Appendix 1

In this appendix as all the text is new it is not underlined or struck through in the usual manner.

The DFSA Rulebook

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

(AML)

in relation to Consultation Papers No. 86 and 89

Contents

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

1 INTRODUCTION

1.1 Application

1.1.1 (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.

(2) For a dealer in precious metals or precious stones, or a dealer in any saleable item of a price equal to or greater than $15,000, chapters 6 to 8 of this module apply only if it engages in any cash or cash-equivalent transaction with a customer equal to or above $15,000, whether the transaction is executed as a single operation or in several connected operations.

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) an 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

* Partially applicable. Relevant Persons should consider these chapters and determine which provisions apply.

Relevant Person	Applicable Chapters			
Authorised Person	**1 - 14**			
Representative Office	**1 - 5**	**10- 14**		
Auditor	**1 -8**	**10 - 14**		
Real estate developer or agency	**1 - 8**	**10 - 16**		
Law firm, notary firm, or other independent legal business	**1 - 8**	**10 - 16**		
Accounting firm, audit firm or insolvency firm	**1 - 8**	**10 - 16**		
Company service provider	**1 - 8**	**10 - 16**		
Single Family Office	**1 - 8**	**10 - 16**		
Dealer in precious metals or precious stones	**1 - 8**	**12**	**13***	**14 - 16**
Dealer in high-value goods	**1 - 8**	**12**	**13***	**14 - 16**

2 OVERVIEW AND PURPOSE OF THE MODULE

Guidance

1. The AML module has been designed to provide a single reference point for all persons and entities (collectively called Relevant Persons) who are supervised by the DFSA for Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and sanctions compliance. Accordingly it applies to Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions (DNFBP), and Auditors, but to each in different degrees. 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.

2. The AML module cannot be read in isolation from other relevant 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 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.

3. 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.

4. 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.

5. 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 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 client on-boarding but may also occur when undertaking on-going CDD.

6. 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.

7. Chapter 9 sets out certain obligations in relation to correspondent banking, wire transfers and other matters which are limited to Authorised Persons, and, in particular, to banks.

8. 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).

9. Chapter 11 sets out the obligation for a Relevant Person (other than certain DNFBPs) to appoint an MLRO and the responsibilities of such a person.

10. 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.

11. Chapter 13 contains the obligations applying to all Relevant Persons concerning Suspicious Activity Reports, which are required to be made under Federal Law No. 4 of 2002.

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

13. 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

14. Under Article 70(3) of the Regulatory Law 2004 (the "Law"), the DFSA has jurisdiction for the regulation of anti-money laundering in the DIFC. This module sets out the regulatory requirements imposed by the DFSA under Article 72 of the Law. 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. 4 of 2002 regarding the Criminalisation of Money Laundering, Federal Law No. 1 of 2004 regarding Combating Terrorism Offences and the Penal Code of the United Arab Emirates. The Rules in this module should not be relied upon to interpret or determine the application of the criminal laws of the U.A.E.

15. Under Article 3 of the Federal Law No.4 of 2002, a Relevant Person may be criminally liable for the offence of money laundering if such an activity is intentionally committed in its name or for its account. Relevant Persons are also reminded that:

    a. the failure to report suspicions of money laundering;

    b. "tipping off"; and

    c. assisting in the commission of money laundering,

    may each constitute a criminal offence that is punishable under the laws of the U.A.E.

Financial Action Task Force

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

17. 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.

18. 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.

19. 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 make appropriate use of UNSC sanctions and resolutions (See chapter 10).

20. 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.

21. 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.

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 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. A Relevant Person should note that, 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.

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.
AMLSCU	Means the Anti-Money Laundering Suspicious Cases Unit of the U.A.E. Central Bank.
Auditor	Means a partnership or company that is registered by the DFSA to provide audit services to: (a) an Authorised Person; (b) a Domestic Fund; or (c) a Public Listed Company.
Authorised Person	Means an Authorised Firm or an Authorised Market Institution.
beneficial owner	Means, in relation to a customer, a natural person: (a) who ultimately controls, directly or indirectly, a customer; (b) who, in relation to a customer which is a legal person or arrangement, exercises (whether directly or indirectly) ultimate effective control over the person or arrangement, or the management of such person or arrangement; (c) who ultimately owns or has an ownership interest in

