures
6.3.1 Customer and Beneficial Owner Identification/Verification
6.3.2 CDD Requirements Concerning Legal Persons and Arrangements
6.3.3 Establishing a Customer Due Diligence Profile
6.3.4 Ongoing Monitoring of the Business Relationship
6.3.5 Reviewing and Updating the Customer Due Diligence Information
6.4 Enhanced Due Diligence (EDD) Measures
6.4.1 Requirements for Politically Exposed Persons (PEPs)
6.4.2 Requirements for High-Risk Customers or Transactions
6.4.3 Requirements for High-Risk Countries
6.4.4 Requirements for Money or Value Transfer Services
6.4.5 Requirements for Non-Profit Organisations
6.5 Simplified Due Diligence (SDD) Measures
6.6 Reliance on a Third Party

7. Suspicious Transaction Reporting
7.1 Role of the Financial Intelligence Department
7.2 Processing of STRs by the FIU
7.3 Meaning of Suspicious Transaction
7.4 Identification of Suspicious Transactions
7.5 Requirement to Report
7.6 Specific Exemption from the Reporting Requirement

Contents

Part IV—AML/CFT Administration and Reporting

7.7 Procedures for the Reporting of Suspicious Transactions
7.8 Timing of Suspicious Transaction Reports (STRs)
7.9 Confidentiality and Prohibition against “Tipping Off”
7.10 Protection against Liability for Reporting Persons
7.11 Handling of Transactions and Business Relationships after Filing of STRs

8. Governance
8.1 Compliance Officer
8.1.1 Appointment and Approval
8.1.2 Responsibilities
8.2 Staff Screening and Training
8.3 Group Oversight
8.4 Independent Audit Function
8.5 Responsibilities of Senior Management
8.6 Governance Issues of Small Organisations

9. Record Keeping
9.1 Obligations and Timeframe for the Retention and Availability of Records
9.2 Required Record Types
9.2.1 Financial Transactions
9.2.2 Customer Information
9.2.3 Company Information
9.2.4 Reliance on Third Parties to Undertake CDD
9.2.5 Ongoing Monitoring of Business Relationships
9.2.6 Suspicious Transaction Reports

10. International Financial Sanctions
10.1 Targeted Financial Sanctions
10.2 UAE Cabinet Decision No. (20) of 2019
10.3 Other International Sanctions
10.4 Sanction Screening, Alert Management, Reporting

Part V—Appendices

11. Appendices
11.1 Glossary of Terms
11.2 Useful Links

Part I—Overview

1. Introduction

1.1 Purpose and Scope

The purpose of these **Anti-Money Laundering and Combating the Financing of Terrorism and the Financing of Illegal Organisations Guidelines for Designated Non-Financial Businesses and Professions ("DNFBPs")** ("Guidelines") is to provide guidance and assistance to supervised institutions that are DNFBPs, in order to assist their better understanding and effective performance of their statutory obligations under the legal and regulatory framework in force in the United Arab Emirates ("UAE" or "State").

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

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

Finally, it should be noted that, except for a brief high-level overview of some key facts regarding the United Nations Targeted Financial Sanctions (TFS) regime, and the related Cabinet Decision No. (20) of 2019 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* included in Section 10, International Financial Sanctions, detailed guidance on the subject of TFS and other international financial sanctions programmes and restrictive measures which affect DNFBPs is outside of the scope of these Guidelines. Due to the significance, complexity and extent of the subject matter, it is more appropriate for this material to be covered in depth in separate guidance materials.

1.2 Applicability

Unless otherwise noted, these Guidelines apply to all Designated Non-Financial Businesses and Professions, and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and their respective

Financial and Commercial Free Zones, whether they establish or maintain a Business Relationship with a Customer, or engage in any of the financial activities and/or transactions or the trade and/or business activities outlined in Articles (2) and (3) of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations*.

Specifically, and without prejudice to the definition of a DNFBP as provided for in the relevant legislative and regulatory framework of the State (see Section 2.1, National Legislative and Regulatory Framework), they are applicable to all such natural and legal persons in the following categories:

- Auditors and accountants;
- Lawyers, notaries and other legal professionals and practitioners;
- Company and trust service providers;
- Dealers in precious metals and stones;
- Real estate agents and brokers;
- Any other Designated Non-Financial Businesses and Professions (DNFBPs) not mentioned above.

1.3 Legal Status

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

As such, these Guidelines do not constitute additional legislation or regulation, and are not intended to set legal, regulatory, or judicial precedent. They are intended rather to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE and their respective Free Zones, and supervised institutions are reminded that the Guidelines do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between these Guidelines and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in these Guidelines should be interpreted as providing any explicit or implicit guarantee or assurance that the Supervisory or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

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

1.4 Organisation of the Guidelines

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

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

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

Part III—Mitigation of ML/FT Risks;

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

Part V—Appendices.

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

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

In certain instances in which there are meaningful differences between the relevant legal and regulatory framework currently in force and previous laws or regulations, or in which there are differences in specific regulatory requirements between various Supervisory

Authorities, the Guidelines may or may not highlight these differences. In the event of such differences or discrepancies, supervised institutions seeking further clarification on matters related to those sections are invited to contact their relevant Supervisory Authority through the established channels.

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

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

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

2.1 National Legislative and Regulatory Framework

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

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

2.2 International Legislative and Regulatory Framework

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

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

- The United Nations (UN).

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

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

2.3 AML/CFT National Strategy Framework

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

The UAE is deeply committed to combating money laundering and the financing of terrorism and illegal organisations. To this end, the Competent Authorities have established the appropriate legislative, regulatory and institutional frameworks for the prevention, detection and deterrence of financial crimes, including ML/FT. They also continue to work towards reinforcing the capabilities of the resources committed to these efforts, and towards improving their effectiveness by implementing the internationally accepted AML/CFT standards recommended and promoted by FATF, MENAFATF and the other FSRBs, as well as by the United Nations, the World Bank and the International Monetary Fund (IMF).

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

- Enhancing the federal legislative and regulatory framework, embodied by the introduction of the new AML/CFT Law and Cabinet Decision, which incorporate the FATF standards;
- Conducting the National Risk Assessment (NRA) to identify and assess the ML/FT threats and inherent vulnerabilities to which the country is exposed, as well as to assess its capacity in regard to combating ML/FT at the national level;
- Formulating a National AML/CFT Strategy and Action Plan that incorporate the results of the NRA and which are designed to ensure the effective implementation, supervision, and continuous improvement of a national framework for the combating of ML/FT, as well as to provide the necessary strategic and tactical direction to the country's public and private sector institutions in this regard.

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

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

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

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

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

- Effective compliance with the laws and regulations governing banking activities and other financial services;
- Awareness by DNFBPs of the relevant ML/FT risks facing the UAE in general, and their sectors in particular, as informed by the results of the NRA, as well as their awareness of their statutory obligations in regard to the management and mitigation of those risks.

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

3. Highlights of Key Provisions Affecting Supervised Institutions

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

3.1 Summary of Minimum Statutory Obligations of Supervised Institutions

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

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

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

3.2 Confidentiality and Data Protection

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

Designated Non-Financial Businesses and Professions are obliged to report suspicions of a Crime to the Competent Authority (see Section 7, Suspicious Transaction Reporting). In reporting their suspicions, they must maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and make reasonable efforts to ensure the information and data reported are protected from access by any unauthorised person.

It should be noted that the confidentiality requirement does not pertain to communication within the supervised institution 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, either directly or indirectly, that a report has been made, under penalty of sanctions (see Section 3.9, Sanctions against Persons Violating Obligations).

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 (see Section 3.9, Sanctions against Persons Violating Obligations).

Under specific circumstances, the AML-CFT Law and the AML-CFT Decision 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 clients against legal or judicial proceedings. For further guidance, see Section 7.4, Specific Exemptions from Reporting Requirement.

3.3 Protection against Liability for Reporting Persons

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

The AML-CFT Law and the AML-CFT Decision provide Designated Non-Financial Businesses and Professions, 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 Competent Authority.

3.4 Statutory Prohibitions

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

Designated Non-Financial Businesses and Professions are prohibited from the following activities:

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

3.5 Money Laundering

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

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

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

- Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source;
- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds;
- Acquiring, possessing or using proceeds upon receipt;
- Assisting the perpetrator of the predicate offense to escape punishment.

Both the AML-CFT Law and the AML-CFT Decision define “funds” as “assets in whatever form, whether tangible, intangible, movable or immovable including national currency,

foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets." They likewise define "proceeds" as "funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds."

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

- Funds bank or other financial accounts, including virtual or so-called crypto currencies;
- Financial instruments or securities, such as shares, bonds, notes, commercial paper, promissory notes, IOUs, share warrants, options, rights (including land rights), or other transferrable securities or bearer negotiable instruments;
- Contracts, loan instruments, titles, claims, insurance policies, or their assignment;
- Intellectual property (including but not limited to patents or registered trademarks), royalties, licenses, or the rights thereto;
- Physical property, including but not limited to commodities, land, precious metals and stones, motor vehicles or vessels, works of art, or any other goods exchanged as payment-in-kind.

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

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

3.6 Predicate Offences

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

regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

FATF has designated 21 (twenty-one) major categories comprising many individual predicate offences. Each of these categories of predicate offences has been criminalised in the legislative framework of the State. Supervised institutions are reminded that this is not an exhaustive list of predicate offences, but simply a convenient categorisation, since in the UAE according to the AML-CFT Law, even crimes that do not appear on this list, whether felonies or misdemeanours, can be predicate offences to money laundering.

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

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

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

3.7 Financing of Terrorism

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

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

> "The number, type, scope, and structure of terrorist actors and the global terrorism threat are continuing to evolve. Recently, the nature of the global terrorism threat has intensified considerably. In addition to the threat posed by terrorist organisations such as ISIL, Al-Qaeda and other groups, attacks in many cities across the globe are carried out by individual terrorists and terrorist cells ranging in size and complexity. Commensurate with the evolving nature of global terrorism, the methods used by terrorist groups and individual terrorists to fulfil their basic need to generate and manage funds is also evolving.
>
> Terrorist organisations use funds for operations (terrorist attacks and pre-operational surveillance); propaganda and recruitment; training; salaries and member compensation;

and social services. These financial requirements are usually high for large terrorist organisations, particularly those that aim to, or do, control territory. In contrast, the financial requirements of individual terrorists or small cells are much lower with funds primarily used to carry out attacks. Irrespective of the differences between terrorist groups or individual terrorists, since funds are directly linked to operational capability, all terrorist groups and individual terrorists seek to ensure adequate funds generation and management."[1]

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

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organisation or terrorist person or intended to finance a terrorist organisation, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or
- Providing, collecting, preparing or obtaining proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or committing such acts on behalf of a terrorist organisation or a terrorist person while aware of their true background or purpose.

There are numerous risk factors that supervised institutions should consider important when assessing their exposure to the risk of terrorist financing (see Section 4.2, Risk Factors), including geographic-, sector-, channel-, product-, service- and customer-specific risks.

3.8 Financing of Illegal Organisations

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

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

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

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

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

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

3.9 Sanctions against Persons Violating Reporting Obligations

(AML-CFT Law 15, 24, 25)

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

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

According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a Crime. It should also be noted that the transactions or funds that are the subject of the suspicion may represent only part of the proceeds of the criminal offence, regardless of their value.

Likewise, the AML-CFT Law provides for sanctions against anyone who warns or notifies a person of a suspicious transaction report or reveals that a transaction is under review or investigation by the Competent Authorities, as follows:

- Imprisonment for no less than six months and a penalty of no less than AED100,000 and no more than AED500,000; or
- Any of these two sanctions.

Part II—Identification and Assessment of ML/FT Risks

4. Identification and Assessment of ML/FT Risks

(AML-CFT Law 16.1; AML-CFT Decision 4.1)

DNFBPs are obliged to identify, assess, and understand the ML/FT risks to which they are exposed. Both the AML-CFT Law and the AML-CFT Decision provide that supervised institutions may utilize a risk-based approach with respect to the identification and assessment of ML/FT risks. Guidance on these subjects is provided in the following sections.

4.1 Risk-Based Approach (RBA)

(AML-CFT Law 16.1; AML-CFT Decision 4.1-3)

Implicit in both the AML-CFT Law and the AML-CFT Decision is the well-established concept of a risk-based approach (RBA) to the identification and assessment of ML/FT risks. Specifically, the AML-CFT Law states that DNFBPs should "identify crime risks within (their) scope of work" and should update their risk assessments on the basis of the various risk factors set out in the AML-CFT Decision. Likewise, the AML-CFT Decision states that FI/DNFBPs' identification, assessment and understanding of the risks should be carried out "in concert with their business nature and size," and that various risk factors should be considered in determining the level of mitigation required. The AML-CFT Decision further provides that enhanced due diligence should be performed in cases where high risks are identified, while simplified due diligence may be performed in certain cases where low risk is identified, unless there is a suspicion of ML/FT.

The use of a RBA thus allows supervised institutions to allocate their resources more efficiently and effectively, within the scope of the national AML/CFT legislative and regulatory framework, by adopting and applying preventative measures that are targeted at and commensurate with the nature of risks they face.

While there are limits to any risk-management approach, and no RBA can be considered as completely failsafe, supervised institutions should nevertheless understand that a risk-based approach is not a justification for ignoring certain ML/FT risks, nor does it exempt them from taking reasonable and proportionate mitigation measures, even for risks that are assessed as low. Their statutory obligations require them to identify, assess and understand the level of risk presented by their customers, and to be in a position to apply sufficient AML/CFT mitigation measures on a risk-appropriate basis at all times.

In order to do so, they should identify and assess their exposure to ML/TF risks on the basis of a variety of dynamic risk factors (see Section 4.4, Risk Factors), some of which are related to the nature, size, complexity and operational environment of their businesses, and

others of which are customer- or relationship-specific. Furthermore, they should take reasonable and proportionate risk mitigation measures based on the severity of the risks identified.

Conducting enterprise-level and business relationship-specific risk assessments (see Section 4.5.3, Assessing Business Relationship Risk and Section 4.5.2, Assessing Enterprise Risk) can assist supervised institutions to understand their risk exposure and the areas they should give priority in combatting ML/TF. DNFBPs should also take into consideration the results of the most recent National Risk Assessment (NRA) as being instructive in regard to the specific risks faced by their sectors and the markets in which they operate.

4.2 The Standard ML Model and Generic ML/FT Risks

To identify, understand and accurately assess the ML/FT risks to which they are exposed at both the enterprise and business relationship levels, DNFBPs should be aware of the source of those risks in the broader context of the classical or standard money laundering model. This model describes the crime of money laundering as consisting of three distinct (though sometimes overlapping) phases, briefly summarised below:

- Placement. In this phase, criminals attempt to introduce Funds or the Proceeds of Crime into the financial system using a variety of techniques or typologies (see Section 4.3, ML/FT Typologies). Once the Funds or Proceeds are so introduced, or placed, into the financial system, they can proceed to the next phase of the process;
- Layering. In this phase, criminals attempt to disguise the illicit nature of the Funds or Proceeds of Crime by engaging in transactions, or layers of transactions, which aim to conceal their origin. Afterwards, they can proceed to the final stage of the process;
- Integration. In this phase, criminals attempt to return, or integrate, their “laundered” Funds or the Proceeds of Crime back into the economy, or to use it to commit new criminal offences, through transactions or activities that appear to be legitimate.

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

Although the sizes of transactions related to the financing of terrorism and illegal organisations are often much smaller than those involved in ordinary money laundering operations, and some of the typologies and specific techniques used may differ, the overall principles and generic risks are the same. The terrorists and criminals involved in these acts attempt to exploit situations and factors favouring anonymity and complexity, in order

to obscure and conceal the illicit source of the Funds, or the illicit destination or purpose for which they are intended, or both.

4.3 ML/FT Typologies

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

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

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

- Transfers through traditional payment/remittance systems;
- Transfers through alternative or non-traditional payment/remittance systems;
- Physical transport, or “muling”, of cash and other stored-value systems (e.g. prepaid cards, traveller’s cheques, bank drafts, bills of exchange, or other negotiable bearer instruments);
- Purchase/sale of precious goods (for example, metals, stones, antiques, artwork, vehicles, race horses);
- Real-estate-based ML;
- Trade-based ML;
- VAT/customs duty carousel and similar fraud schemes;
- Use of business structures (for example, nominees, Legal Arrangements, shell companies, third-party intermediaries, non-profitable organisations).

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

4.4 Risk Factors

(AML-CFT Law 16.1(a)-(b); AML-CFT Decision 4.1(a))

Proper identification of risk factors is crucial to the effective implementation of a risk-based approach to assessing and mitigating ML/FT risk. Identified risk factors are used for the accurate categorisation of risks, as well as for the application of appropriate mitigation measures at both the enterprise and the customer level. At the enterprise level, this includes adopting and applying adequate policies, procedures, and controls to business processes (see Section 5.1, Internal Policies, Controls and Procedures). At the customer level, this includes assigning appropriate risk classifications to customers and applying due diligence measures that are commensurate with the identified risks (see Section 6, Customer Due Diligence).

The AML-CFT Decision outlines several risk factors which supervised institutions must consider, when identifying and assessing their ML/FT risk exposure. DNFBPs may also consider a wide array of additional risk factors, utilising risk identification methods or combinations of methods that are appropriate to their particular circumstances.

Examples of such methods include, but are not limited to:

- Checklists of ML/FT red-flag indicators;
- Input and information from relevant internal sources, including the designated AML/CFT compliance officer;
- Information from national sources, including the results of the NRA with regard to ML/FT trends and sectoral threats and notices or circulars from the relevant Supervisory Authorities;
- Information from publications of relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, UNODC, and others. (Links to some of these sources may be found in Appendix 11.2.)

In keeping with the ever-evolving nature of ML/FT risks, and in order to ensure that they implement risk models that are appropriate to the nature and size of their businesses, supervised institutions are reminded that they should continually update the risk factors which they consider, in order to reflect new and emerging ML/FT risks and typologies.

Guidance with regard to some of the major risk factors that are of particular concern to DNFBPs is provided in the sections below. Some of these risk factors contain both an enterprise-level component and a customer- or Business Relationship-specific component, and supervised institutions are reminded that they should take a holistic view when evaluating exposure to them.

4.4.1 Customer Risk

When identifying and assessing customer risk, supervised institutions should consider both enterprise-level risks and customer-specific or Business Relationship risks.

Enterprise-Level Risk

Enterprise-level, or business-level, risk factors in regard to customers relates to broad categories of customers and the supervised institution's approach to them. The various types and the extent of enterprise-level customer risk to which DNFBPs are exposed may require different levels of AML/CFT resources and mitigation strategies. Supervised institutions should therefore identify these risks in relation to their particular circumstances.

