Appendix 1

The DFSA Rulebook

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module

(AML)

Contents

The contents of this module are divided into the following chapters, sections and appendices:

1 INTRODUCTION 3

1.1 Application 3
1.2 Responsibility for compliance with this module 3
1.3 Application table 4

2 OVERVIEW AND PURPOSE OF THE MODULE 5

3 INTERPRETATION AND TERMINOLOGY 9

3.1 Interpretation 9
3.2 Glossary for AML 9

4 APPLYING A RISK-BASED APPROACH 16

4.1 The risk-based approach 17

5 BUSINESS RISK ASSESSMENT 18

5.1 Assessing business AML risks 18
5.2 AML systems and controls 20

6 CUSTOMER RISK ASSESSMENT 21

6.1 Assessing customer AML risks 22

7 CUSTOMER DUE DILIGENCE 28

7.1 Requirement to undertake customer due diligence 29
7.2 Timing of customer due diligence 29
7.3 Customer due diligence requirements 31
7.4 Enhanced customer due diligence 37
7.5 Simplified customer due diligence 39
7.6 Ongoing customer due diligence 40
7.7 Failure to conduct or complete customer due diligence 41

8 RELIANCE AND OUTSOURCING 43

8.1 Reliance on a third party 43
8.2 Outsourcing 45
8.3 Money Service Providers 46

9 CORRESPONDENT BANKING, ELECTRONIC FUND TRANSFERS AND AUDIT 47

9.1 Application 47
9.2 Correspondent banking 47
9.3 Electronic fund transfers 48
9.3A Additional requirements for Crypto Token transfers 52
9.3B Additional requirements for NFT and Utility Token transfers 53

9.4 Audit 53

10 SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS 54

10.1 Application 54
10.2 Relevant United Nations resolutions and sanctions 54
10.3 Government, regulatory and international findings 54

11 MONEY LAUNDERING REPORTING OFFICER 58

11.1 Application 58
11.2 Appointment of a MLRO 58
11.3 Qualities of a MLRO 59
11.4 Responsibilities of a MLRO 60

12 AML TRAINING AND AWARENESS 61

12.1 Training and awareness 61

13 SUSPICIOUS ACTIVITY REPORTS 63

13.1 Application and definitions 63
13.2 Internal reporting requirements 63
13.3 Suspicious activity report 64
13.4 Tipping-off 65
13.5 Freezing assets 65

14 GENERAL 66

14.1 Groups, branches and subsidiaries 66
14.2 Group policies 67
14.3 Notifications 67
14.4 Record keeping 67
14.5 Annual AML return 69
14.6 Communication with the DFSA 70
14.7 Employee disclosures 70
14.8 Decision making procedures 70

15 DNFBP REGISTRATION AND SUPERVISION 71

15.1 Registration and notifications 71
15.2 Request to withdraw registration 72
15.3 Disclosure of regulatory status 73
15.3A Whistleblowing 73
15.4 Transitional 75

16 TRANSITIONAL RULES 77

16.1 Application 77
16.2 General 77
16.3 Specific relief – Ancillary Service Provider and DNFBPs 77

1 INTRODUCTION

1.1 Application

1.1.1 This module (AML) applies to:

(a) every Relevant Person in respect of all its activities carried on in or from the DIFC;

(b) the persons specified in Rule 1.2.1 as being responsible for a Relevant Person's compliance with this module; and

(c) a Relevant Person, which is a DIFC entity, to the extent required by Rule 14.1.

except to the extent that a provision of AML provides for a narrower application.

1.1.2 For the purposes of these Rules, a Relevant Person means:

(a) an Authorised Firm other than a Credit Rating Agency;

(b) an Authorised Market Institution;

(c) a DNFBP; or

(d) a Registered Auditor.

1.2 Responsibility for compliance with this module

1.2.1 (1) Responsibility for a Relevant Person's compliance with this module lies with every member of its senior management.

(2) In carrying out their responsibilities under this module every member of a Relevant Person's senior management must exercise due skill, care and diligence.

(3) Nothing in this Rule precludes the DFSA from taking enforcement action against any person including any one or more of the following persons in respect of a breach of any Rule in this module:

(a) a Relevant Person;

(b) members of a Relevant Person's senior management; or

(c) an Employee of a Relevant Person.

1.3 Application table

Guidance

Relevant Person	Applicable Chapters	
Authorised Person	**1 - 14**	
Representative Office	**1 - 5***	**10- 14**
Registered Auditor	**1 -8**	**10 - 14**
DNFBP	**1 - 15**	

* Chapters 6 – 9 are unlikely to apply to a Representative Office as such an office is only permitted to carry on limited activities in the DIFC and therefore must not have Customers.

2 OVERVIEW AND PURPOSE OF THE MODULE

Guidance

1. In this module, for simplicity, a reference to "money laundering" also includes terrorist financing, the financing of illegal organisations and proliferation financing (see Rule 3.1.1).

Overview of the DIFC's AML regime

2. The DIFC is governed by two separate and complementary regimes in relation to AML regulation, both administered by the DFSA:

   a. The Federal regime: Under Article 3 of Federal Law No. 8 of 2004, the provisions of Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations and Federal Law No. 7 of 2014 on Combating Terrorism Offences and the implementing regulations under those laws apply in the DIFC. The DFSA, as the DIFC's supervisory authority for Relevant Persons for the purposes of those laws, is obliged to supervise and monitor Relevant Persons for compliance with provisions of the Federal laws and regulations. The DFSA may also impose administrative penalties for breaches of those laws and the implementing regulations. See Article 14 of Federal Law No. 20 of 2018, Article 44 of Cabinet Decision No. 10 of 2019, and Article 22 of Cabinet Decision No. 74 of 2020; and

   b. The DIFC regime: Under Article 70(3) of the DIFC Regulatory Law 2004 (the "Regulatory Law"), the DFSA has jurisdiction for the regulation of anti-money laundering in the DIFC relating to Relevant Persons (see para 4 below) and their officers, employees and agents. The DIFC specific regime is contained in Chapter 2 of Part 4 of the Regulatory Law and any DFSA Rules made in connection with anti-money laundering measures, policies and procedures.

3. Note that under Article 71(1) of the Regulatory Law, the DIFC regime requires compliance with the Federal regime. It follows that a failure to comply with a provision of Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations or Federal Law No. 7 of 2014 on Combating Terrorism Offences or the implementing regulations under those laws may also provide evidence of failure to comply with Article 71(1), which may then be addressed under the disciplinary and remedial provisions of the Regulatory Law and DFSA Rules.

Purpose of the AML module

4. The AML module has been designed to provide a single reference point for all persons and entities (collectively called Relevant Persons) referred to in Rule 1.1.2 who are supervised by the DFSA for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and sanctions compliance. Accordingly it applies to Authorised Firms (other than Credit Rating Agencies), Authorised Market Institutions, Designated Non-Financial Businesses and Professions (DNFBPs), and Registered Auditors. The AML module takes into consideration the fact that Relevant Persons have differing AML risk profiles. A Relevant Person should familiarise itself with this module, and assess the extent to which the chapters and sections apply to it.

5. The AML module cannot be read in isolation from other relevant U.A.E. legislation or developments in international policy and best practice and, to the extent applicable, Relevant Persons need to be aware of, and take into account, how these aforementioned matters may impact on the Relevant Person's day to day operations. This is particularly relevant when considering the list of persons and terrorist organisations issued under Cabinet Decision No. 74 of 2020 and the United Nations Security Council Resolutions (UNSCRs) which apply in the DIFC, and unilateral sanctions imposed by other jurisdictions which may apply to a Relevant Person depending on the Relevant Person's jurisdiction of origin, its business and/or customer base.

Structure of the AML module

6. Chapter 1 of this module contains an application table which should assist a Relevant Person to navigate through the module and to determine which chapters are applicable to it. Chapter 1 also specifies who is ultimately responsible for a Relevant Person's compliance with the AML module. The DFSA expects the senior management of a Relevant Person to establish a robust and effective AML/CTF and sanctions compliance culture for the business.

7. Chapter 2 provides an overview of the AML module and chapter 3 sets out the key definitions in the module. Note that not all definitions used in this module are capitalised.

8. Chapter 4 explains the meaning of the risk-based approach (RBA), which should be applied when complying with this module. The RBA requires a risk-based assessment of a Relevant Person's business (in chapter 5) and its customers (in chapter 6). A risk-based assessment should be a dynamic process involving regular review, and the use of these reviews to establish the appropriate processes to match the levels of risk. No two Relevant Persons will have the same approach, and implementation of the RBA and the AML module permits a Relevant Person to design and implement systems that should be appropriate to their business and customers, with the obvious caveat being that such systems should be reasonable and proportionate in light of the AML risks. The DFSA expects the RBA to determine the breadth and depth of the Customer Due Diligence (CDD) which is undertaken for a particular customer under chapter 7, though the DFSA understands that there is an inevitable overlap between the risk-based assessment of the customer in chapter 6 and CDD in chapter 7. This overlap may occur at the initial stages of customer on-boarding but may also occur when undertaking on-going CDD.

9. Chapter 8 sets out when and how a Relevant Person may rely on a third party to undertake all or some of its CDD obligations. Reliance on a third-party CDD reduces the need to duplicate CDD already performed for a customer. Alternatively, a Relevant Person may outsource some or all of its CDD obligations to a service provider.

10. Chapter 9 sets out certain obligations in relation to correspondent banking, wire transfers, the transfer of Crypto Tokens and other matters which (except for section 9.3B) apply to Authorised Persons, and, in particular, to banks. Section 9.3B applies to DNFBPs which send or receive NFTs or Utility Tokens.

11. Chapter 10 sets out a Relevant Person's obligations in relation to United Nations Security Council resolutions and sanctions, and government, regulatory and international findings (in relation to AML, terrorist financing and the financing of weapons of mass destruction).

12. Chapter 11 sets out the obligation for a Relevant Person to appoint a Money Laundering Reporting Officer (MLRO) and the responsibilities of such a person.

13. Chapter 12 sets out the requirements for AML training and awareness. A Relevant Person should adopt the RBA when complying with chapter 12, so as to make its training and awareness proportionate to the AML risks of the business and the employee role.

14. Chapter 13 contains the obligations applying to all Relevant Persons concerning Suspicious Activity Reports, which are required to be made under Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

15. Chapter 14 contains the general obligations applying to all Relevant Persons, including Group policies, notifications, record-keeping requirements and the annual AML Return.

16. Chapter 15 sets out specific Rules applying to DNFBPs, including the requirement to register with the DFSA, and Chapter 16 contains certain transitional Rules.

The U.A.E. criminal law

17. The U.A.E. criminal law applies in the DIFC and, therefore, persons in the DIFC must be aware of their obligations in respect of the criminal law as well as these Rules. Relevant U.A.E. criminal laws include Federal Law No. 20 of 2018 on Anti-Money Laundering and

Combating the Financing of Terrorism and Illegal Organisations, Federal Law No. 7 of 2014 on Combating Terrorism Offences and the Penal Code of the U.A.E.

18. Under Federal AML legislation a Person may be criminally liable for certain conduct, such as:

    a. money laundering;

    b. financing terrorism;

    c. financing illegal organisations;

    d. 'tipping off';

    e. violation of sanctions;

    f. failure to declare currency or precious metals brought into or taken out of the U.A.E.

19. The U.A.E Central Bank has the power under Federal AML legislation to freeze funds or other assets suspected of relating to money laundering, terrorist financing or the financing of illegal organisations. Other Federal authorities also have powers to apply for the freezing or confiscation of funds or other assets that have been used for such purposes.

20. In a number of places in this module, Guidance cross-refers to specific requirements in Federal AML legislation. Rules or Guidance in this module should not be relied upon to interpret or determine the application of the Federal AML legislation. Relevant Persons should refer to the guidelines issued under the Federal AML legislation to understand their obligations under that legislation.

Financial Action Task Force

21. The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of international standards to combat money laundering and terrorist financing.

22. The DFSA has had regard to the FATF Recommendations in making these Rules. A Relevant Person may wish to refer to the FATF Recommendations and interpretive notes to assist it in complying with these Rules. However, in the event that a FATF Recommendation or interpretive note conflicts with a Rule in this module, the relevant Rule takes precedence.

23. A Relevant Person may also wish to refer to the FATF typology reports which may assist in identifying new money laundering threats and which provide information on money laundering and terrorist financing methods. The FATF typology reports cover many pertinent topics for Relevant Persons, including corruption, new payment methods, money laundering using trusts and company service providers, and vulnerabilities of free trade zones. These typology reports can be found on the FATF website www.fatf-gafi.org.

24. The U.A.E., as a member of the United Nations, is required to comply with sanctions issued and passed by the United Nations Security Council (UNSC). These UNSC obligations apply in the DIFC and their importance is emphasised by specific obligations contained in this module requiring Relevant Persons to establish and maintain effective systems and controls to comply with UNSC sanctions and resolutions (See chapter 10).

25. The FATF has issued guidance on a number of specific UNSC sanctions and resolutions regarding the countering of the proliferation of weapons of mass destruction. Such guidance has been issued to assist in implementing the targeted financial sanctions and activity based financial prohibitions. This guidance can be found on the FATF website www.fatf-gafi.org.

26. In relation to unilateral sanctions imposed in specific jurisdictions such as the European Union, the U.K. (HM Treasury) and the U.S. (Office of Foreign Assets Control), the DFSA expects a Relevant Person to consider and take positive steps to ensure compliance where required or appropriate.

Tax Issues and Exchange of Information for Tax purposes

27. The DIFC benefits from an international customer base with a growing number of customers who may be investing with financial institutions outside their country of residence. These factors create a risk of the services of Relevant Persons being used to hide assets which are subject to taxation, or to launder the unlawful proceeds of tax crimes.

28. The DFSA is committed to protecting the DIFC from being used to facilitate tax crimes and believes that strong AML policies, procedures, systems and controls, including robust customer due diligence requirements, are needed to mitigate the risk of tax crimes.

29. Such measures will also ensure that a Relevant Person is able to comply with other international obligations such as the OECD Automatic Exchange of Information for Tax Purposes Programme and FATF Recommendations, which were updated in 2012 to expand the scope of money laundering predicate offences to include tax crimes (related to direct and indirect taxes).

30. A Relevant Person should therefore establish and maintain appropriate policies, procedures, systems and controls to enable it to detect and deter the laundering of proceeds of tax crimes. For example, as part of its risk-based approach under chapter 4, it should consider its tax risk exposure as a result of the nature of its business, customers, products, services and other relevant factors. It should also conduct appropriate customer due diligence to identify customers who may be subject to tax crime risk (see also the Guidance after Rule 6.1.4).

Virtual Asset Service Providers

31. Federal Cabinet Resolution No. 10 of 2019 applies the requirements under Federal AML legislation to Virtual Asset Service Providers (VASPs), in addition to Financial Institutions and DNFBPs. The DFSA's AML regime applies in addition to the Federal AML legislation. For the purposes of the DFSA's AML regime, VASPs will typically be Authorised Firms or Authorised Market Institutions.

NFTs and Utility Tokens

32. The DFSA excludes a Non-Fungible Token (NFT) and a Utility Token from its Crypto Token definition where such a Token meets specified criteria (see GEN A2.5). The DFSA has, however, prescribed in AML Rule 3.2.1 that a person who carries on the business or profession of issuing or providing services related to a NFT or Utility Token is a DNFBP. An exclusion applies, in the case of an issuer, if the value of each NFT or Utility Token issued is less than $15,000 and, in the case of a service provider, if the service is IT support or advice to an issuer.

Dealers in precious metals or precious stones

33. The Regulatory Law requires a person who carries on a Designated Non-Financial Business or Profession (DNFBP) in or from the DIFC to be registered by the DFSA. In the case of a dealer in precious metals or precious stones, the DNFBP definition applies to a dealer which carries out a single cash transaction, or several cash transactions that appear to be connected, with a value of $15,000 or more. Therefore, a dealer in precious metals or precious stones will not have to register as a DNFBP if it can ensure that the value of each transaction it carries out (single or connected) is under that threshold.

3 INTERPRETATION AND TERMINOLOGY

3.1 Interpretation

3.1.1 A reference in this module to "money laundering" in lower case includes a reference to terrorist financing, the financing of illegal organisations and proliferation financing, unless the context provides or implies otherwise.

Guidance

Chapter 6, section 6.2, of the General (GEN) module sets out how to interpret the Rulebook, including this module.

3.2 Glossary for AML

Guidance

1. In order to make this module easier to read, some of the defined terms in this module have not had the initial letter of each word capitalised in the same way as in other Rulebook modules.

2. Some of the defined terms and abbreviations in this module may also be found in the DFSA's Glossary module (GLO). Where a defined term in this module does not appear in Rule 3.2.1, a Relevant Person should look in GLO to find the meaning. In addition, Rule 9.3.2 of this module sets out definitions relevant to section 9.3 (Electronic fund transfers).

3. In accordance with the interpretation provisions in the Regulatory Law, a reference to legislation includes a reference to the legislation as amended or re-enacted from time to time.