	the customer, whether legally or beneficially, directly or indirectly; (d) on whose behalf or for whose benefit a transaction is being conducted; or (e) on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act. A person not falling into (a) or (b) is not a beneficial owner by reason of (c) or (d) if, having regard to a risk-based assessment of the customer, the ownership interest is small and in the circumstances poses no or negligible risk of money laundering. In (a) to (e), a reference to a "customer" includes a customer account, customer assets and the underlying legal person or arrangements which constitute or make up the customer, customer account or customer assets.
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.
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; (d) in relation to a Single Family Office, a member of the Single Family; or (e) a person with whom a Relevant Person is otherwise establishing or has established a business relationship.
Customer Due Diligence (CDD)	Has the meaning in Rule 7.3.1.
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; (c) a dealer in any saleable item of a price equal to or greater than $15,000; (d) a law firm, notary firm, or other independent legal business; (e) an accounting firm, audit firm or insolvency firm; (f) a company service provider; or (g) a Single Family Office. (2) A person who is an Authorised Person or an 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 Law No. 1 of 2004	Means UAE Federal Law No. 1 of 2004 regarding Combating Terrorism Offences.
Federal Law No. 4 of 2002	Means UAE Federal Law No. 4 of 2002 regarding the Criminalisation of Money Laundering.
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.
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).
Law	Means the Regulatory Law 2004.
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, trusts, 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.

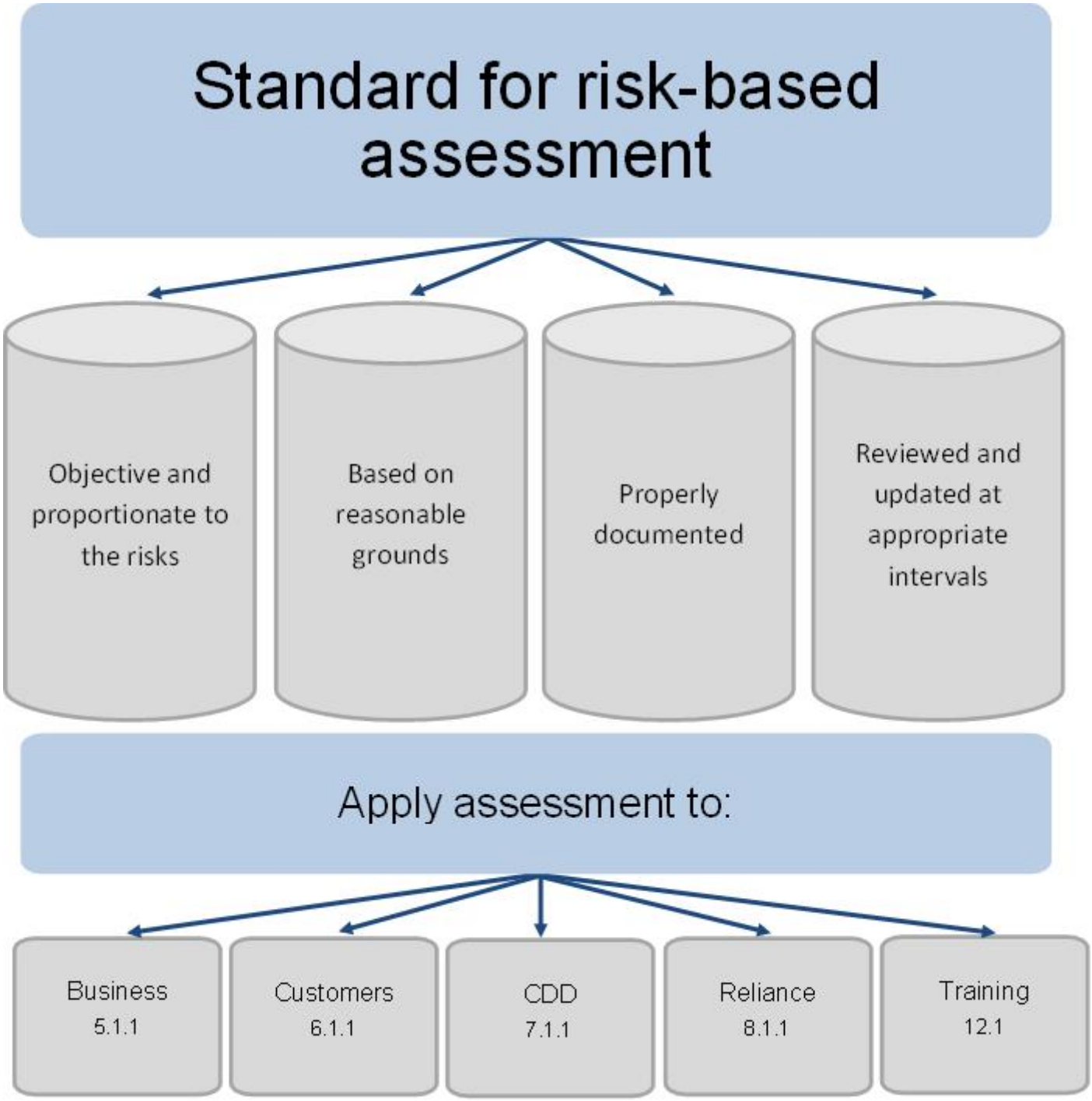
Money Laundering Reporting Officer (MLRO)	Means the person appointed by a Relevant Person pursuant to Rule 11.2.1(1).
natural person	Means an individual.
person	Means a natural or legal person.
Politically Exposed Person (PEP)	Means a natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, including but not limited to, a head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior executive of a state owned corporation, or an important political party official, but not middle ranking or more junior individuals in these categories.
Prescribed Low Risk Customer	Means any of the following customer types: (a) an Authorised Firm; (b) an Authorised Market Institution; (c) a Financial Institution whose entire operations are subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations; (d) a Subsidiary of a Financial Institution referred to in (c), provided that the law that applies to the parent company ensures that the Subsidiary also observes the same AML standards as its Parent; (e) a law firm, notary firm, or other independent legal business or an equivalent person in another jurisdiction whose entire operations are subject to AML regulation and supervision by a competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; (f) an accounting firm, Auditor or other audit firm or insolvency firm or an equivalent person in another jurisdiction whose entire operations are subject to AML regulation and supervision by a competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; (g) a company whose Securities are listed on a Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules; (h) a government body or a non-commercial government entity in the U.A.E. or a FATF member country; and (i) a customer where the business relationship is limited