Some of the numerous enterprise-level risk factors that DNFBPs should consider are:

- Target markets. The risks related to retail customers and 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.

- Size, homogeneity and growth rates of customer base. Supervised institutions with small, homogenous customer bases may face different risks from those with larger, more diverse customer bases. Similarly, entities targeting high levels of market share growth may face different customer risks than those with less aggressive growth targets or more established customer bases.

- Business model and strength of relationship. Supervised institutions may face different levels of customer ML/FT risk, depending on how their business models impact the strength of their customer relationships. For example, entities whose business models rely on more transactional, occasional, or one-off interactions with their customers may be exposed to different risks from institutions with more repetitive or relationship-driven business models.

- IT infrastructure and management information systems (MIS) capabilities. DNFBPs should consider how well their technical infrastructure, including their data management and management information reporting capabilities, are suited to the ML/FT risk-mitigation requirements of the types of customers they deal with, particularly in respect of the size and growth dynamics of their customer base.

Enterprise-level customer risks are not limited to the above-mentioned examples. In this regard, supervised institutions should also consider the results of the NRA, with particular reference to sectoral ML/FT threats, as well as information published from time to time by official sources, including the Supervisory Authorities, the FIU, international organisations like FATF, MENAFATF and other FSRBs, the Egmont Group, and others, in order to be effective in their identification and evaluation of these enterprise-level customer risk factors.

Customer- or Business Relationship-Specific Risk

Special attention should be given to the critical role that customer-specific, or relationship-specific, risk factors play in determining DNFBPs' ML/FT risk mitigation measures, customer risk classifications, and the type and extent of customer due diligence they perform (see Section 6, Customer Due Diligence). The customer-specific risks that supervised institutions should consider include (but are not limited to):

- Complexity and transparency. Business relationships with complex legal, ownership, or direct or indirect group or network structures, or with less transparency with regard to Beneficial Ownership, effective control, or tax residency, may pose different ML/FT risks than those with simpler legal/ownership structures or with greater transparency.
- Regulation/supervision. Supervised institutions may face different risks from customers involved in highly regulated and supervised activities than from those involved in activities that are unregulated.
- Associations or linkages. Customers associated with higher-risk persons or professions (for example, foreign PEPs and/or their companies), or those linked to sectors associated with higher ML/FT risks, may expose DNFBPs to different levels of risk than customers associated with lower-risk persons and professions.

Supervised institutions should give special consideration to the results of the NRA, as well as to information published from time to time by official sources, including the Supervisory Authorities, the FIU, international organisations such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others, when identifying and assessing such customer-specific risk factors.

4.4.2 Geographic Risk

DNFBPs should consider geographic risk factors at both the enterprise and customer-specific levels. Examples of some of these factors include (but are not limited to):

- Regulatory/supervisory framework. Countries with stronger AML/CFT controls present a different level of risk than countries with weaker regulatory and supervisory frameworks.
- 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) (see Section 10, Targeted Financial Sanctions), OFAC sanctions, or EU restrictive measures, that could impact their ML/TF risk exposure and mitigation requirements.
- Reputation. Supervised institutions should consider whether the countries or jurisdictions they deal with are associated with higher or lower levels of ML/FT, corruption, and 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).

- Consistency with customer's profile. DNFBPs should consider whether the countries or jurisdictions that are associated with a customer are consistent with the customer's profile, including principal residential or operating locations and the type of business or professional activities with which the customer is involved.

4.4.3 Product-, Service-, Transaction-Related Risk

The ML/FT risks associated with product, service, and transaction types influence the kinds and levels of AML/CFT resources and mitigation strategies which supervised institutions require. When identifying and assessing these risks, supervised institutions should consider both the enterprise-level risks and customer-specific or Business Relationship risks in relation to their particular circumstances. Some of the risk factors that DNFBPs should consider, among others, are:

- Typology. Supervised institutions should consider whether the product, service, or transaction type is associated with any established ML/FT typologies (see Section 4.3, ML/FT Typologies).

- Complexity. Products, services, or transaction types that favour complexity, especially when that complexity is excessive or unnecessary, can often be exploited for the purpose of money laundering and/or the financing of terrorism or illegal organisations. 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 supervised institutions to different types and levels of ML/FT risk than those with lower complexity or with fewer dependencies on multiple systems and/or market participants.

- Transparency and transferability. Situations that favour anonymity can often be exploited for the purpose of ML/FT. Supervised institutions 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. Some of the factors which DNFBPs should consider in this regard are market size, registration or documentation requirements, operational controls, and accessibility.

- Size/value. Products, services, or transaction types with different size or value parameters or limits may pose different levels of ML/FT risk. In particular, DNFBPs should consider whether the products, services, or transaction types they deal with have adequate controls and/or management reporting thresholds with regard to intrinsic size or value, as well as in regard to changes in size or value patterns over time.

4.4.4 Channel-Related Risk

Different channels for the acquisition and management of customer relationships, as well as for the delivery of products and services, entail different types and levels of ML/FT risk. Supervised institutions should identify and evaluate these risks at both the enterprise-wide and the customer-specific levels.

When evaluating 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. Among others, these may include non-face-to-face channels, such as internet-, phone-, or other remote-access services or technologies; the use of third-party business introducers, intermediaries, agents or distributors; and the use of third-party payment, money/value transfer, or other transaction intermediaries.

4.4.5 Other Risk Factors

Given the ever-evolving nature of ML/FT risks, new risk factors 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 risk factors can ever be considered as exhaustive.

In order to ensure, therefore, that they are in a position to implement risk assessment models and mitigation measures that are appropriate to their particular circumstances, entities should take into consideration the results of the annual NRA. They should also consider consulting publications from official sources on a regular basis, including those of the relevant Supervisory Authorities, the FIU, international organisations such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others. Links to some of these sources may be found in Appendix 11.2.

Examples of some of the types of additional risk factors which DNFBPs may consider in identifying and assessing their ML/FT risk exposure include, but are not limited to the following:

- Novelty/innovation. Supervised institutions should consider the depth of experience with and knowledge of the product, service, transaction, or channel type, at both the enterprise-level (for example, with regard to operational risk) and the customer-specific level. Products, services, transaction, or channel types that are new to the market or to

the enterprise may not be as well understood as, and may therefore pose a different level of ML/TF risk than, more established ones. Likewise, products, services, transaction, or channel types which are unexpected or unusual with respect to a particular type of customer may indicate a different level of potential ML/FT risk exposure than would more traditional or expected product, service, transaction, or channel types in regard to that same type of customer.

- Cyber security/distributed networks. 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 financing of terrorism or of illegal organisations, through cyber attacks or through other means, such as the use of distributed technology or social networks. An example of such a risk is the recent dramatic increase in the global incidence of so-called CEO fraud, in which fraudsters troll companies with phishing e-mails that are purportedly from the CEO or other senior executives, and attempt to conduct fraudulent transactions or obtain sensitive data that can be used for criminal purposes.

4.5 Risk Assessment

(AML-CFT Law 16.1(a) and AML-CFT Decision 4.1)

DNFBPs are obliged to assess and to understand the ML/FT risks to which they are exposed, and how they may be affected by those risks. Specifically, the AML-CFT Law provides that they shall:

> *"…continuously assess, document, and update such assessment based on the various risk factors established in the Implementing Regulation of this Decree-Law and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority upon request."*

Furthermore, the AML-CFT Decision charges supervised institutions with:

> *"…Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request."*

A well-documented assessment of the identified risk factors (see Section 4.4, Risk Factors) is therefore fundamental to the adoption and effective application of reasonable and proportionate ML/FT risk-mitigation measures. The result of such an assessment allows for a systematic categorisation and prioritisation of inherent and residual ML/FT risks, which in turn allows supervised institutions to determine the types and appropriate levels of AML/CFT resources needed for mitigation purposes at both the enterprise and the customer levels.

An effective 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. Supervised institutions with smaller or less complex business models may have simpler risk assessments than those of institutions with larger or more complex business models, which may require more sophisticated methodologies.

However, to be effective, a risk assessment should be based on a methodology that:

- Reflects the supervised institution's management-approved risk appetite and policies;
- Takes into consideration input from relevant internal sources, including the designated AML/CFT compliance officer;
- Takes into consideration relevant information (such as ML/FT trends and sectoral risks) from external sources, including the NRA, Supervisory and other Competent Authorities, and international organisations such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others where appropriate;
- Is properly documented and maintained, regularly evaluated and updated, and communicated to relevant personnel within the organisation.

4.5.1 Documentation, Updating, and Analysis

(AML-CFT Law 16.1(a) and AML-CFT Decision 4.1(a)-(b))

Documentation

Supervised institutions are obliged to document their risk assessment operations, analysis, and supporting data, and to make them available to the Supervisory Authorities upon request. In fulfilling their statutory obligations, DNFBPs should consider incorporating into their documentation adequate information to demonstrate the effectiveness of their risk assessment processes. Examples of such information include, but are not limited to:

- Organisation's overall risk policies (for example, risk appetite statement, customer acceptance policy, and others, where applicable).
- ML/FT risk assessment policies and procedures, including such information as organisational roles and responsibilities; process flows, timing and frequency; internal reporting requirements; and review, testing, and audit requirements.
- Risk assessment model or methodology used, and records related to its evaluation, testing, and updating, as relevant.
- Risk factors identified, and input received from relevant internal sources, including the designated AML/CFT compliance officer.
- Details of the risk-factor analysis that constitutes the risk assessment.

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

Updating

DNFBPs are obliged to keep their risk assessment operations up-to-date on an ongoing basis. In fulfilling this obligation, they should consider reviewing and evaluating their ML/FT risk assessment processes, models, and methodologies periodically, in keeping with the nature and size of their businesses. Supervised institutions should also consider updating their risk assessments whenever they become aware of any internal or external events or developments which could affect their accuracy or effectiveness.

Such developments may include, among other things, changes in business strategies or objectives, technological developments, legislative or regulatory developments, or the identification of material new ML/FT threats or risk factors. In this regard, DNFBPs should take into consideration the results of the most recent NRA, as well as circulars, notifications and occasional published information from official sources, such as the Supervisory Authorities; other national Competent Authorities; or relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others. Links to some of these sources may be found in Appendix 11.2.

Analysis

A key objective of effective ML/FT risk assessment is for supervised institutions to understand the risks to which they are exposed, and how they may be affected by them. In this regard, the AML-CFT Law requires DNFBPs to “maintain a risk identification and assessment analysis with its supporting data.”

Supervised institutions may utilise a variety of models or methodologies to analyse risk, in keeping with the nature and size of their businesses. Among the elements they should consider including in their ML/FT risk assessment analyses are the following:

- Likelihood or probability of occurrence of identified risks;
- Timing of identified risks;
- Impact on the organisation of identified risks.

The result of an effective ML/FT risk assessment is often the classification of identified risks into different categories, such as high, medium, low, or some combination of those categories (such as medium-high, medium-low). Such classifications may assist DNFBPs to prioritise their ML/FT risk exposures more effectively, so that they may determine the appropriate types and levels of AML/CFT resources needed, and adopt and apply reasonable and risk-proportionate mitigation measures.

4.5.2 Assessing Enterprise Risk

(AML-CFT Law 16.1; AML-CFT Decision 4.1)

A main area of concern to DNFBPs in regard to ML/FT risk assessment is that of enterprise, or business-wide, risk. The purpose of a business-wide ML/FT risk assessment is to improve the effectiveness of ML/FT risk management, by identifying the ML/FT risks faced by the enterprise as a whole, determining how these risks are mitigated through internal policies, procedures and controls, and establishing the residual ML/FT risks that should be addressed.

Thus, an effective enterprise risk assessment can allow supervised institutions to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are appropriately aligned with residual risks.

DNFBPs should decide on both the frequency and methodology of enterprise-level ML/FT risk assessments, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/FT risks to which they are exposed, as well as the results of the NRA. In most cases, supervised institutions should consider performing such risk assessments annually; however assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. They should also decide on policies and procedures related to the periodic review of their enterprise risk assessment methodology, taking into consideration changes in internal or external factors. These decisions should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

4.5.3 Assessing Business Relationship Risk

(AML-CFT Law 16.1; AML-CFT Decision 4.1)

The accurate assessment of business relationship risk is fundamental to the risk classification of customers and the effective application of appropriate risk-based customer due diligence measures. DNFBPs should take the necessary steps to ensure that their business relationship risk assessment processes are robust and reliable, and that they incorporate the results of both the NRA and enterprise-wide risk assessments, as well as the input of relevant internal stakeholders, including the designated AML/CFT compliance officer.

In assessing business relationship risk, DNFBPs should analyse customers on the basis of the identified risk factors in order to arrive at a customer risk classification. Supervised

institutions may utilize different methodologies to accomplish their analysis and risk classification, depending on the nature and size of their businesses, and of the risks involved. For example, some entities with smaller or less complex businesses, or with more homogenous customer bases, may elect to assess business relationship risk and assign customer risk classifications on the basis of generic profiles for customers of the same type. Other larger or more complex DNFBPs may elect to assess business relationship risk and assign customer risk classifications using more sophisticated models or scorecards based on weightings of various risk factors.

Regardless of the methodologies they choose, supervised institutions should ensure that their business relationship risk assessment processes and the rationale for their methodologies are well-documented, approved by senior management, and communicated at the appropriate levels of the organisation. They should also decide on policies and procedures related to both the periodic review of their business relationship risk assessment processes, and to the frequency for updating the individual business relationship risk assessments and customer risk classifications produced by them, taking into consideration changes in internal or external factors.

4.5.4 Assessing New Product and New Technologies Risks

(AML-CFT Decision 23)

As part of their obligation to update their ML/FT risk assessments on an ongoing basis, the AML-CFT Decision specifically requires DNFBPs to "identify and assess the risks of money laundering and terrorism financing that may arise when developing new products and new professional practices, including means of providing new services and using new or under-development techniques for both new and existing products."

Supervised institutions 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 consider integrating these ML/FT risk assessment and mitigation requirements into their new product, service, channel, or technology development processes.

For the purpose of assessing the ML/FT risks associated with new products, services, practices, techniques, or technologies, DNFBPs may consider utilising the same or similar risk assessment models or methodologies as those utilised for their enterprise-wide ML/FT risk assessments, updated as necessary for the particular circumstances. They should also document the new product, service, practice, technique, or technology risk assessments, in keeping with the nature and size of their businesses (see Section 4.5.1, Documentation, Updating and Analysis).

4.5.5 Examples of Risk Assessment Operations

(AML-CFT Decision 4.1(b))

The AML-CFT Decision obliges DNFBPs to document their risk assessment operations (see Section 4.5.1, Documentation, Updating and Analysis). Supervised institutions may utilise a variety of processes in assessing their ML/FT risk. Examples of some of these risk assessment processes may include, but are not limited to:

- Obtaining and evaluating input from relevant internal sources, including the designated AML/CFT compliance officer, such as: internal meetings or interviews; internal questionnaires concerning risk identification and controls; review of internal audit reports.
- Obtaining and evaluating relevant information (such as ML/FT trends and sectoral risks) from external sources, including the NRA, Supervisory Authorities, FIU, other national Competent Authorities, and, where appropriate, international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others.
- Evaluating identified ML/FT risks against the organisation's management-approved risk appetite statement and policies.
- Determining the risk model or methodology (including understanding the risk-rating methodologies of purchased IT systems or software packages) for the weighting of risk factors, the classification of risks into different categories, and the prioritisation of risks, at both the enterprise and customer levels.
- Evaluating the likelihood or probability of occurrence of identified ML/FT risks, and determining their timing and impact on the organization.
- Determining the rationale and circumstances for approving and performing manual interventions or exceptions to model-based risk weightings or classifications.
- Testing and auditing the effectiveness and consistency of risk methodologies and their outputs with regard to statutory obligations.

DNFBPs should determine the type and extent of the risk assessment processes that they consider to be appropriate for the size and nature of their businesses, and should consider documenting the rationale for these decisions.

Part III—Mitigation of ML/FT Risks

(AML-CFT Law 16.1(b)(d); AML-CFT Decision 4.2-13, 15, 20)

DNFBPs are obliged to take the necessary measures to manage and mitigate the ML/FT risks to which they are exposed. Both the AML-CFT Law and the AML-CFT Decision provide that supervised institutions may utilize a risk-based approach with respect to mitigation of ML/FT risks.

5. Internal Policies, Controls and Procedures

(AML-CFT Law 16.1(d); AML-CFT Decision 4.2(a), 20)

The AML-CFT Law and the AML-CFT Decision require supervised institutions to implement internal policies, controls and procedures that enable them to manage and mitigate the ML/FT risks they have identified, in keeping with the nature and size of their businesses. Such policies, controls and procedures must be approved by senior management, reviewed for effectiveness and continuously updated, and must apply to all branches, subsidiaries and affiliated entities in which DNFBPs hold a majority interest (see Section 8.3, Group Oversight for more guidance). They must also take into consideration the results of the NRA.

Additionally, supervised institutions should ensure that the policies, controls and procedures they implement to manage and mitigate ML/FT risks are reasonable, proportionate to the risks involved, and consistent with the results of their risk assessments.

The internal policies, controls and procedures that DNFBPs apply to the mitigation of ML/FT risks can be categorised broadly as those related to:

- The identification and assessment of ML/FT risks (see Section 4.5, Risk Assessment).
- Customer due diligence (CDD, EDD, SDD) (see Section 6, Customer Due Diligence), including its review and updating, and reliance on third parties in regard to it.
- Customer and transaction monitoring, and the reporting of suspicious transactions (see Section 7, Suspicious Transaction Reporting).
- AML/CFT governance, including compliance staffing and training, senior management responsibilities, and the independent auditing of risk mitigation measures (see Section 8, Governance).
- Record-keeping requirements (see Section 9, Record Keeping).

Guidance in relation to these categories is provided in the above-referenced sections.

6. Customer Due Diligence (CDD)

(AML-CFT Law 16.1(b); AML-CFT Decision 4.2(b), 4.3, 5-13, 14, 15, 19, 20.1, 22, 24.2-4, 25, 27, 29.2, 30, 31.1, 35.1-2 and 5, 37.1-2, 44.10, 55.1)

6.1 Risk-Based Application of CDD Measures

The AML-CFT Law implicitly recognises the need for a RBA to customer due diligence measures, by obliging supervised institutions to "take the necessary due diligence measures and procedures and define their scope, taking into account the various risk factors and the results of the national risk assessment…." This principle is further emphasised by the AML-CFT Decision, which explicitly provides for the application of enhanced due diligence (EDD) measures to manage identified high risks (see Section 6.4, Enhanced Due Diligence (EDD) Measures), and of simplified due diligence (SDD) to manage identified low risks in the absence of a suspicion of ML/FT (see Section 6.5, Simplified Due Diligence (SDD) Measures).