3.2.1 In this module, the terms and abbreviations listed in the table below have the following meanings:

AML	Means either "anti-money laundering" or this Anti-Money Laundering, Counter-Terrorist Financing and Sanctions module, depending on the context.
Authorised Person	Means an Authorised Firm or an Authorised Market Institution.
Beneficial Owner	(1) In relation to a customer, means a natural person who ultimately owns or controls the customer or a natural person on whose behalf a transaction is conducted or a business relationship is established, and includes: (a) in relation to a body corporate, a person referred to in Rule 7.3.3 (2) or (4); (b) in relation to a foundation, a person referred to in Rule 7.3.5 (2) or (3); and (c) in relation to a trust or other similar legal arrangement, a person referred to in Rule 7.3.6 (2) or (3). (2) In relation to a beneficiary of a life insurance or other similar policy, means a natural person who ultimately

	owns or controls the beneficiary.
body corporate	Any body corporate, including a limited liability partnership, whether constituted under the law of the DIFC, an Emirate, the State or any other country or territory.
Branch	Means a place of business within the DIFC: (a) which has no separate legal personality; (b) which forms a legally dependant part of a Relevant Person whose principal place of business and head office is in a jurisdiction other than the DIFC; and (c) through which the Relevant Person carries on business in or from the DIFC.
Cabinet Decision No. 10 of 2019	Means Federal Cabinet Decision No. 10 of 2019 on the Implementing Regulations of Federal Law No. 20 of 2018.
Cabinet Decision No. 74 of 2020	Means Federal Cabinet Decision No. 74 of 2020 regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing, and Related Resolutions.
Client	Has the meaning in chapter 2 of the Conduct of Business module.
company service provider	Means a person, not falling into parts (1)(a) to (e) or (g) of the definition of a DNFBP that, by way of business, provides any of the following services to a customer: (a) acting as a formation agent of legal persons; (b) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; (c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; or (d) acting as (or arranging for another person to act as) a nominee shareholder for another person.
Contract of Insurance	Has the meaning in GEN Rule A4.1.1.
CTF	Means counter-terrorist financing.
customer	Unless otherwise provided, means: (a) a person where, in relation to a business relationship between the person and a Relevant Person, there is a firm intention or commitment by each party to enter into a contractual relationship or where there is a firm

	commitment by each party to enter into a transaction, in connection with a product or service provided by the Relevant Person; (b) a Client of an Authorised Firm; (c) a Member or prospective Member of, or an applicant for admission of Securities to trading on, an Authorised Market Institution; or (d) a person with whom a Relevant Person is otherwise establishing or has established a business relationship.
Customer Due Diligence (CDD)	Means the measures referred to in section 7.3.
Designated Non-Financial Business or Profession (DNFBP)	Means: (1) The following class of persons whose business or profession is carried on in or from the DIFC: (a) a real estate developer or agency which carries out transactions with a customer involving the buying or selling of real property; (b) a dealer in precious metals or precious stones which carries out any single cash transaction or several transactions that appear to be connected and the value of which is equal to or greater than $15,000; (c) a person who issues, or provides services relating to, Non-Fungible Tokens or Utility Tokens unless; (i) in the case of an issuer of a NFT or Utility Token, each issue involves a single transaction, or multiple transactions that are interrelated, that are equal to or less than $15,000 in value; or (ii) in the case of a service relating to a NFT or Utility Token, the service is providing technology support or technology advice to an issuer; (d) a law firm, notary firm, or other independent legal business; (e) an accounting firm, audit firm or insolvency firm; or (f) a company service provider. (2) A person who is an Authorised Person or a Registered Auditor is not a DNFBP.

DIFC entity	Means a legal person which is incorporated or registered in the DIFC (excluding a registered Branch).
Domestic Fund	A Fund established or domiciled in the DIFC.
Employee	Means an individual: (a) who is employed or appointed by a person in connection with that person's business, whether under a contract of service or for services or otherwise; or (b) whose services, under an arrangement between that person and a third party, are placed at the disposal and under the control of that person.
Enhanced Customer Due Diligence	Means undertaking Customer Due Diligence and the enhanced measures under Rule 7.4.1.
FATF	Means the Financial Action Task Force.
FATF Recommendations	Means the publication entitled the "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation" as published and amended from time to time by FATF.
Federal AML legislation	Means all U.A.E Federal Laws and their implementing regulations relating to money laundering, terrorist financing, the financing of illegal organisations and proliferation financing, as well as sanctions compliance, including Federal Law No. 20 of 2018, Federal Law No. 7 of 2014, Cabinet Decision No. 10 of 2019 and Cabinet Decision No. 74 of 2020.
Federal Law No. 20 of 2018	Means U.A.E Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.
Federal Law No. 7 of 2014	Means U.A.E Federal Law No. 7 of 2014 on Combating Terrorism Offences.
FIU	The Financial Intelligence Unit of the U.A.E.
Financial Institution	A regulated or unregulated entity, whose activities are primarily financial in nature.
Financial Services Regulator	Means a regulator of financial services activities established in a jurisdiction other than the DIFC.
foundation	Means a foundation established under the DIFC Foundations Law 2018 or under any other law.
Governing Body	Means the board of directors, partners, committee of

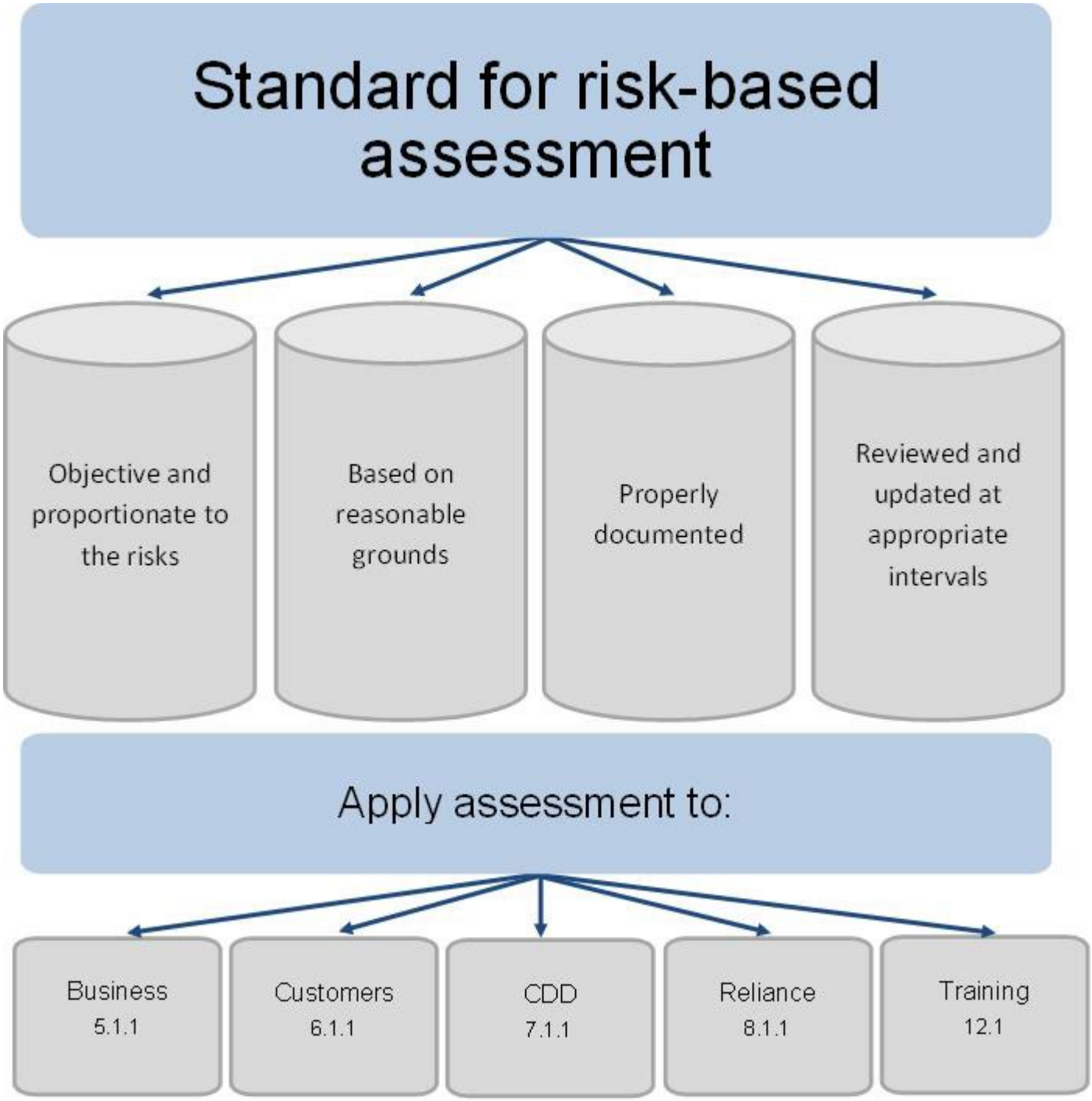
	management or other governing body of: (a) a Body Corporate or Partnership; or (b) an unincorporated association carrying on a trade or business, with or without a view to profit.
Group	Means a Group of entities which includes an entity (the 'first entity') and: (a) any parent of the first entity; and (b) any subsidiaries (direct or indirect) of the parent or parents in (a) or the first entity; or (c) for a legal person which is not a body corporate, refers to that person and any other associated legal persons who are in an equivalent relationship to that in (a) and (b).
Illegal Organisation	An organisation the establishment or activities of which have been declared to be criminal under Federal AML legislation.
IMF	The International Monetary Fund.
International Organisation	Means an organisation established by formal political agreement between member countries, where the agreement has the status of an international treaty, and the organisation is recognised in the law of countries which are members.
Law	Means the Regulatory Law.
legal arrangement	Means an express trust or any other similar legal arrangement.
legal person	Means any entity other than a natural person that can establish a customer relationship with a Relevant Person or otherwise own property. This can include companies, bodies corporate or unincorporate, foundations, anstalten, partnerships, associations, states and governments and other relevantly similar entities.
Member	A person admitted as a member of an Authorised Market Institution in accordance with its Business Rules.
MENAFATF	The Middle East and North Africa Financial Action Task Force.
Money Laundering Reporting Officer (MLRO)	Means the person appointed by a Relevant Person pursuant to Rule 11.2.1(1).
natural person	Means an individual.
Non-Fungible Token	Means a Token referred to in GEN Rule A2.5.3.
OECD	The Organisation for Economic Co-operation and

	Development.
person	Means a natural or legal person.
Politically Exposed Person (PEP)	Means a natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, whether in the State or elsewhere, including but not limited to, a head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior person in an International Organisation, senior executive of a state owned corporation, an important political party official, or a member of senior management or an individual who has been entrusted with similar functions such as a director or a deputy director. This definition does not include middle ranking or more junior individuals in the above categories.
proliferation financing	financing the proliferation of weapons of mass destruction.
Registered Auditor	Has the meaning given to that term in the Regulatory Law.
Regulated Exchange	Means an exchange regulated by a Financial Services Regulator.
Regulated Financial Institution	A person who does not hold a Licence but who is authorised in a jurisdiction other than the DIFC to carry on any financial service by another Financial Services Regulator.
Relevant Person	Has the meaning given to that term in Rule 1.1.2.
senior management	Means: (1) Except in AML Rules 7.3.8(2)(a), 7.3.8(3)(a), 7.4.1(e) and 9.2.1(e), in relation to a Relevant Person every member of the Relevant Person's executive management and includes: (a) for a DIFC entity, every member of the Relevant Person's Governing Body; (b) for a Branch, the person or persons who control the day to day operations of the Relevant Person in the DIFC and would include, at a minimum, the senior executive officer or equivalent officer, such as the managing director; or (c) for a Registered Auditor, every member of the Relevant Person's executive management in the U.A.E. (2) In AML Rules 7.3.8(2)(a), 7.3.8(3)(a), 7.4.1(e) and 9.2.1(e), a member of the executive management of the Relevant Person who has significant responsibility for the management of the Relevant Person's money

	laundering risk exposure. (3) In relation to a customer that is a body corporate, every member of the body corporate's Governing Body and the person or persons who control the day-to-day operations of the body corporate, including its senior executive officer, chief operating officer and chief financial officer.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated or licensed and which is not affiliated with a regulated financial group that is subject to effective consolidated supervision.
Simplified Customer Due Diligence	Means Customer Due Diligence as modified under Rule 7.5.1.
source of funds	Means the origin of funds which relate to a transaction or service and includes how such funds are connected to the source of wealth of a customer or Beneficial Owner.
source of wealth	Means how the global wealth or net worth of a customer or Beneficial Owner is or was acquired or accumulated.
State	Means the U.A.E.
Suspicious Activity Report (SAR)	Means a report regarding suspicious activity (including a suspicious transaction) made to the FIU under Federal Law No. 20 of 2018 and Cabinet Decision No. 10 of 2019.
transaction	Means any transaction undertaken by a Relevant Person for or on behalf of a customer in the course of carrying on a business in or from the DIFC.
Utility Token	Means a Token referred to in GEN A2.5.4.
Virtual Asset Service Provider (VASP)	Has the meaning given in Cabinet Decision No. 10 of 2019.

4 APPLYING A RISK-BASED APPROACH

Figure 1. The Risk-Based Approach (RBA)



4.1 The risk-based approach

4.1.1 A Relevant Person must:

(a) assess and address its AML risks under this module by reviewing the risks to which the person is exposed as a result of the nature of its business, customers, products, services and any other matters which are relevant in the context of money laundering and then adopting a proportionate approach to mitigate those risks; and

(b) ensure that, when undertaking any risk-based assessment for the purposes of complying with a requirement of this module, such assessment is:

(i) objective and proportionate to the risks;

(ii) based on reasonable grounds;

(iii) properly documented; and

(iv) reviewed and updated at appropriate intervals.

Guidance

1. Rule 4.1.1 requires a Relevant Person to adopt an approach to AML which is proportionate to the risks. This is called the "risk-based approach" ("RBA") and is illustrated in figure 1 above. The DFSA expects the RBA to be a key part of the Relevant Person's money laundering compliance culture and to cascade down from the senior management to the rest of the organisation. Embedding the RBA within its business allows a Relevant Person to make decisions and allocate AML resources in the most efficient and effective way.

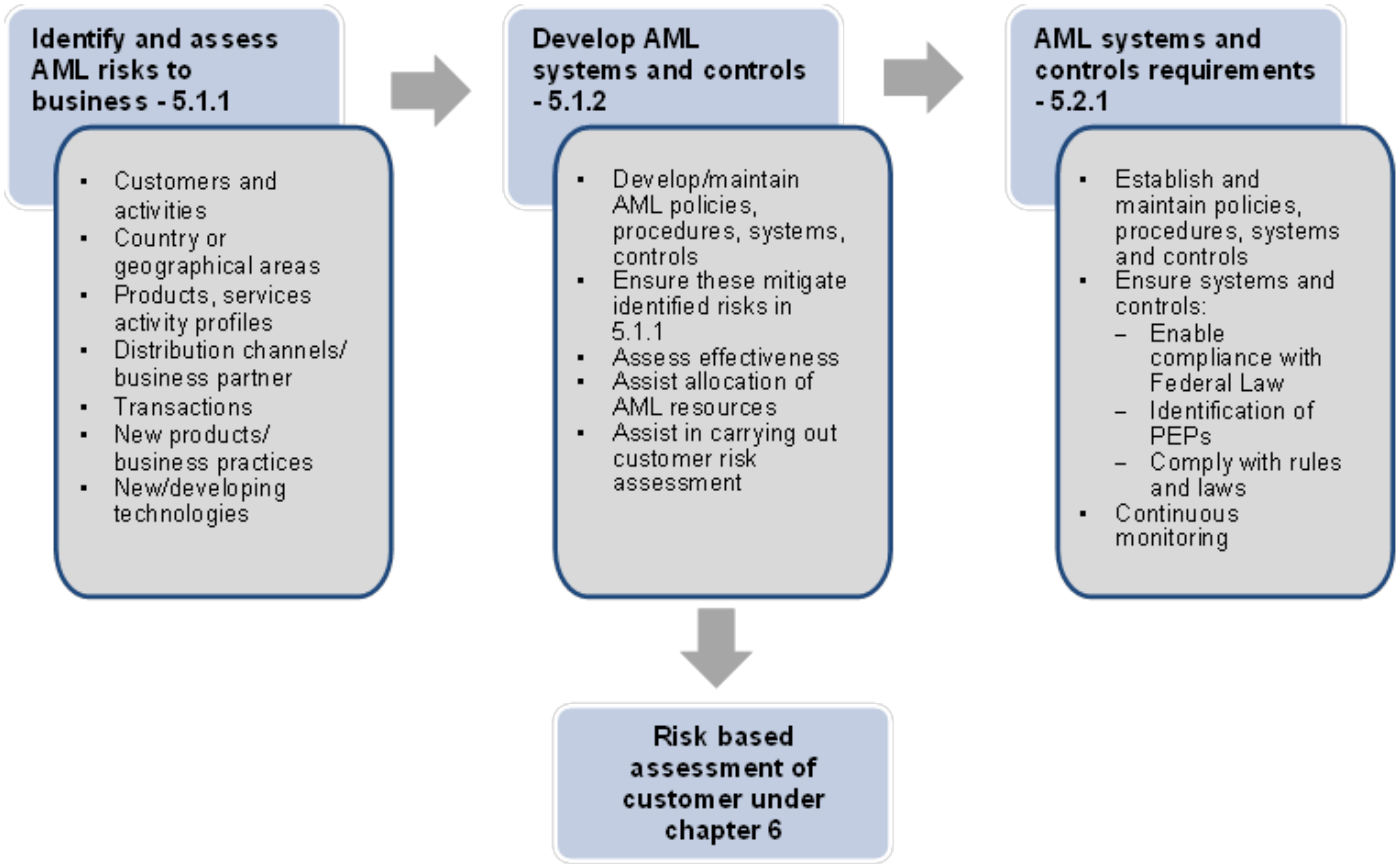
2. In implementing the RBA, a Relevant Person is expected to have in place processes to identify and assess money laundering risks. After the risk assessment, the Relevant Person is expected to monitor, manage and mitigate the risks in a way that is proportionate to the Relevant Person's exposure to those money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted.