	to the provision of one or more of the following products or services: (i) a Contract of Insurance which is non-life insurance; (ii) a Contract of Insurance which is a life insurance product with no investment return or redemption or surrender value; (iii) a Contract of Insurance which is life insurance where the annual premium is no more than $1,000 or where a single premium of no more than $2,500 is paid; (iv) a Contract of Insurance for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral; (v) a Contract of Insurance which is a reinsurance contract not falling into (i) to (iv) which is ceded by an insurer who is a regulated Financial Institution; (vi) a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an Employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme; or (vii) arbitration, litigation or advice on litigation prospects.
Public Listed Company	Has the meaning given in Article 97(2) of the Regulatory Law 2004.
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 in Rule 1.1.2.
senior management	Means, 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 SEO or equivalent, such as the managing director; or (c) for an Auditor, every member of the Relevant

	Person's executive management in the U.A.E.
Simplified Customer Due Diligence	Means Customer Due Diligence as modified under Rule 7.5.1.
Single Family	Has the meaning given to that term in the DIFC Single Family Office Regulations.
Single Family Office	Has the meaning given to that term in the DIFC Single Family Office Regulations.
source of funds	Means the origin of customer's funds which relate to a transaction or service and includes how such funds are connected to a customer's source of wealth.
source of wealth	Means how the customer's global wealth or net worth is or was acquired or accumulated.
Subsidiary	Has the meaning given in Schedule 1 to the DIFC Companies Law.
Suspicious Activity Report (SAR)	Means a report in the prescribed format regarding suspicious activity (including a suspicious transaction) made to the AMLSCU under Rule 13.3.1(c).
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.

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 adopting an approach which is proportionate to 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

(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.