DNFBPs are reminded, however, that the application of a risk-based approach to CDD measures is not to be taken as a static formula by which, for example, all medium-risk customers are necessarily always subjected to normal CDD measures and all low-risk customers are always subjected to SDD measures. Each customer's ML/FT risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behaviour, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, supervised institutions should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/FT risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/FT risk category.

6.2 Circumstances and Timing for Undertaking CDD Measures

(AML-CFT Decision 5.1)

Under normal circumstances, DNFBPs are obliged to undertake CDD measures (including verifying the identity of customers and Beneficial Owners, beneficiaries, or controlling persons) either prior to or during the establishment of a Business Relationship or the opening of an account, or prior to the execution of a transaction for a customer with whom there is no Business Relationship. Guidance in regard to these requirements and certain exceptional circumstances provided for in the AML-CFT Decision is provided in the sub-sections below.

6.2.1 Establishment of a Business Relationship

DNFBPs establish a Business Relationship with a customer when they perform any act for, on behalf of, or at the direction or request of the customer, with the anticipation that it will be of an ongoing or recurring nature, whether permanent or temporary. Such acts may include, but are not limited to:

- Assigning an account number or opening an account (including fiduciary or escrow accounts, and managed accounts held with Financial Institutions) in the customer's name;
- Effecting any transaction in the customer's name or on their behalf, or at the customer's direction or request for the benefit of someone else;
- Providing any form of tangible or intangible product or service (including but not limited to granting credits, guarantees, or other forms of value; buying, selling, or leasing physical goods or property of any kind; giving advice, counsel, information or analysis) to or on behalf of the customer, or at the customer's direction or request for the benefit of someone else;
- Signing any form of contract, agreement, letter of intent, memorandum of understanding, or other document with the customer in relation to the performance of a transaction or series of transactions, or to the provision of any form of tangible or intangible product or service as described above;
- Accepting any form of compensation or remuneration (including but not limited to a deposit, retainer fee, or other form of credit or promise of future payment) for the provision of tangible or intangible products or services, as described above, from or on behalf of the customer;
- Receiving funds or proceeds of any kind (including those held on a fiduciary basis, for safekeeping, or in escrow) from or on behalf of the customer, whether for their account or for the benefit of someone else;
- Any other act performed by supervised institutions in the course of conducting their ordinary business, when done on behalf of, or at the request or direction of, a customer.

In such cases, and other than in the exceptional circumstances described below (see Section 6.2.3, Exceptional Circumstances), DNFBPs are required to undertake appropriate risk-based CDD measures (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures for further guidance). Among other things, these measures should include verifying the identity of the customer (as well as the Beneficial Owners, beneficiaries, or controlling persons), and understanding the nature of their business and the purpose of the Business Relationship.

6.2.2 Occasional Transactions

During the course of business, DNFBPs may be called upon to perform occasional or non-recurring transactions for customers with whom there is no ongoing account or Business Relationship. Examples of such transactions include, but are not limited to:

- Sale or purchase of goods such as precious stones, metals, coins or other valuable property to or from a retail customer;
- Accepting a deposit for a real-estate purchase from a prospective buyer;
- Drafting of a Will, Trust agreement, or other legal agreement for a walk-in customer.

On such occasions, and other than in the exceptional circumstances described below (see Section 6.2.3, Exceptional Circumstances), DNFBPs are required to identify the customer and verify the customer's identity (as well as that of the Beneficial Owners, beneficiaries, or controlling persons). Furthermore, DNFBPs are required to undertake appropriate risk-based CDD measures (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures for further guidance), including among other things understanding the nature of the customer's business and the purpose of the transaction, in the cases specified in Article 6 of the AML-CFT Decision. Namely:

- When carrying out occasional transactions in favour of a Customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- When there is a suspicion of a crime (see Section 7.2, Identification of Suspicious Transactions);
- When there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Some of the indicators of transactions that may appear to be linked include, but are not limited to the following:

  - Multiple transactions with the same or similar customer reference codes;
  - Transactions executed sequentially or in close time proximity, and involving the same or related counterparties;
  - Multiple transactions attempted by a customer with whom there is no Business Relationship at different branches of the same DNFBP on the same day.

6.2.3 Exceptional Circumstances

(AML-CFT Decision 4.3, 5.1(a)-(c), 10, 11.1(b), 13.2)

From time to time, certain situations may arise which fall outside of the normal course of CDD procedural guidelines. Under these circumstances, described below, DNFBPs are permitted to handle the timing, customer identification, and other aspects of customer due diligence procedures exceptionally. Specifically:

- When there is no suspicion of criminal activity, and the ML/FT risks are identified as low, supervised institutions may complete the verification of the customer's identity after establishing the Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision. In such circumstances, the identity verification must be conducted in a timely fashion, and DNFBPs must ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefitting from the Business Relationship prior to the completion of the verification process. Examples of such measures which supervised institutions may consider taking in this regard are, among others:

  - Holding funds in suspense or in escrow until the identification verification is completed;
  - Making the completion of identification verification a condition precedent to the closing of a transaction.

- In the case of Legal Arrangements, such as Trusts or foundations, or of life insurance policies (including funds-generating transactions, such as life insurance products relating to investments and family Takaful insurance) in which there are beneficiaries who are not named, but instead belong to a designated class of future or contingent beneficiaries, DNFBPs are required to obtain sufficient information about the details of the class of beneficiaries so as to be in a position to establish the identity of each beneficiary at the time of the settlement, pay-out, or exercise of their legally acquired rights. Furthermore, supervised institutions must verify the identity of the beneficiaries at the time of settlement or pay-out and prior to the exercise of any related legally acquired rights. They should also ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefitting from the Business Relationship prior to the completion of the verification process. Examples of such measures which supervised institutions may consider taking in this regard are, among others:

  - Holding funds in suspense or in escrow until the identification verification is completed;
  - Making the completion of identification verification a condition precedent to the closing of a transaction.

- When a legal entity customer or its controlling stakeholder meets the conditions specified in Article 10.1-2 of the AML-CFT Decision with regard to publicly listed companies

(including the condition that information concerning the identity of the shareholders, partners, or Beneficial Owners with an interest of 25% or more is available from reliable sources), DNFBPs are exempted from taking the normally required identity verification measures. In this regard, supervised institutions should ensure that the disclosure and transparency requirements of the regulated stock exchange are at least equivalent to those of the State, and should consider documenting the evidence they obtain concerning the relevant disclosure/transparency requirements.

It is important to note that, while DNFBPs are exempted in such situations from verifying the identity of the shareholders, partners or Beneficial Owners (or in the event that no such person can be identified, of the relevant senior management officers), they are not exempted from ascertaining the identity of those persons. To that end, supervised institutions should consider documenting the information obtained from reliable sources which they use to identify the shareholders, partners or Beneficial Owners, as well as the sources of such information. Examples of reliable information sources in this regard include, but are not limited to:

- Stock exchange disclosure reports or websites;
- Corporate annual reports, websites, or other forms of official public disclosure;
- Official or public registries;
- Credit reporting agencies;
- Recognized, well-established media outlets.

- When DNFBPs suspect that a customer or Beneficial Owner is involved in the commitment of a crime related to money laundering, the financing of terrorism, or the financing of illegal organisations, and they have reasonable grounds to believe that undertaking customer due diligence measures would tip off the customer, then they should not apply CDD procedures, but should instead report their suspicion to the FIU along with the reasons that prevented them from carrying out CDD measures.

6.3 Customer Due Diligence (CDD) Measures

The application of risk-based CDD measures is comprised of several components, in keeping with the customer's ML/FT risk classification and the specific risk indicators that are identified. Generally, these components include, but are not limited to, the following categories:

- Identification of the customer, Beneficial Owners, beneficiaries, or controlling persons; and the verification of the identity on the basis of documents, data or information from reliable and independent sources (see Section 6.3.1, Customer and Beneficial Owner Identification/Verification).

- Background screening of the customer, Beneficial Owners, beneficiaries, or controlling persons, to screen for the applicability of targeted or other international financial

sanctions, and, particularly in higher risk situations, to identify any potentially adverse information such as criminal history (see Section 6.4, Enhanced Due Diligence (EDD) Measures).

- Obtaining an understanding of the intended purpose and nature of the Business Relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure (see Section 6.3.3, Establishing a Customer Due Diligence Profile).
- Monitoring and supervision of the Business Relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behaviour (see Section 6.3.4, Ongoing Monitoring of the Business Relationship).

In cases involving higher levels of risk, DNFBPs are generally required to exercise enhanced levels of customer due diligence, such as identifying and/or verifying the customer's source of funds and taking other appropriate risk-mitigation measures (see Section 6.4, Enhanced Due Diligence (EDD) Measures).

As part of their overall AML/CFT framework, DNFBPs should consider using a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of CDD procedures. Examples of the some of the factors they should consider include but are not limited to:

- Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships (see Section 4.5.3, Assessing Business Relationship Risk) and in assigning appropriate risk classifications;
- Circumstances, timing, and composition in regard to the application of CDD measures;
- Frequency of reviews and updates in relation to CDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which CDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, supervised institutions should consider the results of both the NRA and their own enterprise-wide ML/FT risk assessments. Commensurate with the nature and size of the DNFBPs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

Additional guidance related to these and other key aspects of risk-based CDD measures is provided in the following sub-sections.

6.3.1 Customer and Beneficial Owner Identification/Verification

(AML-CFT Decision 4.2(b), 3(a), 5.1, 8.1, 9, 10, 11.2, 13.1, 14.2)

Grounded on the principles of "Know Your Customer" and risk-based customer due diligence, the identification and ID-verification of customers is a fundamental component of an effective ML/FT risk management and mitigation programme. Within the UAE's AML/CFT legislative and regulatory framework, DNFBPs are obliged to identify customers (including the Beneficial Owners, beneficiaries, and controlling persons), whether permanent or walk-in, and whether a natural or legal person or Legal Arrangement, and to verify their identity using documents, data or information obtained from reliable and independent sources.

The specific requirements concerning the timing, extent, and methods of identifying and verifying customers and Beneficial Owners depend in part on the type of customer (whether a natural or legal person) and on the level of risk involved (also see Sections 6.4, Enhanced Due Diligence (EDD) Measures, and 6.5, Simplified Due Diligence (SDD) Measures). However, the core components of a customer's identification generally remain the same in all cases. They are:

- Personal data, including details such as the name, identification number, nationality, date and place of birth (or date and place of establishment, in the case of a legal person or arrangement); and
- Principal address, including evidence of the permanent residential address of a natural person, or the registered address of a legal person or arrangement.

In taking adequate CDD measures, DNFBPs are obliged at a minimum to identify and verify the customer as specified in the relevant articles of the AML-CFT Decision. In fulfilling these requirements, DNFBPs should consider using a risk-based approach to determine the internal policies, procedures and controls they implement in relation to the identification and verification of customers (including the Beneficial Owners, beneficiaries, and controlling persons). The policies and procedures that supervised institutions apply should be reasonable and proportionate to the risks involved, and, in formulating them, entities should consider the following guiding principles:

- The verification of a customer's identity, including their address, should be based on original, official (i.e. government-issued) documents whenever possible. When that is not possible, DNFBPs should consider augmenting the number of verifying documents or the amount of information they obtain from different independent sources. They should also

consider identifying the lack of official documents and the use of alternative means of verification as risk factors when assessing the customer's ML/FT risk classification.

- In addition to name, nationality, and place of birth, a natural person's date of birth and national identification number (or the date of establishment and registration number in the case of a legal person or arrangement) are also important elements comprising a customer's identification, which should be taken into consideration.

- With regard to the identification and verification of foreign nationals, whether customers or Beneficial Owners, beneficiaries or controlling persons, DNFBPs should consider taking steps to understand and request only those types of identification documents that are legally valid in the relevant jurisdictions. Furthermore, when verifying the identity of foreign nationals associated with high-risk factors, DNFBPs should consider validating the authenticity of customer identification documents obtained. Some of the methods that supervised institutions may consider in order to do so, commensurate with the nature and size of their businesses, include but are not limited to:

  - Contacting the relevant foreign embassy or consulate, or the relevant issuing authority;
  - Using commercially available applications to validate the information in machine-readable zones (MRZs) or biometric data chips of foreign identification documents.

- The types of address verification that may generally be considered acceptable include, but are not limited to, the following categories of documents issued in the name of the customer:

  - Bills or account statements from public utilities, including electricity, water, gas, or telephone line providers;
  - Local and national government-issued documents, including municipal tax records;
  - Registered property purchase, lease or rental agreements;
  - Documents from supervised financial institutions, such as bank statements or insurance policies.

- In addition to the identifying and verifying customers, Beneficial Owners, beneficiaries, and controlling persons, DNFBPs should verify the identity of any person legally empowered to act or transact business on behalf of the customer, whether the customer is a legal or natural person. Such persons may include, but are not limited to:

  - Signatories, or other persons with authorised remote access credentials to an account, such as internet or phone banking users;
  - Parents or legal guardians of a minor child, or legal guardians of a physically or mentally disabled or incapacitated person;
  - Attorneys or other legal representatives, including liquidators or official receivers of a legal person or arrangement.

In the event that a legally empowered representative is also a legal person or Legal Arrangement, the normal identification and verification procedures for such entities (including the identification and verification of the Beneficial Owners, beneficiaries, or controlling persons) should be applied.

- When verifying that a person purporting to act on behalf of a customer is so authorised, the following types of documents may generally be considered to be acceptable:
  - A legally valid power-of-attorney;
  - A properly executed resolution of a legal person's or Legal Arrangement's governing board or committee;
  - A document from an official registry or other official source, evidencing ownership or the person's status as an authorised legal representative;
  - A court order or other official decision.
- As part of their procedures for identifying and verifying customers, and for authenticating the original documents upon which the verification is based, DNFBPs should consider including procedures for the certification of the customer identification and address documentation they obtain. Such procedures may encompass certification by employees (for example, by including the name, title of position, date and signature of the verifying employee(s) on the copies of documents maintained on file), as well as by third parties (for example, by including the name, organization, title of position, date and signature of the verifying person, along with a statement representing that the copy of the document is a "true copy of the original"). In cases where documents are obtained from foreign sources in countries which are members of the Hague Apostille Convention, consideration should be given to requesting documents certified by Apostille seal.
- Whenever possible, and commensurate with the nature and size of their businesses, DNFBPs should consider the feasibility of incorporating the "four-eyes" principle (review by at least two people) into their procedures with regard to the verification of customer identification documentation and information, as well as with regard to the entry of the relevant data into their information systems.

6.3.2 CDD Measures Concerning Legal Persons and Arrangements

(AML-CFT Decision 8, 9, 37.1-3)

DNFBPs are obliged to undertake CDD measures concerning legal persons and Legal Arrangements, including identification and verification of the Beneficial Owners, beneficiaries, and other controlling persons, in accordance with the provisions of the AML-CFT Decision. In fulfilling these requirements, they should take the following guidance into consideration:

- Without prejudice to the provisions of Article 9.1(b) of the AML-CFT Decision, when customers that are legal persons are owned or controlled by other legal persons or Legal Arrangements (for example, when customers are subsidiaries of a parent company or a Trust), supervised institutions should make reasonable efforts to identify and verify the Beneficial Owners by looking through each layer of legal persons or Legal Arrangements until the natural persons with owning or controlling interests of 25% or more in aggregate are identified. Furthermore, in the event of multiple legal persons or arrangements with ownership or controlling interests, even where each legal person or arrangement owns or controls less than 25%, DNFBPs should consider whether there are indications that the entities may be related by common ownership, which could reach or surpass the Beneficial Ownership threshold level of 25% in aggregate.

- When undertaking CDD measures on Legal Arrangements which allow funds or other forms of assets to be added or contributed to the arrangement after the initial settlement and by any persons other than the identified settlor(s), DNFBPs should take the necessary steps to ascertain and verify the identity of such persons, and to understand the nature of their relationship with the Legal Arrangement, its settlor(s) and its beneficiaries.

- The AML-CFT Decision obliges trustees in Legal Arrangements to maintain basic information relating to intermediaries, who are subject to supervision, and service providers, including consultants, investors or investment advisors, directors, accountants and tax advisors, who have responsibilities in relation to its management. In order to understand the control structure of a customer that is a Legal Arrangement, and whether acting on behalf of the legal arrangement as trustees or in any other capacity, or dealing with the legal arrangement as a counterparty to a transaction, DNFBPs should obtain this information and include it in the customer's CDD profile. They should also give the same consideration to other forms of Legal Arrangements and their controlling persons (such as, for example, foundations, membership clubs, religious institutions, or others, along with their founders, representatives and other governing or managing officials).

6.3.4 Establishing a Customer Due Diligence Profile

(AML-CFT Decision 7.1, 8.3-4)

The AML-CFT Decision states that DNFBPs should carry out ongoing supervision of their Business Relationships, so as to be able to ensure that the transactions conducted are consistent with the information they have about the customer, the type of activity they are engaged in, the risks they entail, and, where necessary, their source of funds. Supervised institutions are also required to understand the intended purpose and nature of the Business Relationship, and, for legal persons or arrangements, the nature of the customer's business and its ownership and control structure.

In order to fulfil these obligations, supervised institutions should consider establishing a due-diligence profile for their customers, commensurate with the nature and size of their businesses, and with the types and levels of risk involved. Such profiles allow DNFBPs to compare a customer's actual activity with the expected activity more effectively, and thus contribute to their capacity to discover unusual circumstances or potentially suspicious transactions.

When dealing with higher-risk or more complex customers, in addition to the type of information referred to above, DNFBPs may consider obtaining and including in the CDD profile more detailed information about their customers' activities, such as (but not limited to):

- Anticipated size and/or turnover of account balances or transactional activity;
- Expected types and volumes of transactions;
- Known or expected counterparties or third-party intermediaries with whom the customer conducts transactions;
- Known or expected locations related to transactional activity;
- Anticipating timing or seasonality of transactional activity.

Where lower-risk customers are concerned, DNFBPs may consider applying more generic due-diligence profiles in order to compare actual and expected types and levels of activity.

Where legal persons or arrangements are concerned, DNFBPs are obliged to identify any natural person who owns or controls an interest of 25% or more. In order to achieve an effective understanding of the ownership and control structure of a customer that is a legal person or arrangement, supervised institutions should consider obtaining from the customer and including in the profile a detailed explanation or a diagrammatical chart providing the details of any ownership interests of 25% or more, and tracing them through any intermediate legal owners (whether legal persons or arrangements, or natural persons who are nominee stakeholders) to the natural persons who ultimately own or control them.