3. The RBA discourages a "tick-box" approach to AML. Instead a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks. The outcome of using the RBA is akin to using a sliding scale, where the type of CDD undertaken on each customer will ultimately depend on the outcome of the risk-based assessment made of such customer under this chapter.

4. The Rules regarding record-keeping for the purposes of this module are in section 14.4. These Rules apply in relation to Rule 4.1.1(b)(iii).

5 BUSINESS RISK ASSESSMENT

Figure 2. Business risk-based assessment



5.1 Assessing business AML risks

5.1.1 A Relevant Person must:

(a) take appropriate steps to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities;

(b) when identifying and assessing the risks in (a), take into account, to the extent relevant, any vulnerabilities relating to:

(i) its type of customers and their activities;

(ii) the countries or geographic areas in which it does business;

(iii) its products, services and activity profiles;

(iv) its distribution channels and business partners;

(v) the complexity and volume of its transactions;

(vi) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and

(vii) the use of new or developing technologies for both new and pre-existing products;

(c) take appropriate measures to ensure that any risk identified as part of the assessment in (a) is taken into account in its day-to-day operations, including in relation to:

(i) the development of new products, business practices and technologies referred to in Rule 5.1.3;

(ii) the taking on of new customers; and

(iii) changes to its business profile.

5.1.2 A Relevant Person must use the information obtained in undertaking its business risk assessment to:

(a) develop and maintain its AML policies, procedures, systems and controls required by Rule 5.2.1;

(b) ensure that its AML policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 5.1.1;

(c) assess the effectiveness of its AML policies, procedures, systems and controls as required by Rule 5.2.1(c);

(d) assist in allocation and prioritisation of AML resources; and

(e) assist in the carrying out of the customer risk assessment under chapter 6.

New products, business practices and technologies

5.1.3 (1) This Rule applies in relation to:

(a) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and

(b) the use of new or developing technologies for both new and existing products.

(2) Without limiting Rules 5.1.1 and 5.1.2, a Relevant Person must take reasonable steps to ensure that it has:

(a) assessed and identified the money laundering risks relating to the product, business practice or technology; and

(b) taken appropriate steps to manage and mitigate the risks identified under (a),

before it launches or uses the new product, practice or technology.

Guidance

1. Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, and the nature of the products and services sold.

2. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers under chapter 6.

3. Under Article 4 of Cabinet Decision No.10 of 2019, in assessing its money laundering risks and taking steps to mitigate those risks, a Relevant Person is required to take into consideration the results of the National Risk Assessment prepared by the National Anti-Money Laundering and Combating Financing of Terrorism Committee (NAMLCFTC).

5.2 AML systems and controls

5.2.1 A Relevant Person must:

(a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Relevant Person and its activities;

(aa) ensure that its policies, procedures, systems and controls in (a) are appropriately tailored to the nature, scale and complexity of its activities;

(b) ensure that its systems and controls in (a):

(i) include the provision to the Relevant Person's senior management of regular management information on the operation and effectiveness of its AML systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering risks; and

(ii) enable it to determine:

(A) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP); and

(B) if it provides a customer with a life insurance or other similar policy, whether a beneficiary of the policy, or a Beneficial Owner of the beneficiary, is a PEP; and

(iii) enable the Relevant Person to comply with these Rules and Federal AML legislation; and

(c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

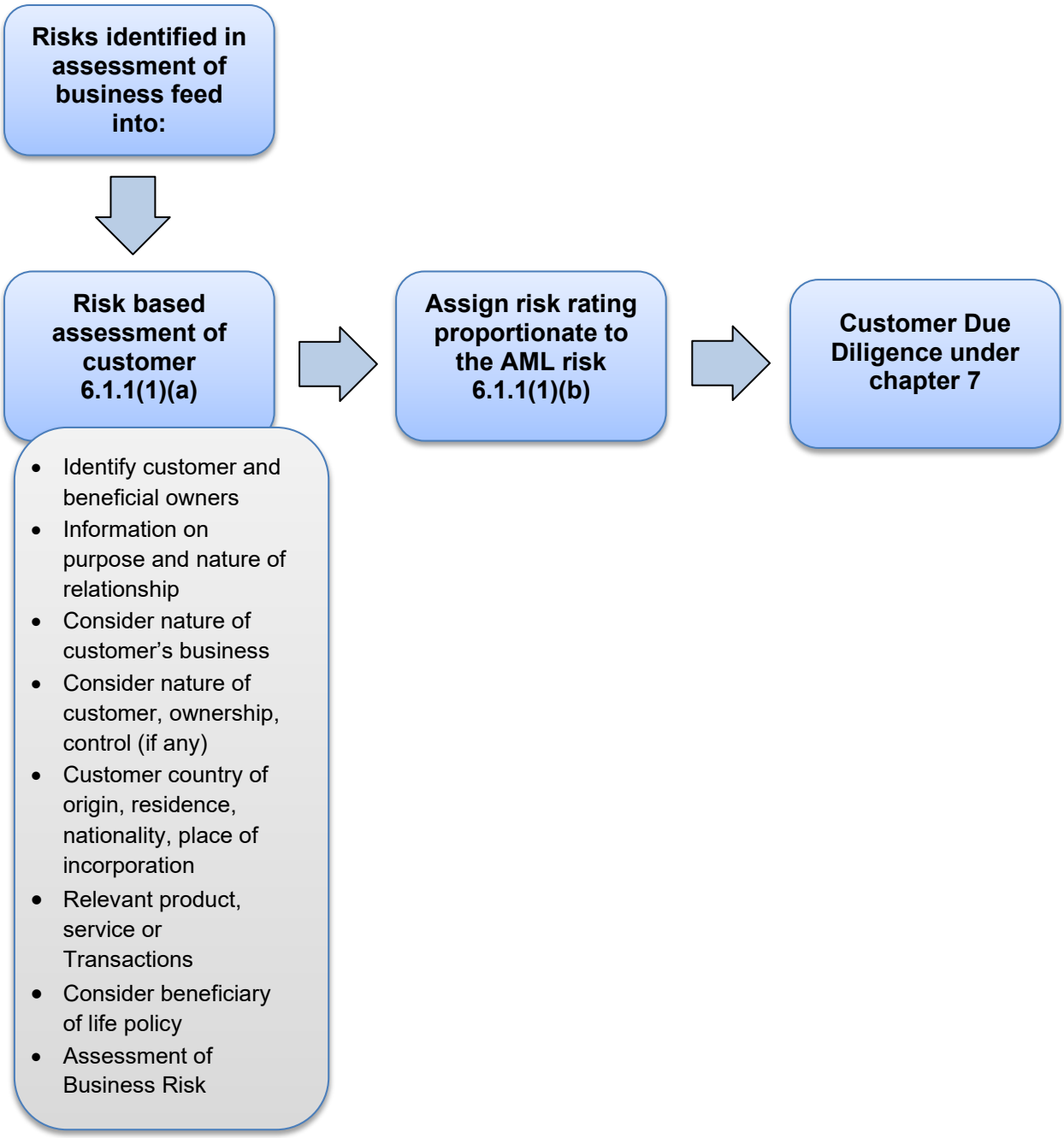
Guidance

1. Under Rule 5.2.1(aa), a Relevant Person is required to ensure that its policies, procedures, systems and controls for the prevention of money laundering are tailored to its risk profile, business model and activities. Generic policies and procedures would not meet that requirement.

2. In Rule 5.2.1(c) the regularity of risk assessments will depend on the nature, size and complexity of the Relevant Person's business and also on when any material changes are made to its business.

6 CUSTOMER RISK ASSESSMENT

Figure 3. Customer risk-based assessment



Guidance

1. This chapter prescribes the risk-based assessment that must be undertaken by a Relevant Person on a customer and the proposed business relationship, transaction or product. The outcome of this process is to produce a risk rating for a customer, which determines the level of Customer Due Diligence (CDD) which will apply to that customer under chapter 7. That chapter prescribes the requirements of CDD and of Enhanced CDD for high risk customers and Simplified CDD for low risk customers.

2. CDD in the context of AML refers to the process of identifying a customer, verifying such identification and monitoring the customer's business and money laundering risk on an on-

going basis. CDD is required to be undertaken following a risk-based assessment of the customer and the proposed business relationship, transaction or product.

3. Relevant Persons should note that the ongoing CDD requirements in Rule 7.6.1 require a Relevant Person to ensure that it reviews a customer's risk rating to ensure that it remains appropriate in light of the AML risks.

4. The DFSA is aware that in practice there will often be some degree of overlap between the customer risk assessment and CDD. For example, a Relevant Person may undertake some aspects of CDD, such as identifying a Beneficial Owner, when it performs a risk assessment of the customer. Conversely, a Relevant Person may also obtain relevant information as part of CDD which has an impact on its customer risk assessment. An example of such relevant information is information on the ownership and control structure of the customer. Where information obtained as part of CDD of a customer affects the risk rating of a customer, the change in risk rating should be reflected in the degree of CDD undertaken.

6.1 Assessing customer AML risks

6.1.1 (1) A Relevant Person must:

(a) undertake a risk-based assessment of every customer; and

(b) assign the customer a risk rating proportionate to the customer's money laundering risks.

(2) The customer risk assessment in (1) must be completed prior to undertaking Customer Due Diligence for new customers, and whenever it is otherwise appropriate for existing customers.

(3) When undertaking a risk-based assessment of a customer under (1)(a) a Relevant Person must:

(a) identify the customer and any Beneficial Owner;

(b) obtain information on the purpose and intended nature of the business relationship;

(c) obtain information on, and take into consideration, the nature of the customer's business;

(ca) take into consideration the nature of the customer, its ownership and control structure, and its Beneficial Ownership (if any);

(d) take into consideration the nature of the customer business relationship with the Relevant Person;

(e) take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;

(f) take into consideration the relevant product, service or transaction;

(fa) if it is providing a customer with a life insurance or other similar policy, take into consideration the beneficiary of the policy and any Beneficial Owner of the beneficiary; and

(g) take into consideration the outcomes of business risk assessment under chapter 5.

Factors that may indicate higher money laundering risk

6.1.2 (1) When assessing if there is a high risk of money laundering in a particular situation, a Relevant Person must take into account, among other things:

(a) customer risk factors, including whether:

(i) the business relationship is conducted in unusual circumstances;

(ii) the customer is resident, established or registered in a geographical area of high risk (as set out in paragraph (c));

(iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;

(iv) the customer is a company that has nominee shareholders or shares in bearer form;

(v) the customer is a business that is cash intensive, such as a business that receives a majority of its revenue in cash; and

(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the business;

(b) product, service, transaction or delivery channel risk factors, including whether:

(i) the service involves private banking;

(ii) the product, service or transaction is one that might favour anonymity;

(iii) the situation involves non face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(iv) payments will be received from unknown or unassociated third parties;

(v) new products and new business practices are involved, including new delivery mechanisms or the use of new or developing technologies for both new and pre-existing products; and

(vi) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in another country; and

(c) geographical risk factors, including:

(i) countries identified in reports by credible sources, such as mutual evaluations, detailed assessment reports or follow-up reports, as:

(A) not having effective systems to counter money laundering; or

(B) not implementing requirements to counter money laundering that are consistent with FATF Recommendations;

(ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering or the production and supply of illicit drugs;

(iii) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations or the State;

(iv) countries providing funding or support for terrorism; and

(v) countries that have organisations operating within their territory that have been designated by the State, other countries or International Organisations as terrorist organisations.

(2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.

(3) When assessing the risk factors referred to in (1), Relevant Persons must bear in mind that the presence of one or more risk factors may not always indicate a high risk of money laundering in a particular situation.

Factors that may indicate lower money laundering risk

6.1.3 (1) When assessing if there is a low risk of money laundering in a particular situation, a Relevant Person must take into account, among other things:

(a) customer risk factors, including whether the customer is:

(i) a public body or a publicly owned enterprise;

(ii) resident, established or registered in a geographical area of lower risk (as set out in paragraph (c));

(iii) an Authorised Person;

(iv) a Regulated Financial Institution that is subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations that are equivalent to the standards set out in the FATF Recommendations;

(v) a Subsidiary of a Regulated Financial Institution referred to in (iv), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent;

(vi) a company whose Securities are listed by the DFSA, another Financial Services Regulator or a Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules;

(vii) a law firm, notary firm or other legal business that carries on its business in or from the DIFC; and

(viii) an accounting firm, insolvency firm, Registered Auditor or other audit firm that carries on its business in or from the DIFC;

(b) product, service, transaction or delivery channel risk factors, including whether the product or service is:

(i) a Contract of Insurance that is non-life insurance;

(ii) a Contract of Insurance that is a life insurance product with no investment return or redemption or surrender value;

(iii) an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;

(iv) a Contract of Insurance which is a reinsurance contract that is ceded by an insurer who is a Regulated Financial Institution;

(v) a pension, superannuation or similar scheme that satisfies the following conditions:

(A) the scheme provides retirement benefits to employees;

(B) contributions to the scheme are made by way of deductions from wages; and

(C) the scheme rules do not permit the assignment of a member's interest under the scheme; and

(vi) a product where the risks of money laundering are adequately managed by other factors such as transaction limits or transparency of ownership; and

(c) geographical risk factors, including whether:

(i) a country has been identified by credible sources as having effective systems to counter money laundering;

(ii) a country is identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, or the production and supply of illicit drugs; and

(iii) on the basis of reports by credible sources, such as mutual evaluations, detailed assessment reports or follow-up reports, a country:

(A) has requirements to counter money laundering that are consistent with the FATF Recommendations; and

(B) effectively implements those Recommendations.

(2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.

(3) When assessing the risk factors referred to in (1), Relevant Persons must bear in mind that the presence of one or more risk factors may not always indicate a low risk of money laundering in a particular situation.

Business relationship not to be established if ownership arrangements prevent identification of beneficial owners

6.1.4 A Relevant Person must not establish a business relationship with the customer which is a legal person or legal arrangement if the ownership or control arrangements of the customer prevent the Relevant Person from identifying one or more of the customer's Beneficial Owners.

Shell Banks

6.1.5 A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

Anonymous or fictitious accounts

6.1.6 A Relevant Person must not establish or maintain an anonymous account, an account in a fictitious name, or a nominee account which is held in the name of one person but which is controlled by or held for the benefit of another person whose identity has not been disclosed to the Relevant Person.

Use of numbered or abbreviated accounts for internal purposes

6.1.7 If a Relevant Person uses a numbered account or an account with an abbreviated name, it must ensure that:

(a) such an account is used only for internal purposes;

(b) it has undertaken the same Customer Due Diligence procedures in relation to the account holder as are required for other account holders;

(c) it maintains the same information in relation to the account and account holder as is required for other accounts and account holders; and

(d) staff performing AML functions, including staff responsible for identifying and monitoring transactions for suspicious activity, and staff performing compliance and audit functions, have full access to information about the account and the account holder.

Guidance on the customer risk assessment

1. The risk assessment of a customer, which is illustrated in figure 3 above, requires a Relevant Person to allocate an appropriate risk rating to every customer. The DFSA would expect risk ratings to be either descriptive, such as "low", "medium" or "high", or a sliding numeric scale such as 1 for the lowest risk to 10 for the highest. Depending on the outcome of a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide to what degree CDD will need to be performed. For a high risk customer, the Relevant Person will need to undertake Enhanced CDD under section 7.4 as well as the normal CDD set out in section 7.3. For a low risk customer, the Relevant Person may be able to undertake Simplified CDD in accordance with section 7.5. For any other customer, the Relevant Person will be required to undertake the normal CDD set out in section 7.3.

2. Using the RBA, a Relevant Person could, when assessing two customers with near identical risk profiles, consider that one is high risk and the other low risk. This may occur, for example, where both customers may be from the same high risk country, but one customer may be a customer in relation to a low risk product or may be a long-standing customer of a Group company who has been introduced to the Relevant Person.

3. In Rule 6.1.4, ownership arrangements which may prevent the Relevant Person from identifying one or more Beneficial Owners include bearer shares and other negotiable instruments in which ownership is determined by possession.

Guidance on the term "customer"

4. The point at which a person becomes a customer will vary from business to business. However, the DFSA considers that it would usually occur at or prior to the business relationship being formalised, for example, by the signing of a customer agreement or the acceptance of terms of business.

5. The DFSA does not consider that a person would be a customer of a Relevant Person merely because such person receives marketing information from a Relevant Person or where a Relevant Person refers a person who is not a customer to a third party (including a Group member).

6. The DFSA considers that a counterparty would generally be a "customer" for the purposes of this module and would therefore require a Relevant Person to undertake CDD on such a person. However, this would not include a counterparty in a transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ordinary business services, for consumption by the Relevant Person such as cleaning, catering, stationery, IT or other similar services.

7. A Representative Office should not have any customers in relation to its DIFC operations.

Guidance on Shell Banks

8. Rule 6.1.5 prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank. A Shell Bank is a bank that has no physical presence in the country in which it is incorporated or licensed, and is not affiliated with a regulated financial Group that is subject to effective consolidated supervision. The DFSA does not consider that the existence of a local agent or low level staff constitutes physical presence.

Guidance on fictitious and anonymous accounts

9. A Relevant Person should note that, in addition to the prohibition in Rule 6.1.6 against establishing anonymous or fictitious accounts or accounts for unknown persons, the Federal AML legislation also prohibits the creation or keeping of records of bank accounts using pseudonyms, fictitious names or numbered accounts, without the account holder's name.

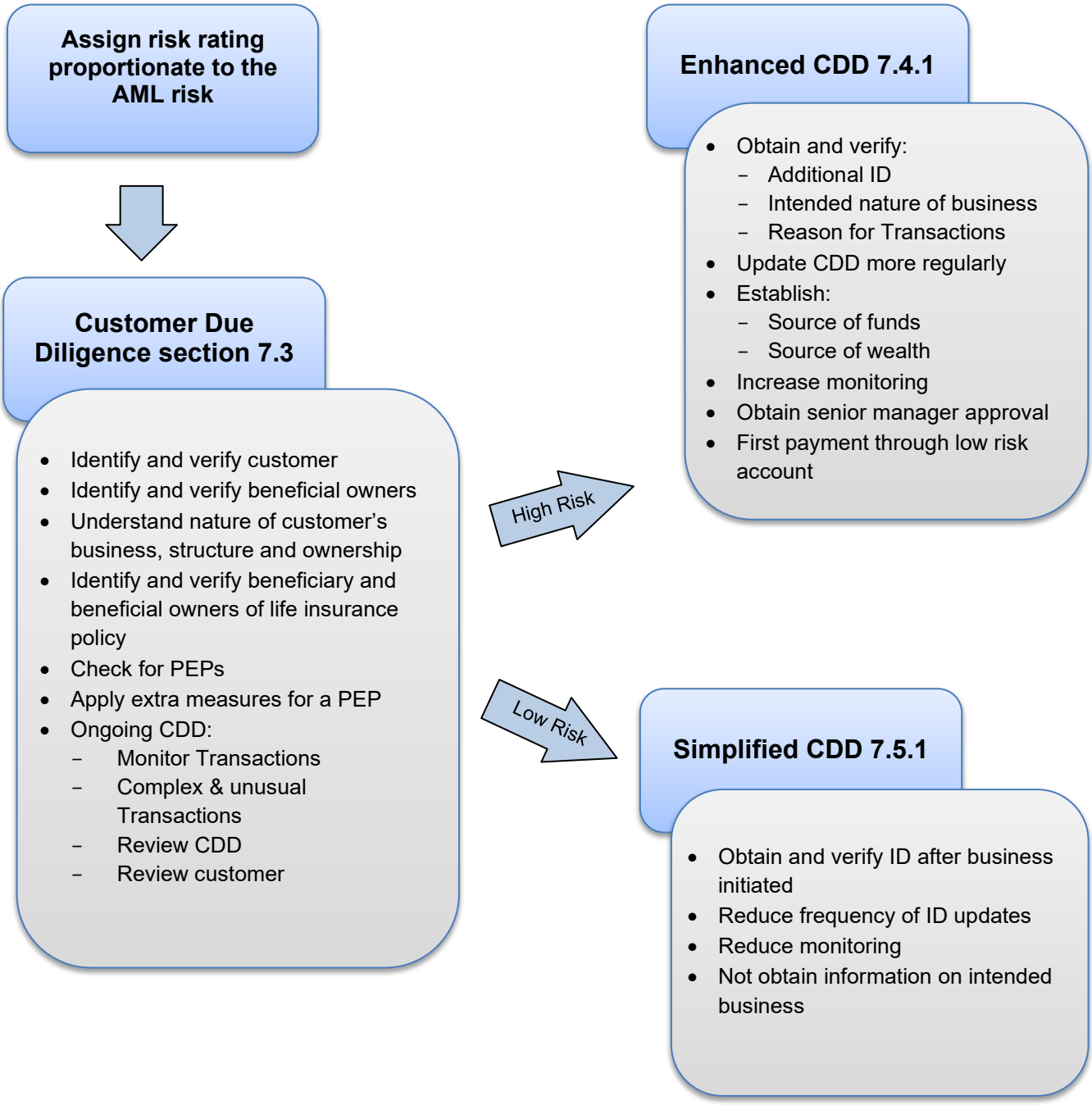
Guidance on Tax Issues

10. A Relevant Person should, when carrying out a customer risk assessment, consider and assess the tax crime risk associated with the customer and factor such risks into the overall risk assigned to that customer. Many of the factors described in Rule 6.1.2 on higher risk customers could also be an indicator of potential tax crimes. For example, the use of complex or unusual corporate structures, the customer's business not being located where the customer lives (without adequate explanation), unusual customer interface, or reluctance by the customer to communicate directly with the Relevant Person.

11. If it is justified based on the risk assessment and where concerns arise, a Relevant Person may wish to seek comfort from its customers by obtaining disclosures or declarations to ascertain if a legitimate explanation exists for the concerns and therefore to allay those concerns.

7 CUSTOMER DUE DILIGENCE

Figure 4. CDD



7.1 Requirement to undertake customer due diligence

7.1.1 (1) A Relevant Person must:

(a) undertake Customer Due Diligence under section 7.3 for each of its customers; and

(b) in addition to (a), undertake Enhanced Customer Due Diligence under Rule 7.4.1 in respect of any customer it has assigned as high risk.

(2) A Relevant Person may undertake Simplified Customer Due Diligence in accordance with Rule 7.5.1 by modifying Customer Due Diligence under section 7.3 for any customer it has assigned as low risk.

Guidance

A Relevant Person should undertake CDD in a manner proportionate to the customer's money laundering risks identified under Rule 6.1.1(1). This means that all customers are subject to CDD under section 7.3. However, for high risk customers, additional Enhanced CDD measures should also be undertaken under section 7.4. For low risk customers, section 7.3 may be modified according to the risks in accordance with section 7.5.

7.2 Timing of customer due diligence

7.2.1 (1) A Relevant Person must, except as otherwise provided in Rule 7.2.2 or in section 7.3:

(a) undertake the appropriate Customer Due Diligence under Rule 7.3.1(1)(a) to (c) and section 7.3 when it is establishing a business relationship with a customer; and

(b) undertake the appropriate Customer Due Diligence under Rule 7.3.1(1)(d) after establishing a business relationship with a customer.

(2) A Relevant Person must also undertake appropriate Customer Due Diligence if, at any time:

(a) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;

(b) it suspects money laundering in relation to a person; or

(c) there is a change in risk-rating of the customer, or it is otherwise warranted by a change in circumstances of the customer.

Establishing a business relationship before verification

7.2.2 (1) A Relevant Person may establish a business relationship with a customer before completing the verification required by Rule 7.3.1 if the following conditions are met:

(a) deferral of the verification of the customer or Beneficial Owner is necessary in order not to interrupt the normal conduct of a business relationship;

(b) there is little risk of money laundering occurring and any such risks identified can be effectively managed by the Relevant Person;

(c) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and

(d) subject to (2), the relevant verification is completed as soon as reasonably practicable and in any event no later than 30 days after the establishment of a business relationship.

(2) Where a Relevant Person is not reasonably able to comply with the 30 day requirement in (1)(d), it must, prior to the end of the 30 day period:

(a) document the reason for its non-compliance;

(b) complete the verification in (1) as soon as possible; and

(c) record the non-compliance event in its annual AML Return.

(3) The DFSA may specify a period within which a Relevant Person must complete the verification required by (1) failing which the DFSA may direct the Relevant Person to cease any business relationship with the customer.

(4) A Relevant Person must ensure that its AML systems and controls referred to in Rule 5.2.1 include risk management policies and procedures concerning the conditions under which business relationships may be established with a customer before completing verification.

Guidance

1. For the purposes of Rule 7.2.1(2)(a), examples of situations which might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained could be where there is a suspicion of money laundering in relation to that customer, where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Relevant Person that a person other than the customer is the real customer.

2. In Rule 7.2.2(1)(a), situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period or executing a time critical transaction, which if not executed immediately, would or may cause a customer to incur a financial loss due to price movement or loss of opportunity or when a customer seeks immediate insurance cover.

3. When complying with Rule 7.2.1, a Relevant Person should also, where relevant, consider Rule 7.7.1 regarding failure to conduct or complete CDD and chapter 13 regarding SARs and tipping off.

4. For the purposes of Rule 7.2.2(1)(d), the DFSA considers that in most situations as soon as reasonably practicable would be within 30 days after the establishment of a business relationship. However, it will depend on the nature of the customer business relationship.

7.3 Customer due diligence requirements

Undertaking customer due diligence

7.3.1 (1) In undertaking Customer Due Diligence required by Rule 7.1.1(1)(a) a Relevant Person must:

(a) identify the customer and verify the customer's identity;

(b) identify any Beneficial Owners of the customer and take reasonable measures to verify the identity of the Beneficial Owners, so that the Relevant Person is satisfied that it knows who the Beneficial Owners are;

(c) if the customer is a legal person or legal arrangement, take reasonable measures to understand the nature of the customer's business and its ownership and control structure; and

(d) undertake on-going due diligence of the customer business relationship under Rule 7.6.1.

(2) If a person ("A") purports to act on behalf of the customer, the Relevant Person must, in addition to (1)(a):

(a) verify that A is authorised to act on the customer's behalf; and

(b) identify A and verify A's identity.

(3) The verification under (1) and (2) must be based on reliable and independent source documents, data or information.

Identifying and verifying the customer

7.3.2 (1) For the purposes of Rule 7.3.1(1)(a), a Relevant Person must identify a customer and verify the customer's identity in accordance with this Rule.

(2) If a customer is a natural person, a Relevant Person must obtain and verify information about the person's:

(a) full name;

(b) date of birth;

(c) nationality;

(d) legal domicile; and

(e) current residential address (other than a post office box).

(3) If a customer is a body corporate, the Relevant Person must obtain and verify:

(a) the full name of the body corporate and any trading name;

(b) the address of its registered office and, if different, its principal place of business;

(c) the date and place of incorporation or registration;

(d) a copy of the certificate of incorporation or registration;

(e) the articles of association or other equivalent governing documents of the body corporate; and

(f) the full names of its senior management.

(4) If a customer is a foundation, the Relevant Person must obtain and verify:

(a) a certified copy of the charter and by-laws of the foundation or any other documents constituting the foundation; and

(b) documentary evidence of the appointment of the guardian or any other person who may exercise powers in respect of the foundation.

(5) If a customer is an express trust or other similar legal arrangement, the Relevant Person must obtain and verify:

(a) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement; and

(b) documentary evidence of the appointment of the trustee or any other person exercising powers under the trust or arrangement.

Guidance

In complying with Rule 7.3.2(2)(a), a Relevant Person should include any current legally recognised name(s) as well as any previously recognised name(s).

Identifying and verifying beneficial owners: body corporate

7.3.3 (1) If a customer is a body corporate, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.

(2) The Relevant Person must identify:

(a) the natural persons who ultimately have a controlling ownership interest in the body corporate, whether legal or beneficial, direct or indirect; and

(b) if there is any doubt about whether the natural persons identified under (a) exert control through ownership interests, or if no natural person exerts control through ownership interests, the natural persons exercising control of the body corporate through other means.

(3) A Relevant Person does not have to identify an ownership interest under (2)(a) if, having regard to a risk-based assessment of the customer, it is reasonably satisfied that the ownership interest is minor and in the circumstances poses no or negligible risk of money laundering.

(4) If a Relevant Person has exhausted all possible means but has not been able to identify the Beneficial Owners under (2), and provided it has no grounds for suspecting money laundering, it must treat the senior management of the body corporate as the Beneficial Owners.

(5) If (4) applies, the Relevant Person must keep a record in writing of all the actions it has taken to identify the Beneficial Owners of the body corporate.

Guidance

1. In exceptional circumstances, a Relevant Person may not be able to identify any natural person as the ultimate owner or controller of a body corporate. In such a case, provided it has exhausted all other means of identifying the owner or controller and it has no grounds for suspecting money laundering, it can treat each of the members of the senior management of the body corporate as the Beneficial Owners (see Rule 7.3.3(4)). However, in such a case the Relevant Person will need to keep records of all the actions it has taken to identify the Beneficial Owners (see Rule 7.3.3(5)).

2. If the ownership or control arrangements of a customer are of such a nature that the Relevant Person is prevented from identifying the Beneficial Owners (for example, if Beneficial Owners hold bearer shares or other negotiable instruments and there is no effective system for recording the current holder of the shares or instruments), the Relevant Person is prohibited from establishing a business relationship with the customer under Rule 6.1.4.

3. For more detailed Guidance on identifying and verifying Beneficial Owners, see the guidance on CDD at the end of section 7.3.

7.3.4 A Relevant Person is not required to comply with Rules 7.3.1(1)(b) and (c) if the customer is either:

(a) a body corporate that:

(i) has its Securities listed by the DFSA, another Financial Services Regulator or a Regulated Exchange; and

(ii) is subject to disclosure requirements which ensure that adequate information about its business, structure and beneficial ownership is publicly available; or

(b) a majority-owned subsidiary of a body corporate referred to in (a).

Identifying and verifying beneficial owners: foundations

7.3.5 (1) If a customer is a foundation, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.

(2) The Relevant Person must identify the founder, guardian, contributors, qualified recipients, other persons entitled to receive any property or income from the foundation and any other natural person who exercises ultimate effective control of the foundation.

(3) If the qualified recipients, or other persons entitled to receive property or income from a foundation, are designated by characteristics or by class, the Relevant Person must obtain sufficient information to satisfy itself that it will be able to establish the identity of the qualified recipient or other person before it makes any payment or transfer of property to the recipient or person.

(4) The Relevant Person must verify the identity of a qualified recipient or other person referred to in (3) before it makes any payment, or transfers any property, from the foundation to that recipient or person.

Identifying and verifying beneficial owners: trusts and similar arrangements

7.3.6 (1) If a customer is a legal arrangement, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.

(2) The Relevant Person must identify:

(a) for a trust, the settlor, trustee, protector, enforcer, beneficiaries and any other natural person who exercises ultimate effective control over the trust; and

(b) for other types of legal arrangements, persons in equivalent or similar positions to those persons referred to in (a).

(3) If the beneficiaries of a trust or arrangement are designated by characteristics or by class, the Relevant Person must obtain sufficient information about the beneficiaries to satisfy itself that it will be able to establish the identity of a beneficiary:

(a) before it makes a distribution to the beneficiary; or

(b) when the beneficiary intends to exercise vested rights.

(4) The Relevant Person must verify the identity of a beneficiary referred to in (3) before it makes a distribution to the beneficiary or the beneficiary exercises vested rights.

Identifying and verifying beneficiary of a life insurance policy

7.3.7 (1) This Rule applies if a Relevant Person is providing a customer with a life insurance or other similar policy.

(2) The Relevant Person must, in addition to complying with Rule 7.3.1:

(a) if a beneficiary is specifically named in the policy, record the name of that person; and

(b) if the beneficiaries of the policy are designated by characteristics or by class, obtain sufficient information to satisfy itself that it will be able to establish the identity of the beneficiaries when any payment is due to be made under the policy.

(3) The Relevant Person must undertake the measures referred to in (2) as soon as the beneficiary of the policy is identified or designated.

(4) The Relevant Person must verify the identity of beneficiaries and any Beneficial Owners of a beneficiary before it makes a payout under the policy.

Guidance

An insurance policy that is similar to a life insurance policy includes life-related protection, or a pension or investment product that pays out to the policyholder or beneficiary upon a particular event occurring or upon redemption.

Politically Exposed Persons: other measures

7.3.8 (1) A Relevant Person must take reasonable measures to determine:

(a) if a customer, or a Beneficial Owner of a customer, is a Politically Exposed Person (PEP); and

(b) for a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP.

(2) If a customer, or a Beneficial Owner of a customer, is a PEP, a Relevant Person must:

(a) obtain the approval of senior management to commence or continue the business relationship with the customer;

(b) take reasonable measures to establish the source of wealth and source of funds of the customer or Beneficial Owner; and

(c) increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

(3) If a beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary, is a PEP, a Relevant Person must:

(a) obtain the approval of senior management to make any payout under the policy;

(b) take reasonable measures to establish the source of wealth and source of funds of the beneficiary or Beneficial Owner of the beneficiary; and

(c) increase the degree and nature of monitoring of its business relationship with the policyholder, to determine whether the customer's transactions or activities appear unusual or suspicious.

(4) A Relevant Person must carry out the additional Customer Due Diligence referred to in (3) before it makes any payout under the policy.

Guidance on CDD

1. Items (a) to (c) in Rule 7.3.2(2) should be obtained from a current valid passport or, where a customer does not possess a passport, an official identification document which includes a photograph. The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties or which is his place of origin.

2. Under Rule 7.3.1(3), a Relevant Person is required to verify the identity of a person based on reliable and independent source documents, data or information. A Relevant Person should generally have sight of original identification documents and retain a copy of the identification document. However in complying with Rule 7.3.1, it may not always be possible to obtain original documents. Where identification documents cannot be obtained in original form, for example, because a Relevant Person has no physical contact with the customer, the Relevant Person should obtain a copy certified as a true copy by a person of good standing such as a registered lawyer or notary, a chartered accountant, a bank manager, a police officer, an Employee of the person's embassy or consulate, or other similar person. The DFSA considers that downloading publicly-available information from an official source (such as a regulator's or other official government website) is sufficient to satisfy the requirements of Rule 7.3.1. The DFSA also considers that CDD information and research obtained from a reputable company or information-reporting agency may also be acceptable as a reliable and independent source as would banking references and, on a risk-sensitive basis, information obtained from researching reliable and independent public information found on the internet or on commercial databases.

3. For higher risk situations the DFSA would expect identification information to be independently verified, using both public and non-public sources.

Guidance on identification and verification of Beneficial Owners

4. In determining whether an individual meets the definition of a Beneficial Owner, regard should be had to all the circumstances of the case, in particular the size of an individual's legal or beneficial ownership in a transaction. The question of what is a "minor" ownership interest for the purposes of the definition of a Beneficial Owner in Rule 7.3.3 will depend on the individual circumstances of the customer. The DFSA considers that the question of whether an ownership interest is minor should be considered in the context of the Relevant Person's knowledge of the customer and the customer risk assessment and the risk of money laundering.