Furthermore, in order to understand the nature of the business of a legal person or Legal Arrangement, DNFBPs should consider obtaining and including in the profile a detailed explanation or diagrammatical chart showing the entity's internal management structure, identifying the persons holding senior management positions, or other positions of control. They should also consider obtaining information about the legal person's or arrangement's majority-owned or controlled operating subsidiaries, including the nature of the business and the operating locations of those subsidiaries.

6.3.5 Ongoing Monitoring of the Business Relationship

(AML-CFT Decision 4.2(b), 4.3(c), 7.1)

With regard to established Business Relationships, DNFBPs are obliged to undertake ongoing supervision of customers' activity, including auditing transactions executed throughout the course of the relationship to ensure that they are consistent with the information, types of activity, and risk profiles of the customers. Supervised institutions should consider using a risk-based approach to determine the policies, methods, procedures and controls they implement in relation to customer monitoring activities, as well as in regard to the extent of monitoring for specific customers or categories of customers.

As part of a risk-based approach to AML/CFT, in the case of customers or Business Relationships identified as high risk, DNFBPs are expected to investigate and obtain more information about the purpose of transactions, and to enhance ongoing monitoring and review of transactions in order to identify potentially unusual or suspicious activities. In the case of customers or Business Relationships that are identified as low risk, DNFBPs may consider monitoring and reviewing transactions at a reduced frequency.

Thus, in keeping with the level of risk involved, supervised institutions should consider evaluating the specifics of the transactions examined in relation to the customer's due diligence information or profile (see Section 6.3, Customer Due Diligence (CDD) Measures, Section 6.4, Enhanced Due Diligence (EDD) Measures, and Section 6.5, Simplified Due Diligence (SDD) Measures), and should also consider obtaining sufficient information on the counterparties and/or other parties involved (including but not limited to information from public sources, such as internet searches), in order to determine whether the transactions appear to be:

- Normal (consideration should be given as to whether the transactions are typical for the customer, for the other parties involved, and for similar types of customers);
- Reasonable (consideration should be given as to whether the transactions have a clear rationale and are compatible with the types of activities that the customer and the counterparties are usually engaged in);
- Legitimate (consideration should be given as to whether the customer and the counterparties are permitted to engage in such transactions, such as when specific licenses, permits, or official authorisations are required).

Examples of some of the methods that may be employed for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;

- Transaction-based rules, in which a certain percentage (or even all) of the transactions of a certain type are examined;
- Location-based rules, in which a certain percentage (or even all) of the transactions involving a specific location (either as origin or destination) are examined;
- Customer-based rules, in which a certain percentage (or even all) of the transactions of particular customers are examined.

DNFBPs may consider using all or any combination of the above methods, or any others that are appropriate to their particular circumstances, to effect ongoing monitoring of the Business Relationship. Furthermore, monitoring procedures may be automated, semi-automated, or manual, depending on the nature and size of their businesses. Whichever methods they elect to use, however, supervised institutions should consider documenting them (see Section 9, Record Keeping), obtaining senior management approval for them, and periodically reviewing and updating them to ensure their effectiveness. They should also consider establishing specific monitoring procedures for customers and business relationships which have been reported as suspicious to the FIU (see Section 7.11, Handling of Transactions and Business Relationships after Filing of STRs).

6.3.6 Reviewing and Updating the Customer Due Diligence Information

(AML-CFT Decision 4.2(b), 4.3(b), 7.2, 12)

The timely review and update of customer due-diligence information is a fundamental component of an effective ML/FT risk management and mitigation programme. DNFBPs are obliged to maintain the due-diligence documents, data and information obtained on customers, and on their Beneficial Owners or beneficiaries in the case of legal persons or arrangements, up to date. The AML-CFT Decision provides that supervised institutions should update the CDD information on High Risk Customers more systematically, and that, in the absence of the suspicion of a crime, they may update those of identified low-risk customers less frequently.

In order to meet this obligation, DNFBPs should consider using a risk-based approach to determine the internal policies, procedures and controls they implement in relation to the review and updating of customer due diligence records. The policies and procedures that supervised institutions apply should be reasonable and proportionate to the risks involved, and, in formulating them, entities are advised to consider parameters such as (but not limited to):

- Circumstances, timing and frequency of customer due diligence reviews and updates. Generally, DNFBPs should consider establishing clear rules with respect to the maximum period of time that should be allowed to elapse between regular due-diligence reviews/updates of customer records for Business Relationships in different risk

categories. Additionally, consideration should be given to establishing clear rules with respect to circumstances that would trigger an interim or special review, or the acceleration of a particular customer's review cycle. Such circumstances might include, but are not necessarily limited to:

- Discovery of information about a customer that is either contradictory or otherwise puts in doubt the appropriateness of the customer's existing risk classification or the accuracy of previously gathered due-diligence data;
- Expiry of a customer's or Beneficial Owner's identification documents;
- Material change in ownership, legal structure, or other relevant data (such as name, registered address, purpose, capital structure) of a legal person or arrangement;
- Initiation of legal or judicial proceedings against a customer or Beneficial Owner;
- Finding materially adverse information about a customer or Beneficial Owner, such as media reports about allegations or investigations of fraud, corruption or other crimes;
- Qualified opinion from an independent auditor on the financial statements of a legal entity customer;
- Transactions that indicate potentially unusual or suspicious patterns of activity.

- Components and extent of review/updates. In keeping with the nature and size of their businesses, DNFBPs should consider clearly defining the contents of customer due-diligence reviews for Business Relationships in different risk categories, including which data elements, documents, or information should be examined and updated if necessary. (In this regard, supervised institutions are advised that, in some cases, productivity tools such as checklists and internal procedural manuals may help to enhance the effectiveness of customer due-diligence reviews and updates.) They may also consider establishing protocols with regard to the extent of the review and examination of due-diligence information for Business Relationships in different risk categories. Examples of such protocols might include, but are not necessarily limited to:

  - When the source of wealth/funds of a customer should be verified;
  - When additional inquiries or investigations should be made pertaining to the nature of a customer's business, the purpose of a Business Relationship, or the reasons for a transaction;
  - How much of a customer's transactional history, including how many and which specific transactions or transaction types, should be reviewed as part of a regular periodic or an interim review.

- Organisational roles and responsibilities. In keeping with the nature and size of their businesses, DNFBPs should consider clearly defining the relevant organisational arrangements in relation to the customer due-diligence review/update process. Examples of such roles and responsibilities might include, but are not necessarily limited to:

  - Carrying out reviews/updates;

- Escalating and/or reporting situations in which risk classifications should be changed, Business Relationships should be suspended or terminated, or unusual or potentially suspicious activities should be further investigated;
- Approving or rejecting reviews of Business Relationships (including senior management involvement with regard to PEPs and other High Risk Customers);
- Undertaking CDD file remediation measures as may be necessary;
- Auditing the quality of customer due-diligence reviews/updates;
- Maintaining records with regard to customer due-diligence reviews/updates, in accordance with statutory record-keeping requirements (see Section 9, Record Keeping).

6.4 Enhanced Due Diligence (EDD) Measures

(AML-CFT Decision 4.2(b), 7.2, 15, 22, 25)

In keeping with a risk-based approach to customer due diligence, DNFBPs are obliged to enhance their customer due diligence measures with regard to customers identified as high-risk, including the specific categories of customer as provided for in the relevant articles of the AML-CFT Decision, such as politically exposed persons (PEPs) (see Section 6.4.1, Requirements for Politically Exposed Persons), customers associated with high-risk countries (see Section 6.4.3, Requirements for High-Risk Countries), and correspondent banking institutions (see Section 6.4.4, Requirements for Correspondent Relationships).

In addition to applying EDD in cases of identified High Risk Customers, DNFBPs should also apply it in any situation in which there are doubts about the accuracy or appropriateness of a customer's ML/FT risk classification, or in which there are red-flag indicators of potentially unusual or suspicious activity. In all cases in which EDD is applied, supervised institutions should ensure that they take reasonable measures to obtain adequate information about the customer, commensurate with the level of the risks identified.

As part of their overall AML/CFT framework, DNFBPs should consider using a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of EDD procedures. Examples of the some of the factors they should consider include but are not limited to:

- Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships (see Section 4.5.3, Assessing Business Relationship Risk) and in assigning appropriate risk classifications, especially with regard to high-risk categories;
- Circumstances, timing, and composition in regard to the application of EDD measures;
- Frequency of reviews and updates in relation to customer EDD information;

- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which EDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, supervised institutions should consider the results of both the NRA and their own enterprise-wide ML/FT risk assessments. Commensurate with the nature and size of the DNFBPs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

Generally speaking, EDD involves a more rigorous application of customer due diligence measures, including, but not limited to, such elements as:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to customer identity;
- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- Increased supervision of the Business Relationship, including the requirement for higher levels of management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

Additional guidance regarding the application of EDD measures to statutory high-risk Business Relationship categories is provided in the following sub-sections.

6.4.1 Requirements for Politically Exposed Persons (PEPs)

(AML-CFT Decision 15)

Due to their potential ability to influence government policies, determine the outcome of public funding or procurement decisions, or obtain access to public funds, politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. The AML-CFT Law and the AML-CFT Decision define PEPs as:

> *"Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following:*

- *Direct family members (of the PEP, who are spouses, children, spouses of children, parents).*
- *Associates known to be close to the PEP, which include:*
  - *Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP.*
  - *Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.*

In addition to undertaking normal customer due diligence procedures, DNFBPs are obliged to put in place appropriate risk management systems to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP. They are also required to take reasonable measures to establish the source of funds of customers and Beneficial Owners identified as PEPs. In this regard, and commensurate with the nature and size of their businesses, supervised institutions should consider taking measures that include, but are not limited to:

- Implementing automated AML/CFT filtering systems which screen customer and transaction information for matches with known PEPs;
- Incorporating thorough background searches into their CDD and EDD procedures, using tools such as:
  - Manual internet search protocols;
  - Public or private databases;
  - Publicly accessible or subscription information aggregation services;
  - Commercially available background investigation services.

If a customer (or Beneficial Owner, beneficiary, or controlling person) is identified as a PEP, DNFBPs are required to take reasonable measures to establish the PEP's source of funds. In this regard, they should also evaluate the legitimacy of the source of funds, including making reasonable investigations into the individual's professional and financial background prior to becoming a PEP, if necessary.

Furthermore, DNFBPs are also required to obtain senior management approval before establishing a Business Relationship with a PEP, or before continuing an existing one. In regard to the latter, senior management should be notified and their approval should be obtained for the continuance of a PEP relationship each time any of the following situations occur:

- An existing customer (or Beneficial Owner, beneficiary, or controlling person) becomes, or is newly identified as, a PEP;

- An existing PEP Business Relationship is reviewed and the customer due diligence information is updated, either on a periodic or an interim basis, according to the organisation's internal policies and procedures;
- A material transaction that appears unusual or out-of-pattern for the Business Relationship is identified in relation to a PEP;
- The beneficiary or Beneficial Owner of a life insurance policy or family *takaful* insurance policy is identified as a PEP, in which case the overall Business Relationship should also be thoroughly examined and consideration given to filing a STR.

With regard to identified Domestic PEPs and individuals who were previously (but are no longer) entrusted with prominent functions at international organisations, the AML-CFT Decision provides that DNFBPs should implement the measures described above when, apart from their PEP status, the Business Relationships associated with such persons could be classified as high-risk for any other reason.

6.4.2 EDD Measures for High-Risk Customers or Transactions

(AML-CFT Decision 4.2(b))

DNFBPs are obliged to apply EDD measures to manage and mitigate the risks associated with identified High Risk Customers and/or transactions. The AML-CFT Decision defines a High Risk Customers as including those who represent a risk:

> *"…either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a customer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party..."*

Examples of the EDD measures that should be taken by supervised institutions are laid out in the relevant article of the AML-CFT Decision. When carrying out such measures (especially as regards obtaining and investigating more information about the nature of the customer's business, purpose of the Business Relationship, or reason for the transaction), DNFBPs should pay particular attention to the reasonableness of the information obtained, and should evaluate it for possible inconsistencies and for potentially unusual or suspicious circumstances. Examples of factors that supervised institutions should take into consideration in this regard include, but are not limited to:

- The reason for a foreign customer's or Beneficial Owner's presence, or establishment of a Business Relationship, in the UAE;
- Consistency between the nature of the customer's business and transactions and the customer's or Beneficial Owner's professional background and employment history (in

regard to which DNFBPs may find it helpful to obtain background information from reliable and independent sources, as well as from internet and social media searches, and from the customer's or Beneficial Owner's CV);

- The level of complexity and transparency of the customer's transactions (and/or legal structure, where legal persons or arrangements are concerned), especially in comparison with the customer's or Beneficial Owner's educational and professional background;
- The nature of any other business interests of (including any other legal persons or arrangements owned or controlled by) the customer or Beneficial Owner;
- Consistency between the customer's line of business and that of the counterparty to the customer's transactions (as identified, for example, through internet searches).

Additionally, and commensurate with the nature and size of their businesses, when carrying out EDD measures in respect of High Risk Customers or Beneficial Owners, DNFBPs should consider taking appropriate risk-mitigation measures such as, but not limited to:

- Performing background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information;
- Using more rigorous methods for the verification of the customer's or Beneficial Owner's identity in regard to High Risk Customers (see Section 6.3.1, Customer and Beneficial Owner Identification/Verification for more information).

6.4.3 Requirements for High-Risk Countries

(AML-CFT Law 16.1(e); AML-CFT Decision 22, 44.7, 60)

DNFBPs are obliged to implement EDD measures commensurate with the ML/FT risks associated with Business Relationships and transactions with customers (and, in the case of legal persons and arrangements, their Beneficial Owners, beneficiaries and other controlling persons) from high-risk countries. Examples of some of the measures supervised institutions should consider applying in this regard include, but are not limited to:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;
- More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;

- Increased investigation to ascertain whether the customers or related persons (Beneficial Owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPs;
- Increased supervision of the Business Relationship, including the requirement for higher levels of internal reporting and management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

Additionally, DNFBPs are obliged to implement all specific CDD measures regarding High Risk Countries as defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, including those related to the implementation of the decisions of the UN Security Council under Chapter VII of the Charter of the United Nations, the *International Convention for the Suppression of the Financing of Terrorism* and the *Treaty on the Non-Proliferation of Nuclear Weapons*, and other related directives (see Section 10, International Financial Sanctions).

In order to fulfil these obligations, and commensurate with the nature and size of their businesses and the risks involved, DNFBPs should consider establishing adequate internal policies, procedures and controls in relation to the application of EDD measures to customers and Business Relationships associated with high-risk countries. Some of the factors to which supervised institutions should give consideration when formulating such policies, procedures and controls, include but are not limited to the following:

- The organisation’s risk appetite and customer acceptance policies pertaining to Business Relationships involving high-risk countries;
- Methodologies and procedures for assessing and categorising country risk, and identifying high-risk countries (in addition to the statutorily defined High Risk Countries);
- Determination and implementation of appropriate risk-based controls (for example, certain product or service restrictions, transaction limits, or others) with regard to customers and Business Relationships associated with high-risk countries;
- Organisational roles and responsibilities in relation to the monitoring, management reporting, and risk management of high-risk country Business Relationships;
- Appropriate procedures for the enhanced investigation of Business Relationships involving high-risk countries in relation to their assessment for possible PEP associations;
- Independent audit policies in respect of EDD procedures pertaining to customers and Business Relationships involving high-risk countries, and the business units that deal with them.

6.4.4 Requirements for Money or Value Transfer Services

(AML-CFT Decision 26, 30)

As part of a risk-based AML/CFT approach, DNFBPs that enter into or maintain Business Relationships with Money or Value Transfer Services (MVTSs), including *Hawalar* services, should take adequate CDD measures that are commensurate with the risks involved (see Sections 6.3, Customer Due Diligence (CDD) Measures and 6.4, Enhanced Due Diligence (EDD) Measures). Examples of measures that supervised institutions should consider in this regard include, but are not limited to:

- Ensuring that the MVTS is properly licensed or registered;
- Obtaining information about and assessing the adequacy of the MVTS's AML/CFT policies, procedures and controls, including those related to Wire Transfers as stipulated in the relevant provisions of the AML-CFT Decision;
- Obtaining the MVTS's list of agents, and identifying and assessing the associated ML/FT risks, especially with regard to high-risk countries or other identified high-risk factors;
- Obtaining sufficient information about the MVTS's ownership and management structure (including taking into consideration the possibility of PEP involvement), the nature and scope of its business, the nature of its customer base, and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks.

DNFBPs that enter into or maintain relationships with MTVSs should also consider using a risk-based approach to determine the appropriate internal AML/CFT policies, procedures and controls they implement in relation to the risk assessment, risk classification, and the type and extent of customer due diligence they perform on them. The policies and procedures that supervised institutions apply should be reasonable and proportionate to the risks involved, and should be adequately documented, senior management approved, and communicated to the relevant employees of the organisation.

6.4.5 Requirements for Non-Profit Organisations

Non-Profit Organisations can often pose increased risks in regard to money laundering, the financing of terrorism, and the financing of illegal organisations. As part of an effective risk-based approach to AML/CFT, DNFBPs that enter into or maintain Business Relationships with non-profit organisations (NPOs) should take adequate CDD measures that are commensurate with the risks involved (see Sections 6.3, Customer Due Diligence (CDD) Measures and 6.4, Enhanced Due Diligence (EDD) Measures). Examples of measures that supervised institutions should consider include, but are not limited to:

- Ensuring that the NPO is properly licensed or registered;

- Obtaining information about and assessing the adequacy of the NPO's AML/CFT policies, procedures and controls;
- Obtaining sufficient information about the NPO's legal, regulatory and supervisory status, including requirements relating to regulatory disclosure, accounting, financial reporting and audit (especially where community/social or religious/cultural organisations are involved, and when those organisations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason);
- Obtaining sufficient information about the NPO's ownership and management structure (including taking into consideration the possibility of PEP involvement); the nature and scope of its activities; the nature of its donor base, as well as of that of the beneficiaries of its activities and programmes; and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks;
- Performing thorough background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) on the NPO's key persons, such as senior management, branch or field managers, major donors and major beneficiaries, to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information.

DNFBPs that enter into or maintain relationships with NPOs should also consider using a risk-based approach to determine the appropriate internal AML/CFT policies, procedures and controls they implement in relation to the risk assessment, risk classification, and the type and extent of customer due diligence they perform on them. The policies and procedures that supervised institutions apply should be reasonable and proportionate to the risks involved, and should be adequately documented, senior management approved, and communicated to the relevant employees of the organisation.