5. When identifying Beneficial Owners, a Relevant Person is expected to adopt a substantive (as opposed to form over substance) approach to CDD for legal persons. Adopting a substantive approach means focusing on the money laundering risks of the customer and the product/service and avoiding an approach which focusses purely on the legal form of an arrangement or sets fixed percentages at which Beneficial Owners are identified (or not). It should take all reasonable steps to establish and understand a corporate customer's legal ownership and control and to identify the Beneficial Owner. The DFSA does not set explicit ownership or control thresholds in defining the Beneficial Owner because the DFSA considers that the applicable threshold to adopt will ultimately depend on the risks associated with the customer, and so the DFSA expects a Relevant Person to adopt the RBA and justify on reasonable grounds an approach which is proportionate to the risks identified. A Relevant Person should not set fixed thresholds for identifying the Beneficial Owner without objective and documented justification as required by Rule 4.1.1. An overly formal approach to defining the Beneficial Owner may result in a criminal "gaming" the system by always keeping his financial interest below the relevant threshold.

6. The DFSA considers that in some circumstances no threshold should be used when identifying Beneficial Owners because it may be important to identify all underlying Beneficial Owners in order to ensure that they are not associated or connected in some way. This may be appropriate where there are a small number of investors in an account or fund, each with a significant financial holding and the customer-specific risks are higher. However, where the customer-specific risks are lower, a threshold can be appropriate. For example, for a low-risk corporate customer which, combined with a lower-risk product or service, a percentage threshold may be appropriate for identifying "control" of the legal person for the purposes of the definition of a Beneficial Owner.

7. For a retail investment fund which is widely-held and where the investors invest via pension contributions, the DFSA would not expect the manager of the fund to look through to any underlying investors where there are none with any material control or ownership levels in the fund. However, for a closely-held fund with a small number of investors, each with a large shareholding or other interest, the DFSA would expect a Relevant Person to identify and verify each of the Beneficial Owners, depending on the risks identified as part of its risk-based assessment of the customer. For a corporate health policy with defined benefits, the DFSA would not expect a Relevant Person to identify the Beneficial Owners.

8. Under Federal AML legislation, if the customer is a legal person, the Relevant Person must identify any person who, alone or jointly with other persons, has a controlling ownership interest of 25% or more in the legal person i.e. it applies a specified threshold. This does not affect the approach that should be taken under Rule 7.3.1(1)(b) and Rule 7.3.3 for verifying the identity of Beneficial Owners, where no threshold is specified (see Guidance items 4 to 7 above). As a result, under the Federal AML legislation a Relevant Person will need to obtain information identifying natural persons who have a controlling interest of more than 25%. Then, in accordance with the risk-based approach in Guidance items 4 to 7, the Relevant Person should determine whether it is necessary also to identify other persons who may be Beneficial Owners, and verify their identity.

Guidance on politically exposed persons

9. Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to a Relevant Person as their position may make them vulnerable to corruption. This risk also extends to members of their families and to known

close associates. Politically Exposed Person ("PEP") status itself does not, of course, incriminate individuals or entities.

10. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such person, if he was committing money laundering, would attempt to place his money offshore where the customer is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his home jurisdiction to confiscate or freeze his criminal property.

11. Corruption-related money laundering risk increases when a Relevant Person deals with a PEP. Corruption may involve serious crimes and has become the subject of increasing global concern. Corruption offences are predicate crimes under the Federal AML legislation. A Relevant Person should note that customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves.

12. The DFSA considers that after leaving office a PEP may remain a higher risk for money laundering if such person continues to exert political influence or otherwise pose a risk of corruption.

13. The fact that an individual is a PEP does not automatically mean that the individual must be assessed to be a high risk customer. A Relevant Person will need to assess the particular circumstances relating to each PEP to determine what risk category is appropriate. If the PEP is assigned a high risk, then the Relevant Person will need to undertake the Enhanced Customer Due Diligence measures under Rule 7.4.1. However, even if a PEP is not assigned a high risk, the Relevant Person is required as a minimum to undertake the additional customer due diligence measures specified in Rule 7.3.8(2) and (3) for PEPs.

7.4 Enhanced customer due diligence

7.4.1 Where a Relevant Person is required to undertake Enhanced Customer Due Diligence under Rule 7.1.1(1)(b) it must, to the extent applicable to the customer:

(a) obtain and verify additional:

(i) identification information on the customer and any Beneficial Owner;

(ii) information on the intended nature of the business relationship; and

(iii) information on the reasons for a transaction;

(b) update more regularly the Customer Due Diligence information which it holds on the customer and any Beneficial Owners;

(c) take reasonable measures to establish:

(i) the source of funds; and

(ii) the source of wealth,

of the customer or, if applicable, of the Beneficial Owner;

(d) increase the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious;

(e) obtain the approval of senior management to commence or continue a business relationship with a customer; and

(f) where applicable, require that any first payment made by a customer in order to open an account with a Relevant Person must be carried out through a bank account in the customer's name with:

(i) a Bank;

(ii) a Regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF recommendations; or

(iii) a Subsidiary of a Regulated Financial Institution referred to in (ii), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent.

Guidance

1. In Rule 7.4.1 Enhanced CDD measures are only mandatory to the extent that they are applicable to the relevant customer or the circumstances of the business relationship and to the extent that the risks would reasonably require it. Therefore, the extent of additional measures to conduct is a matter for the Relevant Person to determine on a case by case basis.

2. In Rule 7.4.1 (e), senior management approval may be given by an individual member of the Relevant Person's senior management. A Relevant Person may also establish a committee to consider high risk customers. However, in that case, the approval would, nonetheless, have to be given by a member of the senior management, who can be a member of the committee.

3. For high risk customers, a Relevant Person should, in order to mitigate the perceived and actual risks, exercise a greater degree of diligence throughout the customer relationship and should endeavour to understand the nature of the customer's business and consider whether it is consistent and reasonable.

4. A Relevant Person should be satisfied that a customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

5. For enhanced CDD, a Relevant Person has to take reasonable measures to establish the source of funds. That is, where the funds for a particular service or transaction will come from (e.g. a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.

6. For enhanced CDD, where there is a Beneficial Owner, establishing the customer's source of funds and wealth may require enquiring into the Beneficial Owner's source of funds and wealth because the source of the funds would normally be the Beneficial Owner and not the customer.

7. The DFSA considers that taking reasonable measures to establish the source of funds includes obtaining independent corroborating evidence such as proof of dividend payments connected to a shareholding, bank statements, salary/bonus certificates, loan documentation and proof of a transaction which gave rise to the payment into the account. A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

8. The DFSA considers that verification of source of wealth includes obtaining independent corroborating evidence such as share certificates, publicly-available registers of ownership, bank or brokerage account statements, probate documents, audited accounts and financial statements, news items from a reputable source and other similar evidence. For example:

   a. for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and

b. for a natural person, this might include documentary evidence which corroborates answers given to questions on the source of wealth in an application form or customer questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide sufficient bank or salary statements covering a number of years to draw up a picture of his source of wealth.

9. A Relevant Person may commission a third party vendor report to obtain further information on a customer or transaction or to investigate a customer or Beneficial Owner in very high risk cases. A third party vendor report may be particularly useful where there is little or no publicly-available information on a person or on a legal arrangement or where a Relevant Person has difficulty in obtaining and verifying information.

10. In Rule 7.4.1(f), circumstances where it may be applicable to require the first payment made by a customer in order to open an account with a Relevant Person to be carried out through a bank account in the customer's name with a financial institution specified in that paragraph include:

a. where, following the use of other Enhanced CDD measures, the Relevant Person is not satisfied with the results of due diligence; or

b. as an alternative measure, where one of the measures in Rule 7.4.1 (a) to (e) cannot be carried out.

7.5 Simplified customer due diligence

7.5.1 (1) Where a Relevant Person is permitted to undertake Simplified Customer Due Diligence under Rule 7.1.1(2), modification of Rule 7.3.1 may include:

(a) verifying the identity of the customer and any Beneficial Owners after the establishment of the business relationship under Rule 7.2.1(3);

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identification document other than by requesting a copy;

(d) reducing the degree of on-going monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or

(e) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

(2) The modification in (1) must be proportionate to the customer's money laundering risks.

Guidance

1. Rule 7.5.1(1) provides examples of Simplified CDD measures. Other measures may also be used by a Relevant Person to modify CDD in accordance with the customer risks.

2. A Relevant Person should not use a "one size fits all" approach for all its low risk customers. Notwithstanding that the risks may be low for all such customers, the degree of CDD undertaken needs to be proportionate to the specific risks identified on a case by case basis.

3. A Relevant Person is not required to identify or verify Beneficial Owners for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions.

4. An example of circumstances where a Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates would be where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.

5. An example of where a Relevant Person might reasonably reduce the degree of on-going monitoring and scrutinising of transactions, based on a reasonable monetary threshold or on the nature of the transaction, would be where the transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the transaction is not material for money laundering purposes given the nature of the customer and the transaction type.

6. For the avoidance of doubt, a Relevant Person should not conduct Simplified CDD where there is any suspicion of money laundering.

7.6 Ongoing customer due diligence

7.6.1 (1) When undertaking ongoing Customer Due Diligence under Rule 7.3.1(1)(d), a Relevant Person must, using the risk-based approach:

(a) monitor transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the Relevant Person's knowledge of the customer, his business and risk rating;

(b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the transactions in (b);

(d) review the adequacy of the Customer Due Diligence information it holds on customers and Beneficial Owners to ensure that the information is kept up to date, particularly for customers with a high risk rating; and

(e) review each customer to ensure that the risk rating assigned to a customer under Rule 6.1.1(1)(b) remains appropriate for the customer in light of the money laundering risks.

(2) A Relevant Person must carry out a review under (1)(d) and (e) periodically and at other appropriate times when a material change or event occurs relating to a customer.

Guidance

1. In complying with Rule 7.6.1(1)(d), a Relevant Person should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up-to-date. Examples of non-static identity documentation include passport number and residential/business address and, for a legal person, its share register or list of partners.

2. A Relevant Person should undertake a review under Rule 7.6.1(1)(d) and (e), both periodically and at other appropriate times such as when:

a. the Relevant Person changes its CDD documentation requirements;

b. an unusual transaction with the customer is expected to take place;

c. there is a material change in the business relationship with the customer; or

d. there is a material change in the nature or ownership of the customer.

3. The degree of the on-going due diligence to be undertaken will depend on the customer risk assessment carried out under Rule 6.1.1.

4. A Relevant Person's transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination thereof, are one of the most important aspects of effective CDD. Whether a Relevant Person should undertake the monitoring by means of a manual or computerised system (or both) will depend on a number of factors, including:

a. the size and nature of the Relevant Person's business and customer base; and

b. the complexity and volume of customer transactions.

Ongoing sanctions screening

7.6.2 A Relevant Person must review its customers, their business and transactions against United Nations Security Council sanctions lists and against any other relevant sanctions list when complying with Rule 7.6.1(1)(d).

Guidance

1. In Rule 7.6.2, a "relevant sanctions list" may include U.A.E, EU, U.K. HM Treasury, U.S. OFAC lists and any other list which may apply to a Relevant Person.

2. A Relevant Person should also be aware of its obligations under Article 21 of Cabinet Decision No. 74 of 2020, which include the obligations to register with the Executive Office for Control and Non-Proliferation (EOCN), screen its databases and transactions, apply or cancel freezing orders, report to regulatory authorities, set-up internal controls and procedures, establish and implement policies and cooperate with the EOCN and regulatory authorities.

7.7 Failure to conduct or complete customer due diligence

7.7.1 (1) Where, in relation to any customer, a Relevant Person is unable to conduct or complete the requisite Customer Due Diligence in accordance with Rule 7.1.1 it must, to the extent relevant:

(a) not carry out a transaction with or for the customer through a bank account or in cash;

(b) not open an account or otherwise provide a service;

(c) not otherwise establish a business relationship or carry out a transaction;

(d) terminate or suspend any existing business relationship with the customer;

(e) return any monies or assets received from the customer; and

(f) consider whether the inability to conduct or complete Customer Due Diligence necessitates the making of a Suspicious Activity Report under Rule 13.3.1(c).

(2) A Relevant Person is not obliged to comply with (1) (a) to (e) if:

(a) to do so would amount to "tipping off" the customer, in breach of Federal AML legislation; or

(b) the FIU directs the Relevant Person to act otherwise.

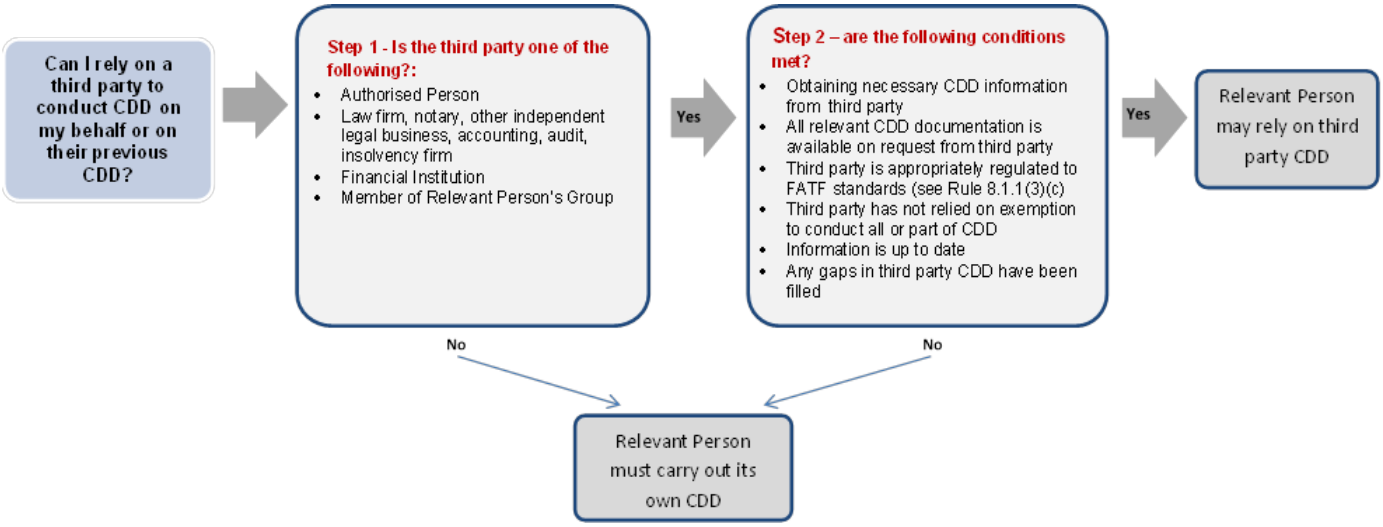
Guidance

1. In complying with Rule 7.7.1(1) a Relevant Person should apply one or more of the measures in (a) to (f) as appropriate in the circumstances. Where CDD cannot be completed, it may be appropriate not to carry out a transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD, such as identifying and verifying a Beneficial Owner cannot be conducted, a Relevant Person should not establish a business relationship with the customer.

2. A Relevant Person should note that Rule 7.7.1 applies to both existing and prospective customers. For new customers it may be appropriate for a Relevant Person to terminate the business relationship before a product or service is provided. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. Whichever route is taken, the Relevant Person should be careful not to tip off the customer.

3. A Relevant Person should adopt the RBA for CDD of existing customers. For example, if a Relevant Person considers that any of its existing customers (which may include customers which it migrates into the DIFC) have not been subject to CDD at an equivalent standard to that required by this module, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with Rule 7.7.1.

8 RELIANCE AND OUTSOURCING



8.1 Reliance on a third party

8.1.1 (1) A Relevant Person may rely on the following third parties to conduct one or more elements of Customer Due Diligence on its behalf:

(a) an Authorised Person;

(b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;

(c) a Financial Institution; or

(d) a member of the Relevant Person's Group.

(2) In (1), a Relevant Person may rely on the information previously obtained by a third party which covers one or more elements of Customer Due Diligence.

(3) Where a Relevant Person seeks to rely on a person in (1) it may only do so if and to the extent that:

(a) it immediately obtains the necessary Customer Due Diligence information from the third party in (1);

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of Customer Due Diligence will be available from the third party on request without delay;

(c) if a person in (1)(b) to (d) is in another country, the person is:

(i) subject to requirements in relation to customer due diligence and record keeping which meet the standards set out in the FATF Recommendations; and

(ii) supervised for compliance with those requirements in a manner that meets the standards for regulation and supervision set out in the FATF Recommendations;

(d) the person in (1) has not relied on any exception from the requirement to conduct any relevant elements of Customer Due Diligence which the Relevant Person seeks to rely on; and

(e) in relation to (2), the information is up to date.

(4) Where a Relevant Person relies on a member of its Group, such Group member need not meet the condition in (3)(c) if:

(a) the Group applies and implements a Group-wide policy on customer due diligence, record keeping, Politically Exposed Persons and AML programmes which meets the standards set out in the FATF Recommendations; and

(b) where the effective implementation of those Customer Due Diligence, record keeping and PEP requirements and AML programmes are supervised at Group level by a Financial Services Regulator or other competent authority in a country, the supervision and regulation meets the standards set out in the FATF Recommendations.

(5) If a Relevant Person is not reasonably satisfied that a customer or Beneficial Owner has been identified and verified by a third party in a manner consistent with these Rules, the Relevant Person must immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.