6.5 Simplified Due Diligence (SDD) Measures

(AML-CFT Decision 4.3, 5, 10)

In keeping with a risk-based approach to customer due diligence, under certain circumstances and in the absence of the suspicion of criminal activity, DNFBPs are permitted to exercise simplified customer due diligence measures (SDD) with regard to customers identified as low-risk.

SDD generally involves a more lenient application of certain aspects of customer due diligence measures, including, but not limited to, such elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification;

- Fewer and less detailed inquiries in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;

- More limited supervision of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

Specifically, the AML-CFT Decision permits the application of SDD in the following circumstances:

- Identified low-risk customers. When the customer or Beneficial Owner is identified as posing a low risk of ML/FT, DNFBPs are permitted to complete the verification of their identity after the establishment of a Business Relationship under the conditions specified in the relevant provisions of the AML-CFT Decision. In this regard, supervised institutions are required to implement appropriate and effective measures to control the risks of ML/FT, including the risks in regard to the customer or Beneficial Owner benefitting from the Business Relationship prior to the completion of the verification process. Examples of such measures which supervised institutions may consider taking in this regard are, among others:

  - Holding funds in suspense or in escrow until the identification verification is completed;
  - Making the completion of identification verification a condition precedent to the closing of a transaction.

  It should be noted that the provision allowing a relaxation of the timing for the completion of the identification verification procedures does not imply that DNFBPs are permitted to establish a Business Relationship without any customer identification at all. On the contrary, in all cases, the basic identification information in relation to the customer (whether a natural or legal person or arrangement) should be obtained; however under the specified conditions, supervised institutions are permitted to establish the Business Relationship prior to the completion of the verification process, which may include (but is not limited to) such steps as: obtaining appropriate supporting documentation, certifications or attestations, when necessary (for example, as regards the corporate documents of a legal person); or obtaining all the necessary information related to the relevant parties of a legal person or Legal Arrangement, such as Beneficial Owners, settlors, trustees or executors, protectors, beneficiaries, or other controlling persons.

- Listed companies. DNFBPs are exempted from identifying and verifying the identity of any shareholder, partner or Beneficial Owner of a legal person under the conditions specified in the relevant provisions of the AML-CFT Decision. Namely:

  - When the relevant identity information is obtained from reliable sources; and
  - When the customer, or the owner holding the controlling interest of the customer, is a company listed on a regulated stock exchange subject to adequate disclosure and

transparency requirements related to Beneficial Ownership; or when the customer, or the owner holding the controlling interest of a legal entity customer, is the majority-held subsidiary of such a listed company.

Without prejudice to the above, in the case of foreign stock exchanges, DNFBPs should consider taking steps to adequately assess and document the relevant disclosure and transparency requirements related to Beneficial Ownership, and to ensure that they are at least equivalent to those of the UAE.

As part of their overall AML/CFT framework, DNFBPs should consider using a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of SDD procedures. Examples of the some of the factors they should consider include but are not limited to:

- Procedures and methodologies they implement in analysing and assessing the ML/FT risk of Business Relationships (see Section 4.5.3, Assessing Business Relationship Risk) and in assigning appropriate risk classifications, especially with regard to low-risk categories;
- Circumstances, timing, and composition in regard to the application of SDD measures;
- Frequency of reviews and updates in relation to customer SDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which SDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, supervised institutions should consider the results of both the NRA and their own enterprise-wide ML/FT risk assessments. Commensurate with the nature and size of the DNFBPs' businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

6.6 Reliance on a Third Party

(AML-CFT Decision 19)

Under certain conditions, the AML-CFT Decision permits DNFBPs to rely on third parties to undertake the required customer due-diligence measures, including those measures specifically laid out in regard to identified high-risk countries (see Section 6.4.3, Requirements for High-Risk Countries), with the responsibility for the validity of the measures resting directly with the supervised institutions. Among the conditions set forth in the AML-CFT Decision concerning the reliance on third parties, it is stipulated that DNFBPs shall:

"Ensure that the third party is regulated and supervised, and adheres to the CDD measures towards Customers and record-keeping provisions of the present Decision."

In order to fulfil this obligation, DNFBPs that rely on third parties to undertake CDD measures on their behalf should implement adequate means, in keeping with the nature and size of their businesses, to ensure the third party's adherence to the requirements of the AML-CFT Law and the AML-CFT Decision in relation to customer due-diligence measures. Examples of such means include, but are not limited to:

- Clearly defined procedures for determining the adequacy of a third-party's CDD measures, including the evaluation of such factors as the comprehensiveness and quality of its policies, procedures and controls; the number of personnel dedicated to customer due-diligence; and its audit and/or quality assurance policies in regard to CDD. (In this regard, supervised institutions are advised that tools such as questionnaires, scorecards, and on-site visits may be useful in evaluating the adequacy of a third party's adherence.)
- Service-level agreements, clearly setting out the roles and responsibilities of the parties and specifying the nature of the CDD and record-keeping requirements to be fulfilled.
- Protocols for the certification by third parties of documents and other records pertaining to the CDD measures undertaken.

In addition to the above, when relying on foreign third parties for the undertaking of CDD measures, DNFBPs should take steps to ensure that the AML/CFT regulatory and supervisory framework under which the third party operates is at least equivalent to that of the State.

Whichever methods are utilized to ensure the adherence of third parties to the statutory CDD and record-keeping requirements, supervised institutions should consider documenting and periodically reviewing them for effectiveness, as part of their overall framework of internal policies, procedures and controls. Furthermore, they should consider documenting the rationale for their assignment of relevant customer risk classifications, as well as their evaluation/analysis of the CDD records obtained from the third parties on which it is based.

Reliance on a third party refers to a DNFBP's delegation to a third party of the entire CDD process, including the identification and verification of customers and Beneficial Owners, beneficiaries or controlling persons of legal entities or arrangements, as well as the investigation and assembly on behalf of the supervised institution of other relevant customer documents, information and data, as per the statutory CDD and record-keeping requirements.

For the purpose of this guidance, it is important to note that supervised institutions are expected to use documents, data or information from reliable and independent sources in

carrying out their CDD obligations, which include, among other things, verifying the identity of customers and Beneficial Owners, beneficiaries or controlling persons of legal entities or arrangements. Supervised institutions are reminded that simply obtaining CDD documents and supporting information from reliable and independent sources during the course of performing their own CDD procedures is not necessarily considered as reliance on a third party.

Reliable and independent sources may include, but are not necessarily limited to, official bodies such as Competent Authorities, governmental departments or agencies, governmental or state-sponsored business registries, public utilities or similar official enterprises; as well as non-official organisations, such as publicly accessible free or subscription information aggregation services, credit reporting agencies, and others.

Without prejudice to the above, on occasion DNFBPs that do not rely entirely on a third party for undertaking CDD measures on their behalf may, during the course of carrying out their own due-diligence procedures, receive certain documents, information or data from a third-party FI or DNFBP. In such cases, supervised institutions should consider obtaining evidence of the third party's regulatory and supervisory status and good standing, and they should also consider obtaining the third party's certification that any CDD documents provided by them (such as, but not limited to, identification documents, proof of address, or documents corroborating a customer's source of funds) are true copies of the originals.

Part IV—AML/CFT Administration and Reporting

7. Suspicious Transaction Reporting

(AML-CFT Law 9.1, 15, 30; AML-CFT Decision 16-18)

Under the AML/CFT legislative and regulatory framework of the UAE, all DNFBPs, with few exceptions (see Section 7.6, Specific Exemption from the Reporting Requirement), are obliged to report to the Financial Intelligence Unit (FIU) suspicious transactions (STRs) and any additional information required in relation to them, and also to maintain up-to-date indicators that can be used to identify the suspicion of a crime involving ML/FT.

In order to fulfil these obligations, supervised institutions should implement adequate internal policies, procedures and controls in relation to the identification and reporting of suspicious transactions. The following sub-sections provide additional guidance in this regard.

7.1 Role of the Financial Intelligence Department

(AML-CFT Law 9-10; AML-CFT Decision 13, 16, 17.1, 21.2 and 5, 40-43, 46.1-4, 49.2-3)

The FIU of the UAE is the **Financial Intelligence Department** of the Central Bank of the UAE. Established within the premises of the Central Bank, the FIU operates independently by legal and regulatory mandate as the central national agency with sole responsibility for performing the following functions:

- Receiving and analysing Suspicious Transactions Reports from FIs and DNFBPs, and disseminating the results of its analysis to the Competent Authorities of the State;
- Receiving and analysing reports of suspicious cases from the Federal Customs Authority;
- Requesting additional information and documents relating to STRs, or any other data or information it deems necessary to perform its duties, from FIs, DNFBPs, and Competent Authorities, including information relating to customs disclosures;
- Cooperating and coordinating with Supervisory Authorities by disseminating the outcomes of its analysis, specifically with respect to the quality of STRs, to ensure the compliance of FIs and DNFBPs with their statutory AML/CFT obligations;
- Sending data relating to STRs and the outcomes of its analyses and other relevant data, including information obtained from foreign FIUs, to national Law Enforcement Authorities, prosecutorial authorities and judiciary authorities when actions are required by those authorities in relation to a suspected crime;

- Exchanging information with its counterparts in other countries, with respect to STRs or any other information to which it has access.

Under the aegis of the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, and for the effective performance of its functions, the FIU maintains operational protocols with numerous national and international Competent Authorities. The Competent Authorities with which the FIU has information-sharing mechanisms in place include, among others, the following (in alphabetical order):

- ADGM (Abu Dhabi Global Market);
- Abu Dhabi Police General Headquarters;
- Dubai Financial Services Authority (DIFC);
- Dubai Gold and Commodities Exchange (DGCX);
- Dubai International Financial Centre;
- Dubai Multi Commodities Centre (DMCC);
- Dubai Police General Headquarters;
- Federal Customs Authority;
- Securities and Commodities Authority;
- Sharjah Police General Directorate.

Additionally, the FIU has been a member of the Egmont Group of Financial Intelligence Units since 2002, and maintains operational protocols for the international exchange of information with at least 45 other Financial Intelligence Units from around the world.

The types of information which the Financial Intelligence Department exchanges with other national and international Competent Authorities include, among others:

- Database search enquiries;
- Search and Freeze requests;
- Requests pertaining to the implementation of UN Security Council Resolutions (see Section 10.1, Targeted Financial Sanctions);
- Mutual Legal Assistance requests with international law enforcement/judicial authorities.

The Financial Intelligence Department thus links the public and private sectors in combating money laundering, the financing of terrorism and illegal organisations, as well as the proliferation of weapons of mass destruction. It also provides training, technical assistance

and guidance on evolving standards and best practices to all stakeholders within the UAE for the strengthening of the country's AML/CFT framework.

7.2 Processing of STRs by the FIU

(AML-CFT Law 9-10; AML-CFT Decision 42, 43.1-3, 49.3)

A core function of the FIU is to conduct operational analysis on STRs and information received from FIs, DNFBPs, as well as from Competent Authorities, and to support the investigations of Law Enforcement Authorities. It does so by identifying specific targets (such as persons, funds, or criminal networks) and by following the trail of specific transactions in order to determine the linkages between those targets and the possible proceeds of crime, money laundering, predicate offences and terrorist financing.

Upon the receipt of STRs or information from reporting institutions or other sources, the FIU assess the information, prioritises the risk, and performs its own analyses using a variety of information sources and analytical techniques. Examples of sources of information the FIU utilises include, but are not limited to:

- Sanctions screening software, such as World Check;
- Exchange Houses' Remittance Reporting System;
- Central Bank's customer accounts and transactional systems databases;
- Databases of Competent Authorities, including the Federal Customs Authority's Cash Declaration System;
- Information received from foreign FIUs, Competent Authorities and/or Law Enforcement Authorities;
- Internet searches, media reports and other public information.

In certain cases, the FIU may request additional information from the reporting entity, Competent Authorities, or even from other supervised institutions which also have a business relationship with the subject of its analysis or investigation, through the Integrated Enquiries Management System (IEMS). Upon concluding its analysis or investigation, the FIU may disseminate information about the case to Law Enforcement Authorities or foreign FIUs, and may, at its own discretion, also provide feedback to the reporting entity in the form of instructions regarding required actions to be taken, or recommendations and guidance.

In addition to the above, the FIU also performs strategic analysis, using data aggregated from the STRs and other information it receives, including from national and international Competent Authorities and FIUs of other countries, to identify trends and patterns relating to ML/FT. As a result of this analysis, it may from time to time disseminate enhanced due

diligence and fraud alerts to DNFBPs as a preventive measure, and may also disseminate information to supervised institutions about prevalent or new and emerging ML/FT typologies, or other specific risks which DNFBPs should take into consideration.

7.3 Meaning of Suspicious Transaction

(AML-CFT Law 16; AML-CFT Decision 17.1)

Within the meaning of the AML-CFT Law and its implementing AML-CFT Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds which 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 the financing of illegal organisations;
- Being intended to be used in an activity related to such crimes.

It should be noted that the only requirement for a transaction to be considered as suspicious is “reasonable grounds” in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators, behavioural patterns, or customer due-diligence information, and it is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved.

DNFBPs should also note that transactions need not be in progress or pending completion in order to be considered as suspicious. Even past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

7.4 Identification of Suspicious Transactions

(AML-CFT Decision 16)

DNFBPs are obliged to put in place indicators that can be used to identify the suspicion of a crime involving ML/FT, and to update those indicators on an ongoing basis in accordance with the instructions of the Supervisory Authorities or the FIU, as well as in keeping with relevant developments concerning ML/FT typologies. Supervised institutions should also consider the results of both the NRA and their own ML/FT risk assessments in this regard.

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

When identifying suspicious transactions, DNFBPs, and their management and employees, should be aware of the facts that, in relation to ML/FT crimes, there is no minimum threshold or monetary value for reporting, and that no amount or transaction size should be considered too small for suspicion. This is of particular significance where the crimes of the financing of terrorism and of illegal organisations is concerned, since typologies related to them may often involve very small amounts of money.

Furthermore, with the exception of obligatory indicators for which reporting is required by the relevant Supervisory Authorities or the FIU, DNFBPs should also note that the presence of an *indicator* of suspicion does not necessarily always mean that a transaction *is* suspicious and needs to be reported. When determining whether a transaction is suspicious, supervised institutions 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 due diligence profile. In some cases, patterns of activity or behaviour that might be considered as suspicious in relation to a specific customer or a particular product type, might not be suspicious in regard to another. For this reason, clear internal policies and procedures with regard to alert escalation and internal suspicious transaction reporting are critical to an effective ML/FT risk-mitigation programme.

While it is impossible to list all the indicators of suspicion in these Guidelines, some useful links to sources of AML/CFT suspicious transaction indicators are provided in Appendix 11.2, Useful Links. A few examples of potentially suspicious transaction types that DNFBPs should take into consideration include:

- Transactions or series of transactions that appear to be unnecessarily complex, that making it difficult to identify the Beneficial Owner, or that do not appear to have a discernible economic 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 far larger than a customer's declared income or turnover;
- Large unexplained cash deposits and/or withdrawals, especially when they are inconsistent with the nature of the customer's business;
- Changes in ownership of legal entities, real estate, or other high-value assets without a clear economic rationale, and/or involving third parties to the transaction whose source of funds is unclear or dubious, and/or with documentation that appears to lack substance or to be fraudulent or forged;
- Transactions involving payments to or from third parties whose relationship with the customer and/or whose source of funds is unclear or dubious;
- Transactions or business structures involving high-risk countries, including those involving "own funds" transfers, particularly in circumstances in which there are no clear reasons for the involvement of such locations;
- Situations in which customers cannot or will not clearly explain the source of funds for a business activity or transaction, or in which the explanation appears to lack credibility;
- Situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide customer due diligence documentation, or provide documentation that is false, misleading, fraudulent or forged.

7.5 Requirement to Report

(AML-CFT Law 9.1, 15, 24; AML-CFT Decision 13.2, 17.1, 20.2)

DNFBPs are obliged to report transactions to the FIU when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime. As previously noted, there is no minimum reporting threshold, and no statute of limitations with regard to ML/FT crimes or reporting of suspicious transactions.

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 report a suspicious transaction, whether intentionally or by gross negligence, is a federal crime. With the exception of the exemption described in Section 7.4, Specific Exemption from the Reporting Requirement below, any person, whether a Designated Non-Financial Business and Profession, or its managers and employees, who fails to perform their statutory obligation to report a suspicion of money laundering, or the financing of

terrorism or of illegal organisations, is liable to a fine of no less than AED100,000 and no more than AED1,000,000 and/or imprisonment.

7.6 Specific Exemption from the Reporting Requirement

(AML-CFT Law 15; AML-CFT Decision 17.2)

DNFBPs that are lawyers, notaries, other legal professionals, and independent legal auditors are exempted by the AML-CFT Law and AML-CFT Cabinet Decision from the statutory reporting obligation on the grounds of professional secrecy only under one specific condition.

When they have obtained information concerning the transactions during the course of:

"…(assessing) their Customers' legal position, or defending or representing them before judiciary authorities or in arbitration, or providing legal opinion with regards to legal proceedings, including providing consultation concerning the initiation or avoidance of such proceedings, whether the information was obtained before or during the legal proceedings, or after their completion, or in other circumstances where such Customers are subject to professional secrecy."

7.7 Procedures for the Reporting of Suspicious Transactions

(AML-CFT Law 9; AML-CFT Decision 17.1(a), 21.2)

As the designated Competent Authority for receiving and analysing STRs from all DNFPBs, it is within the purview of the FIU to determine the procedures for the reporting of suspicious transactions. As stated in the AML-CFT Decision, supervised institutions shall report STRs "via the electronic system of the FIU or by any other means approved by the FIU." In this regard, the Financial Intelligence Department has established an online Suspicious Transaction Reporting System, which requires DNFBPs to choose from a list of suspicious indicators when filing a STR.

Without prejudice to the above, it should be noted that the AML-CFT Decision provides for the reporting of STRs to be effected by the AML/CFT compliance officer appointed by each DNFBP. Specifically, the Cabinet Decision states that the duty of a compliance officer is to:

"Review, scrutinise and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality."

In this regard, as part of their overall risk-based AML/CFT framework and commensurate with the nature and size of their businesses, DNFBPs should establish appropriate policies, procedures and controls pertaining to the internal reporting by their managers and employees of 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 AML/CFT 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 STRs;
- Content requirements and format of internal STRs;
- Appropriate controls for ensuring confidentiality and the protection of data from unauthorised access (also see Section 7.7, 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 AML/CFT compliance officer in regard to reporting to the FIU;
- Other conditions deemed appropriate by the AML/CFT compliance officer.

Such policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation, in keeping with the nature and size of the supervised institution's business.

7.8 Timing of Suspicious Transaction Reports (STRs)

(AML-CFT Law 9; AML-CFT Decision 17.1(a), 21.2)

DNFBPs are obliged to report STRs to the FIU "without any delay." Since it is the responsibility of the designated AML/CFT compliance officer to "review, scrutinise and study records, receive data concerning suspicious transactions, and take decisions to either notify the FIU or maintain the transaction," (see Section 8.1, Compliance Officer) it follows that the time period for reporting STRs to the FIU begins at the moment a decision is made by the designated AML/CFT compliance officer that a transaction (whether pending, in progress, or past) is suspicious. Likewise, it also follows that the internal reporting of suspicious transactions to the AML/CFT compliance officer should be done "without any delay," as soon as a suspicion or reasonable grounds for suspicion are established.

Without prejudice to the above, supervised institutions should note that, with the exception of any obligatory indicators for which immediate reporting to the FIU is required by the relevant Competent Authorities (for example, a positive match of a customer with regard to Targeted Financial Sanctions), some potentially suspicious transactions or indicators of

suspicion may require a degree of internal investigation before a suspicion or reasonable grounds for suspicion are established and an internal STR is reported to the designated AML/CFT compliance officer. 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 and internal reporting of suspicious transactions (including attempted transactions), and the degree and extent of investigations that are appropriate prior to the internal reporting of a suspicious transaction (also see Section 7.2, Identification of Suspicious Transactions). These policies and procedures should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

7.9 Confidentiality and Prohibition against "Tipping Off"

(AML-CFT Law 25; AML-CFT Decision 17.2, 21.2, 31.3, 39)

When reporting suspicious transactions to the FIU, DNFSBs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, 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. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

It should be noted that the confidentiality requirement does not pertain to communication within the supervised institution or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/FT.

It is a federal crime for 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 a penalty of no less than AED100,000 and no more than AED500,000 and imprisonment for a term of not less than six months.

7.10 Protection against Liability for Reporting Persons

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

DNFBPs, as well as their board members, employees and authorised representatives are protected by the relevant articles of the AML-CFT Law and AML-CFT Decision from any administrative, civil or criminal liability resulting from their good-faith performance of their statutory obligation to report suspicious activity to the FIU. However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

7.11 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 in order to mitigate the associated ML/FT risks (see Sections 6.4, Enhanced Due Diligence (EDD) Measures, especially 6.4.2, EDD Measures for High-Risk Customers or Transactions, and 6.3.5 Ongoing Monitoring of the Business Relationship).

Further guidance on both of these topics is provided below.

FIU Instructions

After receiving a STR from a DNFBP, the Financial Intelligence Department may or may not revert to the reporting institution with specific instructions, requests for additional information, feedback or further guidance related to the Suspicious Transaction or to the business relationship in general. In such cases, these communications will generally be directed to the designated AML/CFT compliance officer of the supervised institution. Examples of the types of instructions or requests which the FIU may issue to a reporting institution include, but are not limited to:

- Instructions to reject the transaction;
- Instructions to allow the transaction to proceed (for example, as in cases of Controlled Delivery of Funds in order to allow them to be traced by the Competent Authorities);
- Instructions related to the seizure or freezing of Funds or other assets related to the Customer;

- Instructions to terminate the business relationship;
- Instructions to maintain and monitor the business relationship, and periodically or conditionally report activities related to it to the FIU and/or other Competent Authorities;
- Requests for additional information about the reported transaction, other transactions related to the customer, or about the business relationship in general.

Confidentiality of FIU's Instructions

The responsibility for coordinating the supervised institution's prompt compliance with the FIU's instructions or requests lies with the designated AML/CFT compliance officer. It should be noted that, depending on the nature of the case, the FIU may require the compliance officer to maintain certain information related to its instructions or requests privileged and/or confidential within the supervised institution's organisation. In other words, in some cases, the AML/CFT 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 supervised institution. Regardless of the circumstances surrounding the FIU's instructions or requests, including whether or not the compliance officer is permitted to provide explanations to the staff of the supervised institution, the DNFBP is obliged at all times to follow the AML/CFT compliance officer's instructions in regard to any follow-up actions required in relation to a 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 a STR 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, supervised institutions 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, staff or other problem, and that efforts are underway to resolve it;

- Requesting additional information and/or supporting documentation (for example, evidence of relevant licences or authorisations, shipping or customs documents, additional identification documents, bank or other references) relating to the transaction, the customer, or the counterparty;
- Advising the customer that paperwork related to the transaction has been lost and requesting that it be resubmitted;
- Advising the customer that the transaction is pending an internal approval process;
- Any other reasonable delaying tactics, bearing in mind the obligation to avoid "tipping off" the customer.

During the time interval during which an anticipated, pending, or in-progress Suspicious Transaction that has already been reported to the FIU is being delayed by the supervised institution, any additional suspicions that may arise should also be reported to the FIU as a follow-up to the original STR. Examples of such additional suspicions may include, but are not limited to:

- New adverse information obtained in relation to the transaction, the business relationship, or the counterparty to the transaction;
- Unusual behaviour of the customer as a result of the transaction being delayed, such as but not limited to:
  - Sudden material amendments or changes to the circumstances or details of the transaction;
  - Excessive pressure, intimidation, displays of anger (beyond what would normally be expected) or threats of any kind, aimed at forcing the DNFBP or its employees to complete the transaction;
  - Abrupt cancellation of the transaction, termination of the business relationship, or sudden attempts to withdraw or obtain a refund of the balance of deposits, funds or other assets held by the supervised institution;
  - 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 a STR, and it becomes impossible for the DNFPB 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 supervised institution 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, supervised institutions should determine the appropriate handling of the Suspicious Transaction 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), supervised institutions 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;
- 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.

When deciding to terminate a business relationship for which a STR has been filed and no feedback has been received from the FIU after a reasonable time period, DNFBPs should consider formally advising the FIU of their intention to do so unless there is an official objection. In such cases, they should once again allow for a reasonable time period to receive feedback from the FIU, before initiating procedures to terminate the business relationship.

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 a 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 supervised institution's business;
- Precise nature of the suspicion.

The time period considered to be reasonable could thus vary widely from one case to another.

As a general guideline, the reasonable time periods for feedback from the FIU concerning transaction types that are less complex, more routine, and have faster average processing times (such as an over-the-counter purchases of precious metals or gemstones, for example) would normally be expected to be shorter than those for more complex, less routine transaction types (such as, for example, sales or purchases of legal entities, real estate or other complex assets, or establishing a legal entity or legal arrangement). 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 situations in which no feedback or instructions have been received from the FIU (and, in particular, no specific instructions to terminate the business relationship have been received), 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/FT risks associated with the business relationship.

In such cases, beyond the EDD measures described in previous sections (see Sections 6.4, Enhanced Due Diligence (EDD) Measures and 6.3.5 Ongoing Monitoring of the Business Relationship), DNFBPs should also consider implementing 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 licences 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 consider documenting the specific EDD, ongoing monitoring, and additional control measures to be taken in the form of an action plan. In this regard, supervised institutions should consider obtaining senior management approval for the plan, including its specific conditions, duration and any requirements for its removal, as well as the roles and responsibilities for its implementation, monitoring and reporting, commensurate with the nature and degree of the ML/FT risks associated with the business relationship.

8. Governance

(AML-CFT Law 16.1(d); AML-CFT Decision 4.2(a), 20, 21, 44.4)

In order for the AML/CFT framework of any organisation to be effective, it must be based on the foundation of a sound governance structure, and held together by a strong compliance culture. These include appropriate management structures which are accountable for clear ML/FT risk management and mitigation measures, as well as appropriate independent control functions. Implicit in both the AML-CFT Law and the AML-CFT Decision are the elements of both, concerning which additional guidance is provided in the sections below.

8.1 Compliance Officer (CO)

(AML-CFT Decision 20.3, 21 and 44.12)

8.1.1 Appointment and Approval

DNFBPs are obliged to appoint an AML/CFT compliance officer with the appropriate competencies and experience to perform the statutory duties and responsibilities associated with this role. The AML-CFT Decision stipulates that the AML/CFT compliance officer (“CO”) performs these duties “under his or her own responsibility”, referring to the independent nature of the function, and further provides that the appointment of a person to the position of compliance officer requires the prior consent of the relevant Supervisory Authority.

In determining the competencies, level of experience, and organizational reporting structures that are appropriate for their compliance officers, DNFBPs should take several factors into consideration, including but not limited to:

- The results of the NRA;
- The nature, size, complexity, and risk profile of their industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;

- The organisation's governance framework and management structure, with particular consideration given to the independent nature of compliance as a control function;
- The specific duties and responsibilities of the CO role (described below).

Where appropriate, DNFBPs may also consider engaging in dialogue with Supervisory Authorities, professional associations in their sectors, and industry peers, in relation to the competencies, experience, and governance structures that make for an effective AML/CFT compliance officer and an effective AML/CFT programme.

8.1.2 Responsibilities

(AML-CFT Decision 21.1-5)

The specific duties of the compliance officer are detailed in the relevant provisions of the AML-CFT Decision. These duties can be grouped broadly into the following categories:

- ML/FT Reporting. The AML/CFT compliance officer is the supervised institution's suspicious transaction reporting officer. In this capacity, the CO is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and of illegal organisations, for reporting suspicions to the FIU, and for cooperating with the Competent Authorities in relation to the performance of their duties in regard to AML/CFT.
- AML/CFT Programme Management. The CO should ensure the quality, strength and effectiveness of the supervised institution's AML/CFT programme. As such, the AML/CFT compliance officer should be a stakeholder with respect to the FI's and DNFBP's overarching ML/FT risk policies, risk assessment procedures and controls, and ML/FT risk mitigation framework, including its customer due diligence measures.
- AML/CFT Training and Development. The CO is responsible for helping to establish and maintain a strong and effective AML/CFT compliance culture within the DNFBP. This duty includes working with senior management and other internal and external stakeholders to ensure that the organisation's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/FT.

8.2 Staff Screening and Training

(AML-CFT Decision 20.4-5, 21.4)

In order for their ML/FT risk assessment and mitigation measures to be effective, DNFBPs should ensure that their employees have a clear understanding of the risks involved and can exercise sound judgment, both when adhering to the organisation's ML/FT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/FT risk, supervised institutions should ensure that their

employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks.

Thus, to ensure a high level of competence and AML/CFT programme effectiveness, DNFBPs should formulate and implement appropriate policies, procedures and controls with regard to staff screening and training. These measures should be applied across organisations and financial groups, including their foreign branches and majority-owned subsidiaries. Examples of some of the factors that should be considered when determining appropriate staff screening and training measures include, but are not limited to:

- The results of the NRA;
- The nature, size, complexity, and risk profile of DNFBPs' industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- Effective screening and selection methods in relation the AML/CFT cultural compatibility of their employment candidates;
- Assessment of staff AML/CFT competency in relation to training and development needs;
- The type, frequency, structure, content, and delivery channels of AML/CFT training programmes and development opportunities;
- The effective identification, deployment and management of both internal and external training resources;
- Appropriate methods and tools for assessing the effectiveness of staff hiring, training, and development programmes.

8.3 Group Oversight

(AML-CFT Decision 20, 31, 32)

DNFBPs are obliged to implement appropriate group-wide AML/CFT programmes, and to apply them in relation to all their branches and majority-owned subsidiaries. The specific requirements that must be met by DNFBPs with respect to their foreign branches and majority-owned subsidiaries are set out in the relevant provisions of the AML-CFT Decision, and reflect those to which supervised institutions are subject within the State.

In meeting these obligations with regard to their branches and majority-owned subsidiaries in foreign countries, supervised institutions should ensure that the measures they apply are consistent with the requirements of the AML-CFT Law and AML-CFT Decision. In this regard, DNFBPs should establish appropriate policies and procedures for the exchange of data and information, including customer CDD and transaction-related information, between the foreign branches and subsidiaries and the head office, for the purpose of combating the

crimes of money laundering and the financing of terrorism and of illegal organisations, and for reporting suspicious transactions.

In situations where these measures are not possible due to legislative or regulatory restrictions in the foreign countries in which their branches and majority-owned subsidiaries operate, DNFBPs should implement the necessary additional measures, commensurate with the nature and size of their businesses, that will enable them to manage and mitigate appropriately the ML/FT risks that relate to their foreign operations. Examples of some of the measures that should be considered include but are not limited to:

- Assessing the effectiveness of foreign branches and majority-owned subsidiaries' CDD measures, including evaluating such factors as the comprehensiveness and quality of their policies, procedures and controls, and performing gap analyses in relation to the requirements of the AML-CFT Law and AML-CFT Decision;
- Establishing clear policies, procedures and controls in relation to the type and extent of access which managers and employees of foreign branches and majority-owned subsidiaries have to the supervised institutions' IT and operational systems, including transaction processing systems;
- Establishing clear policies, procedures and controls in relation to the type and extent of access which customers and Business Relationships of foreign branches and majority-owned subsidiaries have to the supervised institutions' products, services and transactional processing capabilities;
- Establishing clear policies, procedures and controls in relation to the type of CDD and transaction-related information, data, and analysis supervised institutions accept from their foreign branches and majority-owned subsidiaries in relation to customer or Business Relationship referrals, and the extent of their reliance on such information (see Section 6.6, Reliance on a Third Party);
- Implementing service-level agreements, clearly setting out the roles and responsibilities of the parties and specifying the nature of the CDD and record-keeping requirements to be fulfilled in relation to customer or Business Relationship referrals;
- Establishing protocols for the certification by the foreign branches and subsidiaries of documents and other records pertaining to the CDD measures undertaken in relation to customer or Business Relationship referrals.

In particular, in cases in which the minimum AML/CFT requirements of host countries in which DNFBPs maintain foreign operations are less strict than those of the State, supervised institutions should take the necessary measures to ensure that their foreign branches and/or majority-owned subsidiaries in those countries implement the requirements of the State, to the extent permitted by the laws and regulations of the host

countries. If such host countries do not permit the proper implementation of the AML/CFT requirements of the State, DNFBPs should apply appropriate additional measures to manage and mitigate the ML/FT risks (including but not limited to those described above). They should also inform the relevant Supervisory Authorities of the circumstances and comply with any additional supervisory actions, controls, or requirements of the Competent Authorities of the State (up to and including, if requested, terminating their operations in the host countries).

8.4 Independent Audit Function

(AML-CFT Decision 20.6)

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. DNFBPs are obliged to have in place an independent audit function to test the effectiveness and adequacy of their internal polices, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organisations. In this regard, DNFBPs should ensure that their independent audit function is appropriately staffed and organised, and that it has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/FT risks to which the supervised institutions are exposed, and with the nature and size of their businesses.

It should be noted that, depending on the nature and size of their businesses, some DNFBPs (particularly smaller ones) may not necessarily have the resources to maintain a fully functioning and effective internal audit unit. In such cases, those supervised institutions should ensure that they take adequate measures to obtain the necessary capabilities from qualified external sources. They should also ensure that they have in place adequate internal capabilities to provide sufficient coordination with and oversight of any external resources they may utilise, and that such external resources are adequately regulated and supervised by relevant Competent Authorities.

DNFBPs should ensure that the periodic inspection and testing of all aspects of their AML/CFT compliance programmes, including ML/FT risk assessment and mitigation measures, and customer due diligence policies, procedures and controls, is incorporated into their regular audit plans. They should also ensure that all their branches and the subsidiaries in which they hold a majority interest, whether domestic or foreign, are part of an independent audit testing programme that covers the effectiveness and adequacy of their internal AML/CFT polices, controls and procedures.

Some of the factors supervised institutions should consider in determining the appropriate frequency and extent of audit testing of their AML/CFT programmes by their independent audit functions include but are not limited to:

- The results of the NRA;
- The nature, size, complexity, and geographic scope of the DNFBPs' businesses, and the results of their enterprise risk assessments;
- The risk profile associated with the products and services they offer and the markets and customer segments they serve;
- The frequency of supervision and inspection by, and the nature of the feedback (including the imposition of administrative sanctions) they receive from, Supervisory Authorities, relative to enhancing the effectiveness of their AML/CFT measures;
- Internal and external developments in relation to ML/FT risks, as well as developments pertaining to the management and operations of the supervised institutions.

8.5 Responsibilities of Senior Management

(AML-CFT Decision 4.2(a), 4.2(b)(5), 8.1(a), 15.1(b) and 15.2, 17.3, 21.3, 25.1(d))

A cornerstone of any sound governance structure, including those related to AML/CFT compliance, is senior management involvement and accountability. The members of a DNFBP's senior management (together with the members of the board of directors in those organisations that have one) are ultimately responsible for the quality, strength and effectiveness of the supervised institution's AML/CFT framework, as well as for the robustness of its compliance culture. In this regard, a supervised institution's senior management should set the so-called "tone at the top," by demonstrating their commitment to ensuring an effective AML/CFT compliance programme is in place, and by clearly articulating their expectations with regard to the responsibilities and accountability of all staff members in relation to it.

Under the AML/CFT legal and regulatory framework of the United Arab Emirates, the senior management all DNFBPs are responsible for performing certain functions related to the assessment, management and mitigation of the ML/FT risks to which their organisations are exposed. These responsibilities can be grouped broadly into categories which include:

- Implementation of governance, control, and operating systems. These include such elements as:
  - Appointing a qualified AML/CFT compliance officer who is approved by the relevant Supervisory Authority;
  - Ensuring a robust and effective independent audit function is in place;
  - Putting in place and monitoring the implementation of adequate management and information systems, internal controls, and policies, procedures to mitigate risks.

- Approval of internal policies, procedures and controls. These include such elements as the supervised institution's policies on overall ML/FT risk appetite and customer acceptance, as well as the framework of AML/CFT policies, procedures and controls related to areas such as:

  - Identification, assessment, understanding, and management/mitigation of ML/FT risks;
  - Performance, review and updating of customer due-diligence (including enhanced and simplified due-diligence) measures;
  - Identification and implementation of indictors to identify suspicious transactions;
  - Record retention and data protection;
  - Staff screening, training and development.

- Oversight of the AML/CFT compliance programme. This includes such elements as:

  - Reviewing and providing comments in relation to the AML/CFT compliance officer's semi-annual reports to the relevant Supervisory Authority;
  - Approving the establishment and continuance of High Risk Customer Business Relationships and their associated transactions, including those with PEPs;
  - Approving the establishment and continuance of Business Relationships involving high-risk countries;
  - Approving the establishment and continuance of relationships with correspondent banks;
  - Ensuring the adequate application of the appropriate components of the AML/CFT compliance programme to all branches and majority-owned subsidiaries, including those operating in foreign jurisdictions.