(6) Notwithstanding the Relevant Person's reliance on a person in (1), the Relevant Person remains responsible for compliance with, and liable for any failure to meet the Customer Due Diligence requirements in this module.

8.1.2 (1) When assessing under Rule 8.1.1(3)(c) or (4) if requirements, supervision or regulation in another jurisdiction meet FATF standards, a Relevant Person must take into account factors including, among other things:

(a) mutual evaluations, assessment reports or follow-up reports published by FATF, the IMF, the World Bank, the OECD or other International Organisations;

(b) membership of FATF or other international or regional groups such as the MENAFATF or the Gulf Co-operation Council;

(c) contextual factors such as political stability or the level of corruption in the jurisdiction;

(d) evidence of recent criticism of the jurisdiction, including in:

(i) FATF advisory notices;

(ii) public assessments of the jurisdiction's AML regime by organisations referred to in (a); or

(iii) reports by other relevant non-government organisations or specialist commercial organisations; and

(e) whether adequate arrangements exist for co-operation between the AML regulator in that jurisdiction and the DFSA.

(2) A Relevant Person making an assessment under (1) must rely only on sources of information that are reliable and up-to-date.

(3) A Relevant Person must keep adequate records of how it made its assessment, including the sources and materials considered.

Guidance

1. In complying with Rule 8.1.1(3)(a), "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, and not just basic information such as name and address. Compliance can be achieved by having that relevant information sent by email or other appropriate means. For the avoidance of doubt, a Relevant Person is not required automatically to obtain the underlying certified documents used by the third party to undertake its CDD. A Relevant Person must, however, under Rule 8.1.1(3)(b) ensure that the certified documents are readily available from the third party on request.

2. The DFSA would expect a Relevant Person, in complying with Rule 8.1.1(5), to fill any gaps in the CDD process as soon as it becomes aware that a customer or Beneficial Owner has not been identified and verified in a manner consistent with these Rules.

3. If a Relevant Person acquires another business, either in whole or in part, the DFSA would permit the Relevant Person to rely on the CDD conducted by the business it is acquiring but would expect the Relevant Person to have done the following:

   a. as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD undertaken; and

   b. to undertake CDD on all the customers to cover any deficiencies identified in (a) as soon as possible following the acquisition, prioritising high risk customers.

4. Where a particular jurisdiction's laws (such as secrecy or data protection legislation) would prevent a Relevant Person from having access to CDD information upon request without delay as referred to in Rule 8.1.1(3)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

5. If a Relevant Person relies on a third party located in a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the Relevant Person must ensure that the foreign jurisdiction has AML regulations that are equivalent to the standards in the FATF Recommendations (see Rule 8.1.1(3)(c) and Rule 8.1.2).

8.2 Outsourcing

8.2.1 A Relevant Person which outsources any one or more elements of its Customer Due Diligence to a service provider (including within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations.

Guidance

1. Prior to appointing an outsourced service provider to undertake CDD, a Relevant Person should undertake appropriate due diligence to assure itself of the suitability of the outsourced service provider and should ensure that the outsourced service provider's obligations are clearly documented in a binding agreement.

2. An Authorised Person should be mindful of its obligations regarding outsourcing set out in GEN Rules 5.3.21 and 5.3.22.

8.3 Money Service Providers

8.3.1 (1) An Authorised Firm that Provides Money Services must:

(a) maintain a complete, current and accurate register of all agents it uses to conduct its Money Services business and make the register available to the DFSA upon request;

(b) include all agents referred to in (a) as part of its AML compliance programme and monitor agents' compliance with the programme;

(c) comply with all applicable AML requirements in the jurisdictions in which it operates, whether directly or through the use of agents;

(d) when executing Payment Transactions, assess and consider all relevant information including information about the payer, payee and any beneficiary, as applicable, to determine whether a Suspicious Activity Report should be made; and

(e) if appropriate, make a Suspicious Activity Report in any jurisdiction impacted or connected to a suspicious Payment Transaction, and make available relevant transaction information to the authorities responsible for AML compliance in the relevant jurisdiction.

(2) An Authorised Firm making an assessment under (1) must rely only on sources of information that are reliable and up-to-date.

(3) An Authorised Firm must keep adequate records of how it made its assessment under (1), including the sources and materials considered.

9 CORRESPONDENT BANKING, ELECTRONIC FUND TRANSFERS AND AUDIT

9.1 Application

9.1.1 This chapter applies only to an Authorised Person, except section 9.3B which applies only to a DNFBP.

9.2 Correspondent banking

9.2.1 An Authorised Firm proposing to have a correspondent banking relationship with a respondent bank must:

(a) undertake appropriate Customer Due Diligence on the respondent bank;

(b) as part of (a), gather sufficient information about the respondent bank to understand fully the nature of the business, including making appropriate enquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(c) determine from publicly-available information the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or relevant regulatory action;

(d) assess the respondent bank's AML controls and ascertain if they are adequate and effective in light of the FATF Recommendations;

(e) ensure that prior approval of the Authorised Firm's senior management is obtained before entering into a new correspondent banking relationship;

(f) ensure that the respective responsibilities of the parties to the correspondent banking relationship are properly documented; and

(g) be satisfied that, in respect of any customers of the respondent bank who have direct access to accounts of the Authorised Firm, the respondent bank:

(i) has undertaken Customer Due Diligence (including ongoing Customer Due Diligence) at least equivalent to that in Rule 7.3.1 in respect of each customer; and

(ii) is able to provide the relevant Customer Due Diligence information in (i) to the Authorised Firm upon request; and

(h) document the basis for its satisfaction that the requirements in (a) to (g) are met.

9.2.2 An Authorised Firm must:

(a) not enter into a correspondent banking relationship with a Shell Bank; and

(b) take appropriate measures to ensure that it does not enter into, or continue a corresponding banking relationship with, a bank which is known to permit its accounts to be used by Shell Banks.

Guidance

Rule 9.2.2 prohibits an Authorised Firm from entering into a correspondent banking relationship with a Shell Bank or a bank which is known to permit its accounts to be used by Shell Banks. See the Guidance after Rule 6.1.7 for more information about what constitutes a Shell Bank.

9.3 Electronic fund transfers

Application

9.3.1 (1) This section applies to an Authorised Person when it sends or transmits funds by electronic means, or when it receives funds (including serial payments and cover payments) by electronic means, on the account of a payer or payee.

(2) This section does not apply to a transfer and settlement between Financial Institutions if the Financial Institutions are acting on their own behalf as the payer and the payee.

Definitions

9.3.2 In this section:

(a) "batch transfer" means a transfer that consists of a number of individual fund transfers that are bundled for transmission, whether the individual fund transfers are intended ultimately for one or more payees;

(b) "beneficiary institution" means the Financial Institution that receives the fund transfer from the ordering institution, whether directly or through an intermediary institution, and makes the funds available to the payee;

(c) "cover payment" means a fund transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction from the ordering institution to the beneficiary institution through one or more intermediary institutions;

(d) "cross-border fund transfer" means a fund transfer where the ordering institution and the beneficiary institution are located in different countries and includes any chain of fund transfers in which at least one of the Financial Institutions involved is located in a different country;

(e) "customer identification number" means a number that is different from the unique transaction reference number and:

(i) uniquely identifies the payer to the ordering institution; and

(ii) refers to a record held by the ordering institution that contains at least one of the following: the payer's address, national identity number or date and place of birth;

(f) "domestic fund transfer" means a fund transfer where the ordering institution and beneficiary institution are located in the same country and includes any chain of fund transfers that takes place entirely within a country, even if the system used to transfer the payment message is located in another country;

(g) "fund transfer" means any transaction carried out on behalf of a payer through a Financial Institution by electronic means with a view to making an amount of funds available to a payee at a beneficiary institution, irrespective of whether the payer and the payee are the same person;

(h) "intermediary institution" means the Financial Institution in a serial payment or cover payment chain that receives and transmits a fund transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;

(i) "ordering institution" means the Financial Institution that transfers the funds upon receiving the request for a fund transfer on behalf of the payer;

(j) "payee" means the natural or legal person identified by the payer as the recipient of the requested fund transfer;

(k) "payer" means the account holder who allows the fund transfer from that account or, if there is no account, the natural or legal person that places the fund transfer order with the ordering institution to perform the fund transfer;

(l) "serial payment" means a direct sequential chain of payment where the fund transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution, directly or through one or more intermediary institutions;

(m) "straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention; and

(n) "unique transaction reference number" means a combination of letters, numbers or symbols, determined by the Financial Institution in accordance with the protocols of the payment and settlement system or messaging system used for the fund transfer, and which permits the traceability of the fund transfer.

Requirements for ordering institution

9.3.3 Before effecting a fund transfer, an Authorised Person that is an ordering institution must:

(a) identify the payer and verify the identity of the payer if the identity has not previously been identified; and

(b) record adequate details of the fund transfer that are sufficient to permit its reconstruction, including but not limited to, the date of the transfer, the payer and payee, and the type and amount of currency transferred and the value date.

9.3.4 For a cross-border fund transfer where the amount to be transferred is $1000 or less, an Authorised Person that is an ordering institution must include in the message or payment instruction that accompanies or relates to the fund transfer the following:

(a) the name of the payer;

(b) the payer's account number (or unique transaction reference number if no account number exists);

(c) the name of the payee; and

(d) the payee's account number (or unique transaction reference number if no account number exists).

9.3.5 For a cross-border fund transfer where the amount to be transferred is more than $1,000, an Authorised Person that is an ordering institution must, in addition to the information required by Rule 9.3.4, include in the message or payment instruction that accompanies or relates to the fund transfer any one of the following:

(a) the payer's address:

(b) the payer's national identity number, such as an identity card number or passport number;

(c) the payer's customer identification number; or

(d) the date and place of birth of the payer.

9.3.6 If several individual cross-border fund transfers from a single payer are bundled in a batch file for transmission, then, in complying with Rules 9.3.4 and 9.3.5, an Authorised Person that is an ordering institution must ensure that:

(a) the batch file contains the payer information required under Rule 9.3.4 and, if applicable, Rule 9.3.5;

(b) it has verified the payer information referred to in (a); and

(c) the batch file contains the payee information required under Rule 9.3.4 for each payee and that information is fully traceable in the payee's country.

9.3.7 For a domestic fund transfer, an Authorised Person that is an ordering institution must either:

(a) include in the message or payment instruction that accompanies or relates to the fund transfer the following:

(i) the name of the payer;

(ii) the payer's account number (or unique transaction reference number if no account number exists); and

(iii) any one of the following:

(A) the payer's address;

(B) the payer's national identity number, such as an identity card number or passport number;

(C) the payer's customer identification number; or

(D) the date and place of birth of the payer; or

(b) include only the payer's account number (or unique transaction reference number if no account number exists), provided that:

(i) those details will permit the transaction to be traced back to the payer and payee; and

(ii) the ordering institution must provide the payer information set out in paragraph (a) within 3 business days of a request for the information by the beneficiary institution or the DFSA or immediately upon request of a law enforcement agency.

Guidance

The payer's address referred to in Rule 9.3.5 or 9.3.7 should be the address that the Relevant Person has verified as part of its Customer Due Diligence on the payer.

9.3.8 An Authorised Person that is an ordering institution must retain a record of payer and payee information it has collected under this section.

9.3.9 An Authorised Person that is an ordering institution must not execute a fund transfer if it is unable to comply with the requirements in Rules 9.3.3 to 9.3.8.

Requirements for beneficiary institution

9.3.10 An Authorised Person that is a beneficiary institution must take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border fund transfers that lack the required payer or payee information.

9.3.11 For a cross-border fund transfer, an Authorised Person that is a beneficiary institution must identify and verify the identity of the payee if the identity has not been previously verified.

Requirements for intermediary institution

9.3.12 An Authorised Person that is an intermediary institution must retain all the required payer and payee information accompanying the fund transfer.

9.3.13 If technical limitations prevent the required payer or payee information accompanying a cross-border fund transfer from remaining with a related domestic fund transfer, an Authorised Person that is a receiving intermediary institution must maintain a record, for at least five years, of all the information received from the ordering institution or another intermediary institution.

9.3.14 An Authorised Person that is an intermediary institution must take reasonable measures, which are consistent with straight-through processing, to identify cross-border fund transfers that lack the required payer or payee information.

Systems and controls concerning fund transfers

9.3.15 A Relevant Person must ensure that its AML systems and controls referred to in Rule 5.2.1 include risk management policies and procedures specifying the steps to be taken if a fund transfer lacks information required under this section, including when to reject or amend a transfer and any follow-up action that is to be taken.

Guidance

The DFSA considers that concealing or removing in a fund transfer any of the information required by this section would be a breach of the requirement to ensure that the fund transfer contains accurate payer and payee information.

9.3A Additional requirements for Crypto Token transfers

9.3A.1 This section applies to an Authorised Person that sends or receives Crypto Tokens.

9.3A.2 (1) An Authorised Person must have adequate policies and procedures in place to mitigate the money laundering risks arising from the transfer of Crypto Tokens.

(2) The policies and procedures in (1) must without limitation address the situation where a transfer of Crypto Tokens is received without relevant information and the circumstances in which such transfer should be rejected, reversed (if technically possible), delayed or permitted.

9.3A.3 (1) An Authorised Person must have in place adequate transaction monitoring procedures to detect the origin, any intermediate transaction, and the destination of Crypto Tokens transferred from or to its customer so that it is able to identify and report any suspicious transaction.

(2) The procedures in (1) must provide for the:

(a) tracking of the transaction history of Crypto Tokens to accurately identify their source and destination; and

(b) identification of transactions involving Digital Wallet addresses that are associated with illicit or suspicious activities.

9.3A.4 (1) Before effecting a Crypto Token transfer ("CTT") with a total value of $1,000 or more, an Authorised Person must conduct due diligence on each VASP counterparty involved in the CTT to identify and assess the money laundering risks associated with the transfer and apply appropriate risk-based measures.

(2) The due diligence under (1) must at least:

(a) identify the VASP counterparty;

(b) collect sufficient information about the VASP to understand:

(i) the nature of its business;

(ii) its reputation; and

(iii) the quality and effectiveness of the money laundering regulation and supervision applying to the VASP in the jurisdictions in which it operates;

(c) determine the nature and expected volume and value of the CTT; and

(d) assess the money laundering controls of the VASP counterparty in order to be satisfied that those controls are adequate and effective.

Guidance

1. When an Authorised Person transfers Crypto Tokens it will be exposed to money laundering risks which may vary depending on a number of factors, including: (a) the types of products and services offered; (b) the types of customers to which the counterparty provides services;

(c) geographical exposures of the counterparty and its customers; (d) the anti-money laundering regime in the jurisdictions in which the counterparty operates and/or is incorporated; and (e) the adequacy and effectiveness of the money laundering controls of the counterparty. The purpose of this section is to ensure that an Authorised Person avoids sending or receiving (where possible) Crypto Tokens to or from an illicit actor or a person that had not been subjected to appropriate due diligence measures.

2. An Authorised Person that sends or receives Crypto Tokens on behalf of a customer should be aware of its obligations under Article 33 bis 3 of Cabinet Decision No 10 of 2019. These obligations include the requirement to obtain and keep accurate information on the sender and beneficiary of the transfer and to provide that information to the VASP immediately and securely.

9.3B Additional requirements for NFT and Utility Token transfers

9.3B.1 A DNFBP that sends or receives NFTs or Utility Tokens must comply with the requirements that would apply to an Authorised Person under section 9.3A and for that purpose a reference to a Crypto Token is taken to be a reference to a NFT or Utility Token (as the case may be).

9.4 Audit

9.4.1 An Authorised Person must ensure that its audit function, established under GEN Rule 5.3.13, includes regular reviews and assessments of the effectiveness of the Authorised Person's money laundering policies, procedures, systems and controls, and its compliance with its obligations in this AML module.

Guidance

1. The review and assessment undertaken for the purposes of Rule 9.4.1 may be undertaken:
   a. internally by the Authorised Person's internal audit function; or
   b. by a competent firm of independent auditors or compliance professionals.
2. The review and assessment undertaken for the purposes of Rule 9.4.1 should cover at least the following:
   a. sample testing of compliance with the Authorised Person's CDD arrangements;
   b. an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and
   c. a review of the nature and frequency of the dialogue between the senior management and the MLRO.

10 SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

10.1 Application

[deleted]

10.2 Relevant United Nations resolutions and sanctions

10.2.1 (1) A Relevant Person must establish and maintain effective systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council.

(2) The systems and controls in referred to in (1) must enable the Relevant Person to comply with the requirements in Article 21 of Cabinet Decision No. 74 of 2020.

Guidance

1. Relevant United Nations Security Council resolutions or sanctions mentioned in Rule 10.2.1 may, among other things, relate to money laundering, terrorist financing or the financing of weapons of mass destruction or otherwise be relevant to the activities carried on by the Relevant Person. For example:

   a. a Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a person engaged in money laundering, terrorist financing or the financing of weapons of mass destruction; and

   b. an Authorised Market Institution should exercise due care to ensure that it does not facilitate fund raising activities or listings by persons engaged in money laundering or terrorist financing or financing of weapons of mass destruction.

2. A Relevant Person should be proactive in checking for, and taking measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council. This should include measures that enable the Relevant Person to comply with its obligations in Article 21 of Cabinet Decision No. 74 of 2020 concerning targeted financial sanctions requirements in the UAE, including the obligation to apply or cancel freezing orders and to report and cooperate with regulatory authorities. Relevant Persons should ensure they are fully conversant with these requirements.