- Application of the directives of Competent Authorities. This includes such elements as:

  - Applying the directives of Competent Authorities for implementing UN Security Council decisions under Chapter VII of the Charer of the United Nations, and other related directives (see Section 10, International Financial Sanctions);
  - Implementing CDD measures defined by the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations, regarding High Risk Countries;
  - Implementing all other directives of the relevant Competent Authorities of the State, including Cabinet Decision (20) of 2019 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* (see Section 10, International Financial Sanctions), which may enter into effect from time to time.

8.6 Governance Issues with respect to Small Organisations

Some DNFBPs may operate as small or mid-sized businesses, without large staff organisations or sophisticated IT infrastructures. In such cases, individual managers and employees may often be called upon to undertake multiple roles and responsibilities in the course of day-to-day business activities, and it may be difficult at times to maintain a clear separation of duties or functions. While a supervised institution's small size does not in any way exempt it from fulfilling its obligations under the AML-CFT Law and AML-CFT Decision, and without prejudice to guidance provided in the previous sections, the following additional considerations are of particular importance to small and mid-sized DNFBPs.

- In situations in which the responsibilities of the AML/CFT compliance officer are delegated to a manager or staff member who also has other responsibilities, DNFBPs should undertake their best efforts to ensure that the designated AML/CFT compliance officer does not have day-to-day responsibility for sales and/or customer business relationship management.

- When an adequate separation of responsibilities is not possible due to the small size of a DNFBP's organisation, supervised institutions should take the necessary steps to ensure that operational and AML/CFT policies and procedures (particularly those pertaining to Customer Due Diligence, the identification of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and Sanctions Lists—see Sections 6, Customer Due Diligence (CDD), 6.4.3 Requirements for High-Risk Countries, and 10, International Financial Sanctions) are clearly formulated, documented, and adhered to during the establishment and ongoing monitoring of business relationships and the carrying out of transactions.

- In such cases, DNFBPs should ensure that they clearly document the rationale for any policy and/or procedural exceptions they make, along with any additional ML/FT risk-mitigation measures they implement, and that these records are properly retained in accordance with the statutory record-keeping requirements (see Section 9, Record Keeping). Supervised institutions should also consider referring to any significant policy or procedural exceptions, along with their rationale, associated additional ML/FT risk-mitigation measures, and senior management comments, in the AML/CFT compliance officer's required semi-annual reports to the relevant Supervisory Authorities.

- DNFBPs that are unable to ensure a clear and effective separation of AML/CFT responsibilities from those related to the day-to-day management of their businesses, including but not limited to sales and customer business relationship management functions, due to the small size of their organisations should also consider taking additional measures to enhance the application of their independent audit controls (see Section 8.4, Independent Audit Function). Examples of such measures include but are not limited to:

- Incorporating the audit of policies, procedures (particularly those pertaining to Customer Due Diligence, the identification of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and Sanctions Lists), and records related to exceptions made to them, as part of their audit plans and/or their service-level agreements with their external providers of independent audit services;
- Increasing the frequency of independent audits and random audit inspections;
- Applying stricter criteria with regard to the review of past transactions, such as increasing the number of transactions reviewed for a given time period, reducing size threshold limits for transactions to be reviewed, or taking other reasonable measures in this regard.

9. Record Keeping

9.1 Obligations and Timeframe for the Retention and Availability of Records

(AML-CFT Law 16.1(a),(f); AML-CFT Decision 7.2, 24, 36, 37.3)

DNFBPs are obliged to maintain detailed records, documents, data and statistics for all financial transaction types, as well as a variety of record types and documents associated with their ML/FT risk assessment and mitigation measures, as specified in the relevant provisions of the AML-CFT Decision (see Section 9.2, Required Record Types). Supervised institutions are required to maintain the records in an organised fashion so as to permit data analysis and the tracking of financial transactions, and to make the records available to the Competent Authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, depending on the circumstances, from the date of the most recent of any of the following events:

- Termination of the Business Relationship or the closing of a customer's account with the supervised institution;
- Completion of a casual transaction (in respect of a customer with whom no Business Relationship is established);
- Completion of an inspection of the records by the Supervisory Authorities;
- The issue date of a final judgment by the competent judicial authorities;
- Liquidation, dissolution, or other form of termination of a legal person or arrangement.

Without prejudice to the above, DNFBPs should note that it is the prerogative of the Competent Authorities to require the retention of the records of any supervised institution, whether data, statistics, or records pertaining to a specific customer or transaction or to general categories of customers or transactions which they deemed to be of interest, for a longer period of time at their own discretion.

In order to fulfil their record-keeping obligations, and commensurate with the nature and size of their businesses, DNFBPs should determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records. The policies, procedures and controls should be documented, approved by senior management, and communicated to appropriate levels of the organisation. Examples of the factors which DNFBPs should give consideration to when formulating the relevant policies, procedures and controls, include but are not limited to:

- Organisational roles and responsibilities in regard to the risk assessment, implementation, review and updating of policies, procedures and controls related to

record-keeping and data protection, including appropriate business contingency and escalation procedures;

- Organisational roles and responsibilities in relation to record-keeping (including logging, cataloguing and organisation, archiving, handling and transferring of records and documents, as well as of the destruction of expired records);
- Physical and cyber security, and the protection of active and archived data and records from unauthorised access;
- Appropriate audit and quality assurance testing policies.

9.2 Required Record Types

(AML-CFT Law 16.1(a),(b),(f); AML-CFT Decision 7.2, 24)

The AML-CFT Law and AML-CFT Decision oblige DNFBPs to retain several types of records, which can be classified broadly into the following categories:

- Financial Transaction Records. This category relates to operational and statistical records, documents and information concerning all financial transactions executed or processed by the supervised institution, whether domestic or international in nature.
- CDD Records. This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:
  - Customer Information
  - Company Information
  - Reliance on Third Parties to Undertake CDD
  - Ongoing Monitoring of Business Relationships
  - Suspicious Transaction Reports (STRs)

Additional guidance related to these record types is provided in the following sub-sections.

9.2.1 Financial Transactions

(AML-CFT Law 16.1(f); AML-CFT Decision 24.1-3, 28.1-2, 29.4)

DNFBPs are obliged to retain the operational and statistical records, documents and information concerning all financial transactions executed or processed by the supervised institution, whether domestic or international in nature, and irrespective of the type of customer and whether or not a Business Relationship is maintained, for a minimum period of five (5) years. Some examples of the type of records, documents and information which must be retained include but are not limited to:

- Customer correspondence, requests or order forms related to the initiation and performance of all types of transactions;
- Customer payment advices, receipts, invoices, billing notifications, bills of exchange, statements of account, expense reimbursement requests or notifications;
- Credit-related correspondence and documentation, including those involving accounts receivable, cash advances or advance settlements, promissory notes, loans or guarantees and their amendments and supporting documents, disbursement or repayment records, collateral pledges, or any other form of customer credit;
- Deal tickets, trade blotters and ledgers, settlement and dividend payment records related to customer funds managed, legal structures or arrangements, or any other forms of asset trades or exchanges;
- Escrow or fiduciary account transaction records;
- Sale, purchase, lease, merger-acquisition, and similar agreements;
- Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

In addition to the above, DNFBPs should compile notes on any particularly large or unusual transactions, and keep these notes as part of their records.

9.2.2 Customer Information

(AML-CFT Law 16.1(b); AML-CFT Decision 24.2-4, 27.7, 28.1-2, 29.4, 37.1-3)

DNFBPs are required to retain all customer records and documents obtained through the performance of CDD measures in relation to Business Relationships, including customers, Beneficial Owners, beneficiaries, or other controlling persons. Examples of such records include but are not limited to:

- Customer account information and files;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls);
- Copies of personal identification documents, KYC and CDD (including EDD and SDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries and investigations;
- Customer risk assessment and classification records.

9.2.3 Company Information

(AML-CFT Law 16.1(b); AML-CFT Decision 8.1(b), 9.1, 34-36)

The AML-CFT Decision provides that the administrators, liquidators, or any other stakeholders involved in the dissolution of a company are obliged to retain the records, documents and information specified in the relevant articles for a minimum period of five (5) years from the date of its dissolution, liquidation or termination. These records pertain to corporate documents as well as to information on Beneficial Owners, legal shareholders, and senior managers. Such records include but are not limited to documents and information concerning:

- Company formation, registration, deregistration, liquidation, dissolution or expiry, including documents such as share registers, memoranda and articles of association, deeds of settlement and foundation charters, or similar documents, along with any amendments to them (whether the organisation is for-profit or not-for-profit);
- Changes to company information, such as name, registered address, legal representatives and corporate officers (directors, company secretary), or legal form;
- Identification and identity verification documents related to Beneficial Owners, shareholders, nominee shareholders, directors, senior management officers and, in the case of Legal Arrangements, settlors or founders, protectors, beneficiaries, trustees or executors, governing council or committee members, or similar controlling persons.

In order to fulfil their statutory record-keeping obligations in this regard, and commensurate with the nature and size of their businesses, supervised institutions (and in particular, DNFBPs engaged as corporate attorneys, trustees, or company service providers, administrators, liquidators, directors, or any other form of stakeholders) should determine the appropriate policies, procedures and controls related to the adequate retention, organisation, and maintenance of records. The policies, procedures and controls should be documented, approved by senior management, and communicated to appropriate levels of the organisation (see Section 9.1, Obligations and Timeframe for the Retention and Availability of Records for additional guidance concerning policies, procedures, controls and statutory retention periods related to record-keeping and data protection).

9.2.4 Reliance on Third Parties to Undertake CDD

(AML-CFT Law 16.1(b); AML-CFT Decision 24.2-4, 19.1(b)-2(a))

DNFBPs that rely on third parties, whether unaffiliated or members of their own financial groups, are obliged to ensure that copies of all the necessary documents collected through the performance of CDD measures can be obtained upon request and without delay, and that the third parties adhere to the record-keeping provisions of the AML-CFT Decision. See Section 9.2.2, Customer Information above for examples of such records.

In order to fulfil their statutory obligations, and commensurate with the nature and size of their businesses, 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:

- Organisational roles and responsibilities in regard to the assessment, monitoring and testing of the third party's policies, procedures and controls related to record-keeping and data protection, including appropriate business contingency and escalation procedures;
- Organisational roles and responsibilities for the implementation of service-level agreements with third parties governing the provision of record-keeping services;
- Operational procedures related to request and transfer of records and documents, as well as their physical and cyber security, and the protection of active and archived data and records from unauthorised access;
- Appropriate audit and quality assurance testing policies related to the monitoring and testing of the third-party's record-retention framework.

9.2.5 Ongoing Monitoring of Business Relationships

(AML-CFT Law 16.1(b),(f); AML-CFT Decision 24.2-4)

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

- Transaction review, analysis, and investigation files, with their related correspondence;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to transactions or their analysis and investigation;
- Customer due diligence records, documents, profiles or information gathered in the course of reviewing, analysing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;
- Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.

9.2.6 Suspicious Transaction Reports (STRs)

(AML-CFT Law 16.1(f); AML-CFT Decision 24.2-4)

DNFBPs are required to retain all records and documents pertaining to suspicious transaction reports and the results of all analysis or investigations performed. Such records relate to both internal STRs and those filed with the FIU, and include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
- Competent authority request for information (RFIs), and their related investigation files and correspondence;
- Customer due diligence and Business Relationship monitoring records, documents and information obtained in the course of analysing or investigating potentially suspicious transactions, and all internal or external correspondence or communication records associated with them;
- STRs (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence;
- Notes concerning feedback provided by the FIU with respect to reported Suspicious Transactions, as well as notes or records pertaining to any other actions taken by, or required by, the FIU.

10. International Financial Sanctions

The United Arab Emirates is a member of several multinational and international organisations and governing bodies, including the United Nations. As such, the UAE is a party to many international agreements and conventions pertaining to the combating of money laundering and the financing of terrorism, as well as to the prevention and suppression of the proliferation of weapons of mass destruction. These conventions include, among others, the *International Convention for the Suppression of the Financing of Terrorism* and the *Treaty on the Non-Proliferation of Nuclear Weapons*.

DNFBPs are obliged to comply with the directives of the Competent Authorities of the State in relation to the agreements and conventions referred to above, including but not limited to Cabinet Decision No. (20) of 2019 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions*. Moreover, it should be noted that many DNFBPs are also affected by unilateral international sanctions programmes and restrictive measures implemented by other countries and supranational blocs (see Section 10.2, Other International Financial Sanctions).

Due to the significance, complexity and extent of the subject matter of international financial sanctions, it is deemed appropriate that this material be covered in depth in separate guidance materials. However, while it is outside of the scope of these Guidelines to provide detailed guidance on these topics, a brief high-level overview of the key elements of TFS, Cabinet Decision No. (20) of 2019, and a few other major international financial sanctions regimes is included in the sub-sections below.

10.1 Targeted Financial Sanctions (TFS)

(AML-CFT Law 16.1(e), 28; AML-CFT Decision 44.7, 60)

Targeted Financial Sanctions are international sanctions rules established to comply with the United Nations Security Council resolutions under Chapter VII of the Charter of the United Nations. The UAE adheres to the decisions issued by the UN Security Council under that Chapter, as well as to the FATF recommendations concerning their implementation.

Consequently, both the AML-CFT Law and AML-CFT Decision authorise the Competent Authorities of the State, including the relevant Supervisory Authorities, to ensure the full compliance of DNFBPs in implementing these decisions and other related directives; and all DNFBPs are obliged to promptly apply the directives of the Supervisory Authorities in this regard. Specifically, the AML-CFT Law and its Implementing AML-CFT Decision provide that:

> *"Every natural or legal person shall immediately comply with the instructions issued by the Competent Authorities in the State concerning the implementation of the decisions issued by UN Security Council under Chapter VII of the Charter of the United Nations regarding the prevention and suppression of terrorism and Terrorism Financing, and the prevention and suppression of the proliferation of Weapons of Mass Destruction and its financing, and any other related Decisions."*

And further, that:

> *"Imprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the Competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions."*

TFS require countries to freeze, without delay, the funds or other assets of any person or entity either designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, such persons.

DNFBPs should ensure that they have adequate internal mechanisms, including the necessary policies, procedures and controls in place, commensurate with the nature and size of their businesses, in order to fulfil their obligations to promptly apply the directives of the relevant Supervisory Authorities in regard to the related directives.

10.2 UAE Cabinet Decision No. (20) of 2019

(AML-CFT Law 16.1(e), 28; AML-CFT Decision 60)

The AML-CFT Law and the AML-CFT Decision oblige DNFBPs to promptly apply directives issued by the Competent Authorities of the State for implementing the decisions issued by the UN Security Council under Chapter VII of the Charter of the United Nations. In furtherance of this requirement, Cabinet Decision No. (20) of 2019 (the "Decision") sets out the legislative and regulatory framework in the UAE for the management of terrorism lists and the implementation of UN Security Council Resolutions relating to the combating of terrorism and its financing, and the suppression of the proliferation of weapons of mass destruction. In general, the Decision accomplishes the following:

- Defines the relevant Competent Authorities and their duties in regard to the implementation of UN Security Council Resolutions and related decisions, and sets out the mechanisms by which local and international terrorism lists are established and amended in the UAE;

- Establishes the legal and administrative framework for the freezing and unfreezing of assets of listed persons;
- Defines the related processes for the filing and of petitions and grievances with the relevant Competent Authorities, and their subsequent adjudication;
- Establishes the authority of the Supervisory Authorities to ensure the compliance of DNFBPs with the obligation to implement the relevant Security Council Resolutions and to impose adequate administrative penalties in cases of negligence or failure to do so;
- Defines the obligations of DNFBPs for the purpose of implementing the provisions of the Decision; and provides certain protections against administrative liability for persons acting in compliance with them, as well as administrative and penal sanctions for persons violating the same.

For convenience, the specific obligations of DNFBPs, as well as the protections and penalties, are summarised further below. These obligations derive in part from the relevant Articles (11 and 12) of the Decision, which state the following:

- **Article 11 (Cabinet Decision No. (20) of 2019)**

"Every natural or legal person should, without delay or prior notice, freeze Funds owned, controlled or held, in whole or in part, directly or indirectly by any of the following:

1. *An individual or organization designated by the UN Security Council or any relevant Security Council committee pursuant to any relevant Security Council resolutions.*

2. *An individual acting, directly or indirectly, on behalf of, or as directed, controlled or dominated by, any person or organization listed in the Sanctions List.*

In all cases, the rights of bona fide third parties shall be considered when implementing any of the freezing procedures."

- **Article 12 (Cabinet Decision No. (20) of 2019)**

"Any natural or legal person shall be prohibited from making available any Funds in his/her possession or under his/ her control, or other financial services, whether directly or indirectly, for, or to the benefit of, any person or organization listed in the Sanctions List, unless pursuant to a permission of the Office [the Executive Office of the Committee for Goods and Materials Subject to Import and Export Control], and in coordination with the relevant 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], or in line with related Security Council resolutions."

With reference to the above, the Decision defines "without delay" as meaning "within hours from issuance of the listing decision by the Sanctions Committee." In practical terms,

DNFBPs should consider this to mean within hours (and usually within the same business day) of identifying a customer or transaction as being subject to the provisions of the relevant Security Council Resolutions, and certainly prior to the execution of any transactions for such persons or organisations. It is also important to note that, according to the provisions of the Decision, DNFBPs are obliged to take responsibility for freezing the Funds (including assets in any form) of listed persons and organisations, which are in their possession or under their control, or which they receive for any reason (including as payment for products or services), even without receiving specific instructions from any Competent Authority to do so.

Under certain conditions involving payments due under contracts, agreements, or obligations entered into prior to the person becoming subject to the relevant UN Security Council resolutions, DNFBPs may be permitted to accept funds from listed persons or organisations, provided that the funds thus accepted are subject to freezing and are reported to the Office, or that permission for the relevant disposition of the funds is obtained from the Office. The specific conditions are covered in detail in Articles 13 and 14 of the Decision, to which supervised institutions are referred.

Summary of the Obligations of DNFBPs under Cabinet Decision (20) of 2019

The principal obligations of DNFBPs under Cabinet Decision (20) of 2019 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* relate to the following categories of actions:

- Maintaining a continuously up-to-date awareness of the persons and organisations listed in the relevant Sanctions Committees lists and comparing these on an ongoing basis with their customer databases;
- Ensuring, prior to entering into business relationships or conducting any transactions with natural or legal persons or legal arrangements, that such persons or organisations are not included in the relevant Sanctions List;
- Freezing (or unfreezing when so instructed by the Competent Authorities) the Funds of listed persons or organisations, which the supervised institutions hold, have access to, or otherwise control;
- Immediately reporting to the Supervisory Authorities when listed persons or organisations are identified and/or when the Funds of such persons or organisations are frozen, as well as in other specific situations noted below.