3. A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with this module.

10.3 Government, regulatory and international findings

10.3.1 (1) A Relevant Person must establish and maintain systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable steps to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions (each of which is referred to in this Rule as a "finding") issued by:

(a) the government of the U.A.E. or any government departments in the U.A.E.;

(b) the Central Bank of the U.A.E.;

(c) the FIU;

(d) the National Anti-Money Laundering and Combating Financing of Terrorism And Financing of Illegal Organizations Committee (NAMLCFTC);

(e) FATF;

(f) U.A.E. enforcement agencies; and

(g) the DFSA,

concerning the matters in (2).

(2) For the purposes of (1), the relevant matters are:

(a) arrangements for preventing money laundering, terrorist financing or the financing of weapons of mass destruction in a particular country or jurisdiction;

(b) findings that the anti-money laundering regime of a relevant country or jurisdiction has material deficiencies; and

(c) the names of persons, groups, organisations or entities or any other body where suspicion of money laundering or terrorist financing or the financing of weapons of mass destruction exists.

(3) For the purposes of (1), measures in a finding that a Relevant Person must comply with include, but are not limited to, countermeasures:

(a) requiring specific elements of enhanced due diligence;

(b) requiring enhanced reporting mechanisms or systematic reporting of financial transactions;

(c) limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;

(d) prohibiting Relevant Persons from relying on third parties located in a specified jurisdiction to conduct customer due diligence;

(e) requiring correspondent relationships with banks in a specified jurisdiction to be reviewed, amended or, if necessary, terminated;

(f) prohibiting the execution of specified electronic fund transfers; or

(g) requiring increased external audit requirements for financial groups with respect to branches and subsidiaries located in a specified jurisdiction.

(4) The systems and controls referred to in (1) must enable the Relevant Person to comply with the requirements in Article 21 of Cabinet Decision No. 74 of 2020.

(5) A Relevant Person must immediately notify the DFSA in writing if it becomes aware of non-compliance by a person with a finding and provide the DFSA with sufficient details of the person concerned and the nature of the non-compliance.

Guidance

1. The purpose of this Rule is to ensure that a Relevant Person takes into consideration the broad range of tools used by competent authorities and international organisations to communicate AML/CTF risks to stakeholders.

2. The DFSA may require enhanced due diligence or other specific countermeasures to address risks identified in a specific country or jurisdiction. The DFSA may impose such countermeasures either when called upon to do so by FATF or independently of any FATF request.

3. Relevant Persons considering transactions or business relationships with persons located in countries or jurisdictions that have been identified as deficient, or against which the U.A.E. or the DFSA have outstanding advisories, should be aware of the background against which the assessments, or the specific recommendations have been made. These circumstances should be taken into account in respect of introduced business from such jurisdictions, and when receiving inward payments for existing customers or in respect of inter-bank transactions. Relevant Persons should refer to the NAMLCFTC website which provides information concerning national AML and CTF initiatives, including countermeasures for high risk countries and updates on developments for high risk countries pursuant to Article 22 of Cabinet Decision No. 10 of 2019.

4. The Relevant Person's MLRO is not obliged to report all transactions from these countries or jurisdictions to the FIU if they do not qualify as suspicious under the Federal AML legislation, unless instructed to do so by the NAMLCFTC. See chapter 13 on Suspicious Activity Reports.

5. Transactions with counterparties located in countries or jurisdictions which are no longer identified as deficient or have been relieved from special scrutiny (for example, taken off sources mentioned in this Guidance) may nevertheless require attention which is higher than normal.

6. In order to assist Relevant Persons, the DFSA will, from time to time, publish U.A.E., FATF or other findings, guidance, directives or sanctions. However, the DFSA expects a Relevant Person to take its own steps in acquiring relevant information from various available sources. For example, a Relevant Person may obtain relevant information from the consolidated list of sanctions in the U.A.E Cabinet, European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury, as well as from sources containing lists of dual-use goods or goods subject to export control.

7. In addition, the systems and controls mentioned in Rule 10.3.1 should be established and maintained by a Relevant Person taking into account its risk assessment under chapters 5 and 6. In Rule 10.3.1, taking reasonable measures to comply with a finding may mean that a Relevant Person cannot undertake a transaction for or on behalf of a person or that it may need to undertake further due diligence in respect of such a person.

8. A Relevant Person should be proactive in obtaining and appropriately using available national and international information, for example, suspect lists or databases from credible public or private sources with regard to money laundering, including obtaining relevant information from sources mentioned in Guidance 6 above.

9. The risk of terrorists entering the financial system can be reduced if Relevant Persons apply effective AML strategies, particularly in respect of CDD. Relevant Persons should assess which countries carry the highest risks and should conduct an analysis of transactions from countries or jurisdictions known to be a source of terrorist financing.

10. The DFSA may require Relevant Persons to take any special measures it may prescribe with respect to certain types of transactions or accounts where the DFSA reasonably believes that any of the above may pose a money laundering risk to the DIFC.

11 MONEY LAUNDERING REPORTING OFFICER

11.1 Application

[deleted]

11.2 Appointment of a MLRO

11.2.1 (1) A Relevant Person must appoint an individual as MLRO, with responsibility for the implementation of the Relevant Person's anti money laundering policies, procedures, systems and controls and day to day oversight of its compliance with the Rules in this module and other relevant anti money laundering legislation applicable in the DIFC.

(2) A Relevant Person must ensure that the individual appointed as MLRO is suitable to perform the role and has an appropriate level of seniority and independence to act in the role.

(3) The MLRO in (1) and Rule 11.2.5 must be resident in the U.A.E, except in the case of the MLRO for a Registered Auditor or a Representative Office.

Guidance

1. Authorised Firms are reminded that under GEN Rule 7.5.1, the MLRO function is a mandatory appointment. For the avoidance of doubt, the individual appointed as the MLRO of an Authorised Firm, other than a Representative Office, is the same individual who holds the Licensed Function of Money Laundering Reporting Officer of that Authorised Firm. Authorised Firms are also reminded that the guidance under GEN Rule 7.5.2 sets out the grounds under which the DFSA will determine whether to grant a waiver from the residence requirements for an MLRO. The same guidance would apply by analogy to other Relevant Persons seeking a waiver from the MLRO residence requirements.

2. The individual appointed as the MLRO of an Authorised Market Institution is the same individual who holds the position of Money Laundering Reporting Officer of that Authorised Market Institution under the relevant AMI Rule.

11.2.2 [Deleted]

11.2.3 An Authorised Firm, other than a Representative Office, must appoint an individual to act as a deputy MLRO of the Authorised Firm to fulfil the role of the MLRO in his absence.

11.2.4 A Relevant Person's MLRO must deal with the DFSA in an open and co-operative manner and must disclose appropriately any information of which the DFSA would reasonably be expected to be notified.

Guidance

1. The individual appointed as the deputy MLRO of an Authorised Firm need not apply for Authorised Individual status for performing the Licensed Function of Money Laundering Reporting Officer, subject to Rules in GEN section 11.6.

2. A Relevant Person other than an Authorised Firm should make adequate arrangements to ensure that it remains in compliance with this module in the event that its MLRO is absent. Adequate arrangements would include appointing a temporary MLRO for the period of the

MLRO's absence or making sure that the Relevant Person's AML systems and controls allow it to continue to comply with these Rules when the MLRO is absent.

11.2.5 A Relevant Person may outsource the role of MLRO to an individual outside the Relevant Person provided that the relevant individual under the outsourcing agreement is and remains suitable to perform the MLRO role.

Guidance

Where a Relevant Person outsources specific AML tasks of its MLRO to another individual or a third party provider, including within a corporate Group, the Relevant Person remains responsible for ensuring compliance with the responsibilities of the MLRO. The Relevant Person should satisfy itself of the suitability of anyone who acts for it.

11.3 Qualities of a MLRO

11.3.1 A Relevant Person must ensure that its MLRO:

(a) is fit and proper, and has the competence and capability, to perform the MLRO role and has adequate knowledge and understanding of relevant AML legislation;

(b) has direct access to its senior management;

(c) has sufficient resources including, if necessary, an appropriate number of appropriately trained Employees to assist in the performance of his duties in an effective, objective and independent manner;

(d) has a level of seniority and independence within the Relevant Person to enable him to act on his own authority; and

(e) has timely and unrestricted access to information sufficient to enable him to carry out his responsibilities in Rule 11.4.1.

Guidance

1. The DFSA considers that a Relevant Person will need to consider this Rule when appointing an outsourced MLRO. Any external MLRO that is appointed will need to have the actual or effective level of seniority that the role requires and the capacity to fully meet its responsibilities if acting for more than one Relevant Person.

2. To comply with Rule 11.3.1(a), the MLRO should, among other things have sufficient knowledge and understanding of:

   a. the Federal AML Legislation and the DFSA's AML Module and the Relevant Person's obligations under that legislation, including its reporting obligations and the appropriate mechanisms and authorities for that reporting;

   b. the business model of the Relevant Person and the risk profile to which the Relevant Person may be exposed in respect of money laundering, terrorist financing, proliferation financing and targeted financial sanctions.

11.4 Responsibilities of a MLRO

11.4.1 A Relevant Person must ensure that its MLRO implements and has oversight of and is responsible for the following matters:

(a) the day-to-day operations for compliance by the Relevant Person with its AML policies, procedures, systems and controls;

(b) acting as the point of contact to receive notifications from the Relevant Person's Employees under Rule 13.2.2;

(c) taking appropriate action under Rule 13.3.1 following the receipt of a notification from an Employee ;

(d) making Suspicious Activity Reports in accordance with Federal AML legislation;

(e) acting as the point of contact within the Relevant Person for competent U.A.E. authorities and the DFSA regarding money laundering issues;

(f) responding promptly to any request for information made by competent U.A.E. authorities or the DFSA;

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in chapter 10; and

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under chapter 12.

12 AML TRAINING AND AWARENESS

12.1 Training and awareness

12.1.1 A Relevant Person must

(a) provide AML training to all relevant Employees at appropriate and regular intervals;

(b) ensure that its AML training enables its Employees to:

(i) understand the relevant legislation relating to money laundering, including Federal AML legislation;

(ii) understand its policies, procedures, systems and controls related to money laundering and any changes to these;

(iii) recognise and deal with transactions and other activities which may be related to money laundering;

(iv) understand the types of activity that may constitute suspicious activity in the context of the business in which an Employee is engaged and that may warrant a notification to the MLRO under Rule 13.2.2;

(v) understand its arrangements regarding the making of a notification to the MLRO under Rule 13.2.2;

(vi) be aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

(vii) understand the roles and responsibilities of Employees in combating money laundering, including the identity and responsibility of the Relevant Person's MLRO and deputy, where applicable; and

(viii) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in chapter 10; and

(c) ensure that its AML training:

(i) is appropriately tailored to the Relevant Person's activities, including its products, services, customers, distribution channels, business partners, level and complexity of its transactions; and

(ii) indicates the different levels of money laundering risk and vulnerabilities associated with the matters in (c)(i).

Guidance

1. The DFSA considers it appropriate that all new relevant Employees of a Relevant Person be given appropriate AML training as soon as reasonably practicable after commencing employment with the Relevant Person.

2. Relevant Persons should take a risk-based approach to AML training. The DFSA considers that AML training should be provided by a Relevant Person to each of its relevant Employees at intervals appropriate to the role and responsibilities of the Employee. In the case of an Authorised Firm the DFSA expects that training should be provided to each relevant Employee at least annually.

3. The manner in which AML training is provided by a Relevant Person need not be in a formal classroom setting, rather it may be via an online course or any other similarly appropriate manner.

4. A relevant Employee would include a member of the senior management or operational staff, any Employee with customer contact or which handles or may handle customer monies or assets, and any other Employee who might otherwise encounter money laundering in the business.

13 SUSPICIOUS ACTIVITY REPORTS

13.1 Application and definitions

13.1.1 [deleted]

13.1.2 In this chapter, "money laundering" and "terrorist financing" mean the criminal offences defined in the Federal AML legislation.

13.2 Internal reporting requirements

13.2.1 A Relevant Person must establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or transactions in relation to potential money laundering or terrorist financing.

13.2.2 A Relevant Person must have policies, procedures, systems and controls to ensure that whenever any Employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting;

that a person is engaged in or attempting money laundering or terrorist financing, that Employee promptly notifies the Relevant Person's MLRO and provides the MLRO with all relevant details.

Guidance

1. Circumstances that might give rise to suspicion or reasonable grounds for suspicion include:

   a. Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;

   b. Transactions requested by a person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a Relevant Person in relation to a particular customer;

   c. where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection;

   d. where a customer refuses to provide the information requested without reasonable explanation;

   e. where a customer who has just entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;

   f. an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

   g. unnecessary routing of funds through third party accounts; or

   h. unusual transactions without an apparently profitable motive.

2. The requirement for Employees to notify the Relevant Person's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

3. A Relevant Person may allow its Employees to consult with their line managers before sending a report to the MLRO. The DFSA would expect that such consultation does not prevent making a report whenever an Employee has stated that he has knowledge, suspicion or reasonable grounds for knowing or suspecting that a person may be involved in money laundering. Whether or not an Employee consults with his line manager or other Employees, the responsibility remains with the Employee to decide for himself whether a notification to the MLRO should be made.

4. An Employee, including the MLRO, who considers that a person is engaged in or engaging in activity that he knows or suspects to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime of money laundering or terrorist financing.

5. CDD measures form the basis for recognising suspicious activity. Sufficient guidance must therefore be given to the Relevant Person's Employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering or terrorist financing is taking place. This should involve training that will enable relevant Employees to seek and assess the information that is required for them to judge whether a person is involved in suspicious activity related to money laundering or terrorist financing.

6. A transaction that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transaction profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

7. Effective CDD measures may provide the basis for recognising unusual and suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising 'suspicious activity' is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

8. A Relevant Person may consider implementing policies and procedures whereby disciplinary action is taken against an Employee who fails to notify the Relevant Person's MLRO.

13.3 Suspicious activity report

13.3.1 A Relevant Person must ensure that where the Relevant Person's MLRO receives a notification under Rule 13.2.2, the MLRO, without delay:

(a) inquires into and documents the circumstances in relation to which the notification made under Rule 13.2.2 was made;

(b) determines whether in accordance with Federal AML legislation a Suspicious Activity Report must be made to the FIU and documents such determination;

(c) if required, makes a Suspicious Activity Report to the FIU as soon as practicable; and

(d) notifies the DFSA of the making of such Suspicious Activity Report immediately following its submission to the FIU.

13.3.2 Where, following a notification to the MLRO under 13.2.2, no Suspicious Activity Report is made, a Relevant Person must record the reasons for not making a Suspicious Activity Report.

13.3.3 A Relevant Person must ensure that if the MLRO decides to make a Suspicious Activity Report, his decision is made independently and is not subject to the consent or approval of any other person.

Guidance

1. Relevant Persons are reminded that the failure to report suspicions of money laundering or terrorist financing may constitute a criminal offence that is punishable under the laws of the State.

2. SARs under Federal AML legislation should be sent to the FIU via the FIU's electronic system or by other means approved by the FIU.

3. In the preparation of a SAR, if a Relevant Person knows or assumes that the funds which form the subject of the report do not belong to a customer but to a third party, this fact and the details of the Relevant Person's proposed course of further action in relation to the case should be included in the report.

4. If a Relevant Person has reported a suspicion to the FIU, it must in accordance with the Federal AML legislation provide any additional information requested by the FIU. The FIU may instruct the Relevant Person on how to continue its business relationship, including effecting any transaction with a person. If the customer in question expresses his wish to move the funds before the Relevant Person receives instruction from the FIU on how to proceed, the Relevant Person should immediately contact the FIU for further instructions.

13.4 Tipping-off

Guidance

1. Relevant Persons are reminded that in accordance with Federal AML legislation, Relevant Persons or any of their Employees must not disclose, directly or indirectly, to the Customer or to any other person that they have reported, or are intending to report, a suspicious transaction. They also must not disclose information contained in an SAR or the fact that a suspicious transaction is being investigated.

2. If a Relevant Person reasonably believes that performing CDD measures will tip-off a customer or potential customer, it may choose not to pursue that process and should file a SAR. Relevant Persons should ensure that their Employees are aware of and sensitive to these issues when considering the CDD measures.

13.5 Freezing assets

Guidance

The DFSA has power under the Regulatory Law to restrict an Authorised Person from disposing of or transferring property including, for example, assets or other funds suspected of relating to money laundering. It may also apply to the Court for an order restraining a person from transferring or disposing of any assets suspected of relating to money laundering. In cases involving suspected money laundering, the DFSA will usually take such action in co-ordination with the FIU.

14 GENERAL

14.1 Groups, branches and subsidiaries

14.1.1 (1) A Relevant Person which is a DIFC entity must ensure that its policies, procedures, systems and controls required by Rule 5.2.1 apply to:

(a) any of its branches or Subsidiaries; and

(b) any of its Group entities in the DIFC.

(2) Where the anti-money laundering requirements in another jurisdiction differ from those in the DIFC, the Relevant Person must require its branch or Subsidiary in that jurisdiction to apply the higher of the two standards, to the extent permitted by the law of that jurisdiction.

(3) Where the law of another jurisdiction does not permit the implementation of policies, procedures, systems and controls that are equivalent to or higher than those that apply to the Relevant Person in the DIFC, the Relevant Person must:

(a) inform the DFSA in writing; and

(b) apply appropriate additional measures to manage the money laundering risks posed by the relevant branch or Subsidiary.

Guidance

A Relevant Person which is a DIFC entity should conduct a periodic review to verify that any branch or Subsidiary operating in another jurisdiction is in compliance with the obligations imposed under these Rules.