In addition to the above, the Cabinet Decision prohibits persons who, by virtue of their positions in relation to supervised institutions, have access to or become aware of information provided or exchanged with a Competent Authority under the relevant

provisions of the Decision, from disclosing such information in any form, except for the purpose of implementing the Decision.

With respect to the reporting of listed persons and organisations, DNFBPs should note the following key points:

- They are obliged to report to the relevant Supervisory Authorities the details of any customers identified as listed persons or organisations regardless of whether they are past, current, or prospective customers; regardless of whether they maintain(ed) business relationships with such customers or interact(ed) with them only in the form of occasional or attempted transactions; and also regardless of whether they perform(ed) any transactions related to such persons or organisations.

- Supervised institutions are also required to report to the relevant Supervisory Authorities the details of any customers that are identified as *potential* matches with listed persons or organisations, when they cannot resolve the similarities (i.e. cannot either confirm the match as true or conclusively reject it as a false positive) based on the information available to them and therefore have not frozen the Funds of such persons or organisations, or have not undertaken other procedures in compliance with the prohibition requirements prescribed in the relevant UN Security Council Resolutions. In such cases, DNFBPs should avoid executing any transactions related to such persons or organisations, pending feedback or instructions from the relevant Supervisory Authorities.

- In the case of Suspicious Transactions (whether past, in-progress, or attempted) involving listed persons or organisations, DNFBPs should file the STRs with the FIU as per the normal procedures (see Section 7, Suspicious Transaction Reporting). At the same time, they should report the details of the listed persons or organisations to the relevant Supervisory Authorities in accordance with the provisions of the Decision.

Summary of Protections/Penalties for DNFBPs under Cabinet Decision (20) of 2019

Cabinet Decision No. (20) of 2019 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* establishes an exemption against administrative liability arising from damages or claims against persons acting in good faith in compliance with its provisions. It also establishes administrative and penal sanctions against persons violating its provisions.

In other words, the Decision protects DNFBPs, as well as their directors, management, and employees acting in good faith in compliance with its provisions, when they: freeze or deny the disposal of, or access to, Funds; refuse to provide financial services related to frozen Funds; or decline to perform or fulfil any other obligation by reason of compliance with the

relevant provisions of the Decision, the relevant UN Security Council Resolutions, or the related directives of the Competent Authorities.

For the purpose of enforcement, Cabinet Decision No. (20) of 2019 authorises the Supervisory Authorities to impose "adequate administrative penalties in case of negligence or failure to implement the provisions of this Decision." Additionally, the Decision subjects any person who violates their obligations under its relevant provisions to the administrative and penal punishments stipulated in the AML-CFT Law. Specifically, Article 28 of the AML-CFT Law provides that:

> *"Imprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the Competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions."*

10.3 Other International Sanctions

In addition to TFSs and related programmes of the United Nations, many other countries and supranational blocs also maintain international economic, trade or travel sanctions programmes and restrictive measures of their own. Similar to the TFS regimes, these unilateral measures often require the freezing of funds or other assets of listed natural or legal persons and organisations. They may also require general or specific licences in order to conduct business or engage in transactions with persons or entities from certain countries. DNFBPs who engage in transactions in the currencies of those countries and supranational blocs, whether for their own account or on behalf of their customers and Business Relationships, may be affected by such international financial sanctions regimes. Some of the major international financial sanctions programmes are those of:

- The United States of America. The United States maintains a significant number of economic, trade, and other sanctions programmes in accordance with its foreign policy and national security objectives. Some of these programmes are comprehensive, affecting entire countries or jurisdictions, while others are selective, targeting specific governments, sectors, organisations and/or persons.

  Many of the United States' sanctions programmes are administered by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"); however, some (for example, certain trade licensing and travel restriction programmes) may be administered by other departments or agencies of the US government.

  The United States requires all US persons, including citizens and permanent residents (green card holders), no matter where they are located, to comply with the provisions of OFAC sanctions programmes. Additionally, all persons and entities within the United

States, all US incorporated entities and their foreign branches, and, in the case of certain programmes, the foreign subsidiaries of US legal entities and non-US persons in possession of US-origin goods, are also required to comply. In this regard, DNFBPs that conduct business or transactions in US dollars should note that the clearing of US dollar-denominated transactions through a US financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of OFAC sanctions programmes.

Fines for violations of OFAC sanctions can be substantial, and may include both civil and criminal penalties. While these can vary according to the sanctions programme, depending on the case, civil and criminal penalties can often exceed several millions of US dollars.

- The European Union. In the context of its Common Foreign and Security Policy (CFSP), the European Union maintains a number of economic, trade and other sanctions programmes, or "restrictive measures". Such restrictive measures may be imposed against third countries, entities or persons, in line with the EU's CFSP objectives.

  Certain restrictive measures of the EU, such as arms embargoes or restrictions on admission, may be implemented at the national level by each member state. Others are implemented at the EU level, such as measures relating to restrictions on economic relations with third countries or those freezing funds and economic resources. Other types of restrictive measures that have been used by the EU include, among others, embargoes on equipment that could be used for internal repression, export or import restrictions, flight bans, bans on the provision of financial services, investment bans, and sectoral bans or measures aimed at preventing the misuse of equipment, technology or software for monitoring and intercepting of the internet or other forms of communication.

  Generally, the EU requires compliance with its sanctions programmes in situations where linkages exist with the EU. These may involve, among other things, persons or entities within the territory of the European Union, or onboard aircraft or marine vessels registered in EU member states; nationals of EU member states; legal persons or arrangements incorporated or constituted under the laws of any EU member state (including, in some instances, the owned or controlled non-EU subsidiaries of EU domiciled legal entities); or persons or organisations conducting any business or transactions, in whole or in part, within the European Union. In this regard, DNFBPs that conduct business or transactions in euros should note that the clearing of euro-denominated transactions through a EU financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of EU restrictive measures.

  The European Union's regulations imposing restrictive measures also provide for penalties in the case of violations of the measures. Such penalties may vary according to

the specifics of the situation and the member state involved; however, the common EU approach to the imposition of penalties provides that they should be effective, proportionate and dissuasive.

- The United Kingdom. In addition to the EU-wide restrictive measures which it has applied during its tenure as a member state of the European Union, the UK also has the ability to impose its own financial sanctions and restrictive measures under domestic legislation, including:

  - Terrorist Asset-Freezing Act 2010 (TAFA 2010)
  - Counter Terrorism Act 2008 (CTA 2008)
  - Anti-Terrorism, Crime and Security Act 2001 (ATCSA 2001)

  Such sanctions may be imposed upon persons, organisations, or sectors, and may include measures such as the targeted freezing of assets, and restrictions on a variety of financial markets and services, including but not limited to: investment bans; restriction on access to capital markets; orders to cease banking relationships and activities, or to cease doing all business; requirements to obtain permission before making or receiving certain payments or transfers of funds; or restrictions on the provision of various types of financial, insurance, brokerage, advisory or other services.

  The competent authority for the UK's financial sanctions regime is HM Treasury's Office of Financial Sanctions Implementation (OFSI). Other restrictive measures are administered by other departments of the UK government, such as the implementation of trade sanctions and embargoes by the Department for International Trade (Export Control Organisation) and the implementation of travel bans by the Home Office.

  The UK requires compliance with its financial sanctions by all persons and organisations located within, or undertaking activities within, the territory of the UK, as well as by all UK persons wherever they are located. In addition, all UK nationals and legal entities (including their non-UK branches) established under UK law must also comply with UK financial sanctions, regardless of where their activities take place. In this regard, DNFBPs that conduct business or transactions in British pounds should note that the clearing of British pound-denominated transactions through a UK financial institution or clearing system is an activity that can place funds and their related assets under the jurisdiction of UK financial sanctions programmes.

  Penalties for the violation or circumvention of UK financial sanctions can be severe, depending on the exact nature of the offence and the type of sanction. Current sentencing guidelines may include monetary fines of up to one (1) million pounds sterling, and criminal prosecution with maximum prison terms of up to seven (7) years.

10.4 Sanction Screening, Alert Management, Reporting

In order to fulfil their obligation to comply with the provisions of Cabinet Decision No. (20) of 2019, as well as with the directives of the relevant Competent Authorities and Supervisory Authorities in regard to TFS and other decisions issued by the UN Security Council, and to manage their exposure to the risks associated with unilateral international financial sanctions programmes and restrictive measures implemented by other countries, DNFBPs should take steps to ensure that they have adequate internal policies, procedures and controls in place, commensurate with the nature and size of their businesses. Some of the factors to which supervised institutions should give consideration in this regard include, but are not limited to:

- Organisational roles and responsibilities related to the identification, understanding, assessment, monitoring and management of the risks associated with TFS and other international financial sanctions regimes and restrictive measures;
- Information and operating systems, procedures and controls pertaining to customer and Business Relationship screening, alert management, escalation, and reporting related to TFS and other international financial sanctions regimes and restrictive measures;
- Information and operating systems, policies, procedures and controls related to the implementation of the requirements of TFS and other international financial sanctions regimes and restrictive measures;
- Staff training and awareness-building requirements pertaining to TFS and other international financial sanctions regimes and restrictive measures;
- Appropriate independent audit policies and testing procedures with respect to the operational and control framework for TFS and other international financial sanctions regimes and restrictive measures.

Part V—Appendices

11 Appendices

11.1 Glossary of Terms

Term	Definition
Beneficial Owner:	Natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement.
Beneficiary Financial Institution	The Financial Institution that receives a wire transfer from an Ordering Financial Institution directly or indirectly via an Intermediary Financial Institution and makes funds available to the beneficiary.
Business Relationship	Any ongoing commercial or financial relationship established between Financial Institutions, Designated Non-Financial Businesses and Professions, and their customers in relation to activities or services provided by them.
CBUAE:	Central Bank of United Arab Emirates
Client:	Any person involved in or attempts to carry out any of the activities specified in the Implementing Regulations of this Decree Law with one of the Financial Institutions or designated nonfinancial businesses and professions.
Committee:	National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organisations.
Competent Authorities:	The competent government authorities in the State entrusted with the implementation of any provision of the Decree-Law and the present Decision.
Confiscation:	Permanent expropriation of private funds or proceeds or instrumentalities by an injunction issued by a competent court.
Controlled Delivery:	Process by which a Competent Authority allows the entering or transferring of illegal or suspicious funds or crime revenues to and from the UAE for the purpose of investigating a crime or identifying the identity of its perpetrators.

Term	**Definition**
Core Principles for Financial Supervision:	Basel Committee on Banking Supervision (BCBS) Principles 1-3, 5-9, 11-15, 26, and 29; International Association of Insurance Supervisors (IAIS) Principles 1, 3-11, 18, 21-23, and 25; and International Organisation of Securities Commission (IOSCO) Principles 24, 28, 29 and 31; and Responsibilities A, B, C and D.
Correspondent Banking Relationship:	Relationship between a correspondent financial institution and a respondent one through a current account or any other type of account or through a service related to such an account and includes a corresponding relationship established for the purpose of securities transactions or transfer of funds.
Crime:	Money laundering crime and related Predicate Offences, or Financing of Terrorism or Illegal Organisations.
Customer Due Diligence (CDD):	Process of identifying or verifying the information of a Customer or Beneficial owner, whether a natural or legal person or a Legal Arrangement, and the nature of its activity and the purpose of the Business Relationship and the ownership structure and control over it for the purposes of the Decree-Law and this Decision.
Customer:	Anyone who performs or attempts to perform any of the acts defined in Article 2 and 3 of the present Decision with any Designated Non-financial business or profession.
Decree-Law (or “AML-CFT Law”):	Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations.
Decision (or “AML-CFT Decision” or “Cabinet Decision”):	Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
Designated Nonfinancial Businesses and Professions (DNFBPs):	Anyone who conducts one or several of the commercial or professional activities defined in Article 3 of the present Decision.
Egmont Group:	The Egmont Group is an intergovernmental body of 159 Financial Intelligence Units (FIUs), which provides a platform for the secure exchange of expertise and financial intelligence to combat money laundering and the financing of terrorism (ML/FT).

Term	**Definition**
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.
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 Institutions:	Anyone who conducts one or several of the financial activities or operations of /or on behalf of a Customer.
Financial Transactions or Activities:	Any activity or transaction defined in Article (2) of the present Decision.
Financing of Illegal Organisations:	Any physical or legal action aiming at providing funding to an illegal organisation, or any of its activities or members.
Financing of Terrorism:	Any of the acts mentioned in Articles (29, 30) of Federal Law no. (7) of 2014 on combating terrorism offences.
FIU:	Financial Intelligence Unit.
Freezing or Seizure:	Temporary attachment over the moving, conversion, transfer, replacement or disposition of funds in any form, by an order issued by a Competent Authority.
Funds:	Assets in whatever form, whether tangible, intangible, movable or immovable including national currency, foreign currencies, documents or notes evidencing the ownership of those assets or associated rights in any forms including electronic or digital forms or any interests, profits or income originating or earned from these assets.
Governor:	Governor of the Central Bank

Term	Definition
High Risk Customer:	A customer who represents a risk either in person, activity, Business Relationship, nature or geographical area, such as a customer from a high-risk country or non-resident in a country that does not hold an identity card, or a costumer having a complex structure, performing complex operations or having unclear economic objective, or who conducts cash-intensive operations, or operations with an unknown third party, or operations without directly confronting any other high risk operations identified by Financial Institutions, or Designated Non-Financial Businesses and Professions, or the Supervisory Authority.
Illegal Organisations:	Organisations whose establishment is criminalised or which exercise a criminalised activity.
Intermediary Account:	Corresponding account used directly by a third party to conduct a transaction on its own behalf.
Intermediary Financial Institution:	The Financial Institution that receives and sends wire transfer between the Ordering Financial Institution and the Beneficiary Financial institution or another Intermediary Financial Institution.
Law Enforcement Authorities:	Federal and local authorities which are entrusted under applicable legislation to combat, search, investigate and collect evidences on the crimes including AML/CFT crimes and financing illegal organisations.
Legal Arrangement:	A relationship established by means of a contract between two or more parties which does not result in the creation of a legal personality such as Trusts or other similar arrangements.
Local List:	The List issued by the Cabinet pursuant to Article (3) of Cabinet Decision No. (20) of 2019 Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions.
MENAFATF:	MENAFATF is a FATF-Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with international AML/CFT standards. The UAE is one of the founding members of MENAFATF.
Means:	Any means used or intended to be used for the commitment of an offence or felony.
Minister:	Minister of Finance
Money Laundering:	Any of the acts mentioned in Clause (1) of Article (2) of the Decree-Law.

Term	**Definition**
Non-Profit Organisations (NPOs):	Any organised group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit Legal Arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities.
Politically Exposed Persons (PEPs):	Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation; and the definition also includes the following: 1. Direct family members (Of the PEP, who are spouses, children, spouses of children, parents). 2. Associates known to be close to the PEP, which include: a- Individuals having joint ownership rights in a legal person or arrangement or any other close Business Relationship with the PEP. b- Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.
Predicate Offense:	Any act constituting an offense or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.
Proceeds:	Funds generated directly or indirectly from the commitment of any crime or felony including profits, privileges, and economic interests, or any similar funds converted wholly or partly into other funds.
RBA:	A Risk-Based Approach is a method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk.
Registrar:	Entity in charge of supervising the register of commercial names for all types of establishments registered in the State.
Sanctions Committee:	The UN Security Council Committee established as per resolution nos. 1988 (2011), 1267 (1999), 1989 (2011), 2253 (2015), 1718 (2006) and all other related resolutions.

Term	**Definition**
Sanctions List:	A list wherein individuals and terrorist organizations, which are subject to the Sanctions imposed as per the Security Council Sanctions Committee are listed, along with their personal data and the reasons for Listing.
Settlor:	A natural or legal person who transfers the control of his funds to a Trustee under a document.
Shell Bank	Bank that has no physical presence in the country in which it is incorporated and licensed, and is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
State:	United Arab Emirates
Supervised institutions:	Financial institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) which fall under the scope of Federal Decree-Law No. (20) of 2018 on Facing Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, and of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
Supervisory Authority:	Federal and local authorities, which are entrusted by legislation to supervise Financial Institutions, Designated Non-Financial Businesses and Professions and non-profit organisations or the Competent Authority in charge of approving the pursuit of an activity or a profession in case a supervisory authority is not assigned by legislations.
Suspicious Transactions:	Transactions related to funds for which there are reasonable grounds to believe that they are earned from any misdemeanour or felony or related to the Financing of Terrorism or of illegal organisations, whether committed or attempted.
TFS:	Targeted Financial Sanctions are part of an international sanctions regime issued by the UN Security Council under Chapter (7) of the United Nations Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.
Transaction:	All disposal or use of Funds or proceeds including for example: deposit, withdrawal, conversion, sale, purchase, lending, swap, mortgage, and donation.

Term	**Definition**
Trust:	A legal relationship in which a settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose. These assets constitute funds that are independent of the trustee's own estate, and the rights to the trust assets remain in the name of the settlor or in the name of another person on behalf of the settlor.
Trustee:	A natural or legal person who has the rights and powers conferred to him by the Settlor or the Trust, under which he administers, uses, and acts with the funds of the Settlor in accordance with the conditions imposed on him by either the Settlor or the Trust.
UNODC:	United Nations Office on Drugs and Crime
Undercover Operation:	Process of search and investigation conducted by one of the judicial impoundment officers by impersonating or playing a disguised or false role in order to obtain evidence or information related to the Crime.
Wire Transfer:	Financial transaction conducted by a Financial Institution or through an intermediary institution on behalf of a transferor whose funds are received by a beneficiary in another financial institution, whether or not the transferor and the beneficiary are the same person.

11.2 Useful Links

Institution	URL
Abu Dhabi Global Market	https://www.adgm.com/
Abu Dhabi Securities Exchange	http://www.adx.ae/
Basel Committee on Banking Supervision (BCBS)	http://www.bis.org/bcbs/index.htm
Central Bank of the UAE	https://www.centralbank.ae
Dubai Financial Market	http://www.dfm.ae/
Dubai Financial Services Authority (DFSA)	http://www.dfsa.ae/
Egmont Group	https://egmontgroup.org
FATF	http://www.fatf-gafi.org
Gulf Cooperation Council For The Arab States (GCC)	http://www.gcc-sg.org/
International Organisation of Securities Commissions (IOSCO)	http://www.iosco.org/
Interpol/Money Laundering	http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/default.asp
MENAFATF	http://www.menafatf.org/
Securities and Commodities Authority	http://www.sca.ae/
United Nations	http://www.un.org/
United Nations Office on Drugs & Crime – Global Programme Against Money Laundering	http://www.unodc.org/unodc/money-laundering/index.html
Wolfsberg Group	https://www.wolfsberg-principles.com/