14.1.2 A Relevant Person must:

(a) communicate the policies and procedures which it establishes and maintains in accordance with these Rules to its Group entities, branches and Subsidiaries; and

(b) document the basis for its satisfaction that the requirement in Rule 14.1.1(2) is met.

Guidance

In relation to an Authorised Firm, if the DFSA is not satisfied in respect of AML compliance of its branches and Subsidiaries in a particular jurisdiction, it may take action, including making it a condition on the Authorised Firm's Licence that it must not operate a branch or Subsidiary in that jurisdiction.

14.2 Group policies

14.2.1 A Relevant Person which is part of a Group must ensure that it:

(a) has developed and implemented policies and procedures for the sharing of information between Group entities, including the sharing of information relating to Customer Due Diligence and money laundering risks;

(b) has in place adequate safeguards on the confidentiality and use of information exchanged between Group entities, including consideration of relevant data protection legislation;

(c) remains aware of the money laundering risks of the Group as a whole and of its exposure to the Group and takes active steps to mitigate such risks;

(d) contributes to a Group-wide risk assessment to identify and assess money laundering risks for the Group; and

(e) provides its Group-wide compliance, audit and AML functions with customer account and transaction information from branches and subsidiaries when necessary for AML purposes.

14.3 Notifications

14.3.1 A Relevant Person must inform the DFSA in writing as soon as possible if, in relation to its activities carried on in or from the DIFC or in relation to any of its branches or Subsidiaries, it:

(a) receives a request for information from a regulator or agency responsible for AML, counter-terrorism financing, or sanctions regarding enquiries into potential money laundering or terrorist financing or sanctions breaches;

(b) becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;

(c) becomes aware of any money laundering or sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or

(d) becomes aware of a significant breach of a Rule in this module or a breach of Federal AML legislation by the Relevant Person or any of its Employees.

14.4 Record keeping

14.4.1 A Relevant Person must maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;

(b) records (consisting of the original documents or certified copies) in respect of the customer business relationship, including:

(i) business correspondence and other information relating to a customer's account;

(ii) sufficient records of transactions to enable individual transactions to be reconstructed; and

(iii) internal findings and analysis relating to a transaction or any business, such as if the transaction or business is unusual or suspicious, whether or not it results in a Suspicious Activity Report;

(c) notifications made under Rule 13.2.2;

(d) Suspicious Activity Reports and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the FIU;

(f) the documents in Rule 14.4.2; and

(g) any other matter that the Relevant Person is expressly required to record under these Rules,

for at least six years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

14.4.1A A Relevant Person must provide to the DFSA or a law enforcement agency immediately on request a copy of a record referred to in Rule 14.4.1.

14.4.2 A Relevant Person must document, and provide to the DFSA immediately on request, any of the following:

(a) the risk assessment of its business undertaken under Rule 5.1.1;

(b) how the assessment in (a) was used for the purposes of complying with Rule 6.1.1(1);

(c) the risk assessment of the customer undertaken under Rule 6.1.1(1)(a); and

(d) the determination made under Rule 6.1.1(1)(b).

Guidance

1. The records required to be kept under Rule 14.4.1 may be kept in electronic format, provided that such records are readily accessible and available to respond promptly to any DFSA requests for information. Authorised Persons are reminded of their obligations in GEN Rule 5.3.24.

2. If the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

3. The records maintained by a Relevant Person should be kept in such a manner that:

   a. the DFSA or another competent authority is able to assess the Relevant Person's compliance with legislation applicable in the DIFC;

   b. any transaction which was processed by or through the Relevant Person on behalf of a customer or other third party can be reconstructed;

   c. any customer or third party can be identified; and

d. the Relevant Person can satisfy without delay any regulatory enquiry or court order to disclose information.

4. The DFSA would ordinarily expect a Relevant Person to be able to provide a copy of a record or assessment referred to in Rule 14.4.1 or 14.4.2 within 24 hours of a request by the DFSA. However, if a request is complex or if records are kept outside the DIFC as set out in Rule 14.4.3, the DFSA may allow further time to comply with the request.

14.4.3 Where the records referred to in Rule 14.4.1 are kept by the Relevant Person outside the DIFC, a Relevant Person must:

(a) take reasonable steps to ensure that the records are held in a manner consistent with these Rules;

(b) ensure that the records are easily accessible to the Relevant Person; and

(c) upon request by the DFSA, ensure that the records are immediately available for inspection.

14.4.4 A Relevant Person must:

(a) verify if there is secrecy or data protection legislation that would restrict access without delay to the records referred to in Rule 14.4.1 by the Relevant Person, the DFSA or the law enforcement agencies of the U.A.E.; and

(b) where such legislation exists, obtain without delay certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons in (a).

14.4.5 A Relevant Person must be able to demonstrate that it has complied with the training and awareness requirements in chapter 12 through appropriate measures, including the maintenance of relevant training records.

Guidance

1. In complying with Rule 14.4.3, Authorised Persons are reminded of their obligations in GEN Rule 5.3.24.

2. The DFSA considers that "appropriate measures" in Rule 14.4.5 may include the maintenance of a training log setting out details of:

   a. the dates when the training was given;

   b. the nature of the training; and

   c. the names of Employees who received the training.

14.5 Annual AML return

14.5.1 A Relevant Person must complete the AML Return form on the DFSA electronic portal and submit it to the DFSA by the end of September each year. The annual AML Return must cover the period from 1 August of the previous year to 31 July of the reporting year.

14.6 Communication with the DFSA

14.6.1 A Relevant Person must:

(a) be open and cooperative in all its dealings with the DFSA; and

(b) ensure that any communication with the DFSA is conducted in the English language.

14.7 Employee disclosures

14.7.1 A Relevant Person must ensure that it does not prejudice an Employee who discloses any information regarding money laundering to the DFSA or to any other relevant body involved in the prevention of money laundering.

Guidance

The DFSA considers that "relevant body" in Rule 14.7.1 would include the FIU or another financial intelligence unit, the police, or a Dubai or Federal ministry.

14.8 Decision making procedures

14.8.1 The procedures in Schedule 3 to the Regulatory Law apply to a decision of the DFSA to impose an administrative penalty under Article 14(1) of Federal Law No. 20 of 2018.

14.8.2 If the DFSA decides to exercise its power under Article 14(1) of Federal Law No. 20 of 2018 in relation to a person, the person may refer the matter to the FMT for review.

Guidance

The Rules in this section apply where the DFSA makes a decision to impose an administrative penalty under Federal Law No. 20 of 2018. The administrative penalties referred to in that Article include fines, bans from working in a sector, suspension or restriction of activities and other measures. The DFSA may also impose sanctions under DIFC laws, for example, under Article 90 of the Regulatory Law, in which case, the relevant provision will specify the procedures that apply.

15 DNFBP REGISTRATION AND SUPERVISION

Guidance

1. A DNFBP should ensure that it complies with and has regard to relevant provisions of the Regulatory Law. The Regulatory Law gives the DFSA a power to supervise DNFBPs' compliance with relevant AML laws in the State. The Regulatory Law requires a DNFBP to be registered by the DFSA to conduct its activities in the DIFC. Rule 15.1.2 sets out the criteria a DNFBP must meet to be registered. The Regulatory Law also gives the DFSA a number of other important powers in relation to DNFBPs, including powers of enforcement. This includes a power to obtain information and to conduct investigations into possible breaches of the Regulatory Law. The DFSA may impose fines for breaches of the Regulatory Law or the Rules. It may also suspend or withdraw the registration of a DNFBP in various circumstances.

2. The DFSA takes a risk-based approach to regulation of persons which it supervises. Generally, the DFSA will work with DNFBPs to identify, assess, mitigate and control relevant risks where appropriate. RPP describes the DFSA's enforcement powers under the Regulatory Law and outlines its policy for using these powers.

3. Rule 3.2.1 defines a DNFBP by setting out a list of businesses or professions which, if carried on in or from the DIFC, constitute a DNFBP.

4. In determining if a person is carrying on a business or profession in the DIFC that falls within the DNFBP definition, the DFSA will adopt a 'substance over form' approach. That is, it will consider what business or profession is in fact being carried on, and its main characteristics, and not just what business or profession the person purports, or is licensed, to carry on in the DIFC.

5. The DFSA considers that "a law firm, notary firm or other independent legal business" in paragraph (1)(d) of the DNFBP definition, includes any business or profession that involves a legal service, including advice or services related to laws in the State or other jurisdictions. The DFSA does not consider it necessary for the purposes of the definition that:

   a. the relevant person is licensed to provide legal services in the State; or

   b. the individuals or employees providing the legal service are qualified or authorised to do so, whether in the State or in any other jurisdiction.

6. The DFSA considers that "an accounting firm, audit firm or insolvency firm" in paragraph (1)(e) of the DNFBP definition, includes forensic accounting services that use accounting skills, principles and techniques to investigate suspected illegal activity or to analyse financial information for use in legal proceedings.

7. The DFSA would also consider a tax advisory business carried on in or from the DIFC to be a DNFBP as it is likely to involve elements of both legal and accounting services i.e. advice on taxation law and the use of accounting skills to analyse financial records, and so fall within either paragraph (1)(d) or (e) of the DNFBP definition.

15.1 Registration and notifications

15.1.1 An applicant for registration as a DNFBP must apply to the DFSA by completing and submitting the appropriate form on the DFSA electronic portal.

15.1.2 (1) To be registered as a DNFBP, an applicant must demonstrate to the DFSA's satisfaction that:

(a) it is fit and proper to perform anti-money laundering functions; and

(b) it has adequate resources and systems and controls, including policies and procedures, to comply with applicable anti-money laundering requirements under Federal AML legislation, the Regulatory Law and these Rules.

(2) In assessing if an applicant is fit and proper under (1)(a), the DFSA may, without limiting the matters it may take into account under that paragraph, consider the applicant, its senior management, its beneficial owners, other entities in its Group and any other person with whom it has a relationship.

(3) The DFSA will in assessing if an applicant is fit and proper, consider the cumulative effect of matters that, if taken individually, may be regarded as insufficient to give reasonable cause to doubt the fitness and propriety of the applicant.

Guidance

Under the Regulatory Law, the DFSA may suspend or withdraw the registration of a DNFBP where the DNFBP no longer meets the criteria for registration.

Annual Information Return

15.1.3 A DNFBP must complete the annual information return in AFN for each calendar year and submit the return to the DFSA by 31 January of the following year.

Notification of changes

15.1.4 A DNFBP must notify the DFSA, by completing and submitting the appropriate form on the DFSA electronic portal, of any change in its:

(a) name;

(b) legal status;

(c) address;

(d) MLRO;

(e) senior management; or

(f) beneficial ownership,

before such change takes effect or promptly thereafter if it is not possible to make the notification before the change takes effect.

15.2 Request to withdraw registration

15.2.1 (1) A DNFBP must notify the DFSA in writing 14 days in advance of it ceasing to carry on its DNFBP business activities in or from the DIFC.

(2) The notice must include a request to cancel its registration, an explanation of the reason for it ceasing business, and attached copies of any relevant documents.

Guidance

1. A DNFBP may request the withdrawal of its registration because, for example, it no longer meets the definition of a DNFBP, becomes insolvent or enters into administration, or proposes to leave the DIFC.

2. In addition to being able to withdraw registration at a DNFBP's request, the DFSA may suspend or withdraw the registration of a DNFBP on its own initiative in various circumstances (see Article 71F of the Regulatory Law).

15.3 Disclosure of regulatory status

15.3.1 A DNFBP must not:

(a) misrepresent its regulatory status with respect to the DFSA expressly or by implication; or

(b) use or reproduce the DFSA logo without express written permission from the DFSA and in accordance with any conditions for use.

15.3A Whistleblowing

Interpretation

15.3A.1 In this section:

(a) "regulatory concern", in relation to a DNFBP, means a concern held by any person that the DNFBP or an officer or employee of the DNFBP has or may have:

(i) contravened a provision of legislation administered by the DFSA; or

(ii) engaged in money laundering, fraud or any other financial crime;

(b) "whistleblower" means a person who reports a regulatory concern to a person specified in Article 68A(3) of the Regulatory Law.

Policies and procedures

15.3A.2 (1) A DNFBP must have appropriate and effective policies and procedures in place:

(a) to facilitate the reporting of regulatory concerns by whistleblowers; and

(b) to assess and, where appropriate, escalate regulatory concerns reported to it.

(2) The policies and procedures required under (1) must be in writing.

(3) A DNFBP must periodically review the policies and procedures to ensure they are appropriate, effective and up to date.

Record of whistleblowing reports

15.3A.3 An Authorised Person must maintain a written record of each regulatory concern reported to it by a whistleblower, including appropriate details of the regulatory concern and the outcome of its assessment of the reported concern.

Guidance

1. The requirements in this section apply only to a DNFBP, as other Relevant Persons are subject to similar requirements in other parts of the Rulebook – see, for example, GEN 5.4 and AUD 4.11.

2. The DFSA expects a DNFBP to implement policies and procedures under Rule 15.3A.2 that are appropriate based on the nature, scale and complexity of the DNFBP's business. For example, a larger or more complex DNFBP is expected to have more detailed and comprehensive policies and procedures in place.

3. The policies and procedures should:

    a. include internal arrangements to allow for reports to be made by whistleblowers;

    b. include adequate procedures to deal with, assess and, where appropriate, escalate reports to the senior management of the DNFBP or, if necessary, to the DFSA or to any other relevant authority;

    c. include reasonable measures to protect the identity and confidentiality of whistleblowers;

    d. include reasonable measures to protect the whistleblower from suffering any detriment, as a result of the report;

    e. ensure that, where appropriate and feasible, feedback is provided to the whistleblower; and

    f. include reasonable measures to manage any conflicts of interest and ensure the fair treatment of any person who is the subject of an allegation in a report.

4. A DNFBP's whistleblowing policies and procedures should generally encourage reporting of concerns first to the DNFBP itself. However, the policies and procedures should also take into account that there may be circumstances where it is appropriate, or a whistleblower may prefer, to report the concerns directly to the DFSA or to another relevant authority.

5. The records under Rule 15.3A.3 should include:

    a. the date the report was received;

    b. a summary of the concerns raised;

    c. steps taken by the DNFBP in relation to the report until the matter is resolved;

    d. any steps taken to maintain the confidentiality of the whistleblower and to ensure fair treatment of the whistleblower;

    e. the list of persons who have knowledge of the report;

    f. the outcome of the assessment of the report including the rationale for the outcome and any decision on whether or not to disclose the report to the DFSA or any other relevant authority; and

    g. references or links to all documentation and review papers in relation to the report.

6. A DNFBP may be required to make its records of whistleblowing reports available to the DFSA for inspection.

7. In addition to the requirements in these Rules, Article 68A of the Regulatory Law provides legal protection to a whistleblower who discloses information about suspected misconduct in good faith to a specified person, such as the relevant DNFBP, the auditor of the DNFBP, the DFSA or other relevant authorities.

8. The protection under the Regulatory Law applies to any person who makes such a disclosure. For example, the disclosure may be made by a person who is or has been an officer, employee or agent of a DNFBP, a Person who provides services or products to a DNFBP or a person who has no formal connection with the DNFBP.

9. The protection under the Regulatory Law is from liability, dismissal or detriment for making that disclosure. However, it does not, for example, prevent a DNFBP from taking action against an employee for other legitimate reasons, such as if the employee has engaged in misconduct.

10. A DNFBP should, as part of its policies and procedures, inform its officers and employees of the protection under Article 68A of the Regulatory Law.

15.4 Transitional

15.4.1 (1) This Rule applies to a Person who, immediately before the commencement date, was registered as a DNFBP, other than a Person who was registered as a DNFBP by reason only of being a dealer in any saleable item of a price equal to or greater than $15,000.

(2) The Person is on the commencement date taken to continue to be registered by the DFSA as a DNFBP.

(3) The Person must, by no later than the end of the transitional period, certify in writing to the DFSA:

(a) that it continues to carry on its DNFBP business or profession in or from the DIFC;

(b) the names of the individuals who comprise its senior management;

(c) details of its beneficial owners;

(d) the name of the individual it has appointed as MLRO; and

(e) that it has in place adequate resources and systems and controls to comply with applicable anti-money laundering requirements under the Law, these Rules and Federal AML legislation.

(4) The DFSA may require the certification in (3) to be in such form and verified in such manner as it thinks fit.

(5) In this Rule:

(a) "commencement date" means the day on which the Regulatory Law Amendment Law 2018 comes into force; and

(b) "transitional period" means the period starting on the commencement date and ending three months after that date.

Guidance

If a DNFBP fails to provide the duly completed certification to the DFSA by the end of the transitional period, it will contravene these Rules. The DFSA may because of that failure take steps to suspend or withdraw the DNFBP's registration.

16 TRANSITIONAL RULES

16.1 Application

16.1.1 This chapter applies to every person to whom a provision of the Previous Regime applied.

16.1.2 For the purposes of this chapter:

(a) "Ancillary Service Provider" has the meaning that it had under the Previous Regime;

(b) "Commencement Date" means 14 July 2013;

(c) "Current Regime" means the Rules in force on the Commencement Date;

(d) "DNFBP" has the meaning that it had in DNF chapter 2 under the Previous Regime; and

(e) "Previous Regime" means the Rules that were in force immediately prior to the Commencement Date.

16.2 General

16.2.1 A Relevant Person must continue to maintain any records required to be maintained under the Previous Regime until such time as the requirement to hold such record would have expired had the Previous Regime still been in force.

16.3 Specific relief – Ancillary Service Provider and DNFBPs

16.3.1 A person who, immediately prior to the Commencement Date, was an Ancillary Service Provider or was registered as a DNFBP is deemed, on the Commencement Date, to be registered as a DNFBP for the purposes of the Current Regime.