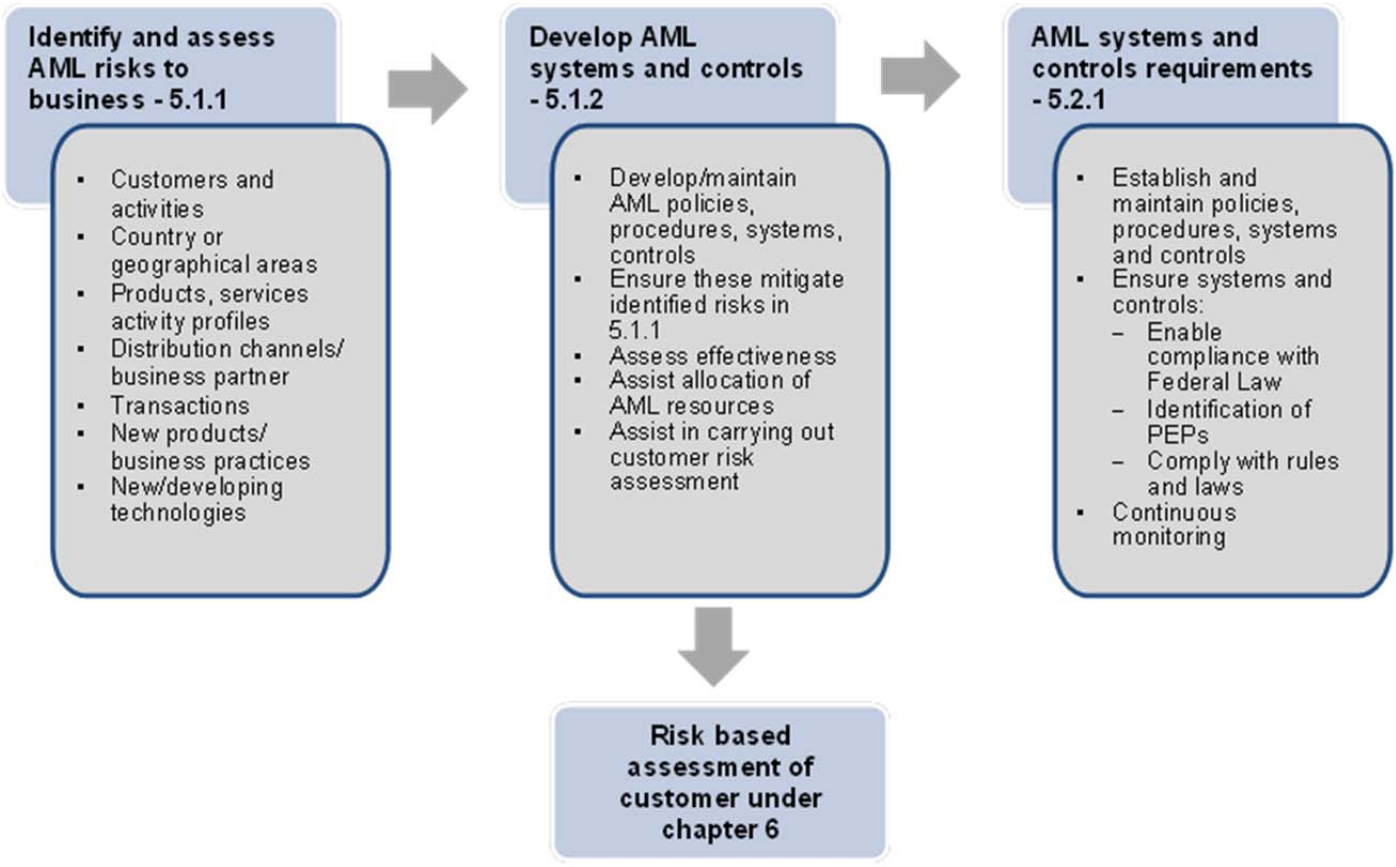
2. In implementing the RBA, a Relevant Person is expected to have in place processes to identify, assess, monitor, manage and mitigate money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted. Simplified measures are not permitted where there is a suspicion of money laundering.

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;

(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.

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 to 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. For instance, if a Relevant Person reasonably concludes that a particular business line poses a negligible risk of money laundering, it may decide, using the RBA, that all its customers in that business line should be treated as posing a lower risk of money laundering, and it may apply Simplified Customer Due Diligence.

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;

(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;

(ii) enable it to determine whether a customer or a beneficial owner is a Politically Exposed Person; and

(iii) enable the Relevant Person to comply with these Rules, Federal Law No.4 of 2002, Federal Law No.1 of 2004 and any other relevant Federal laws; and

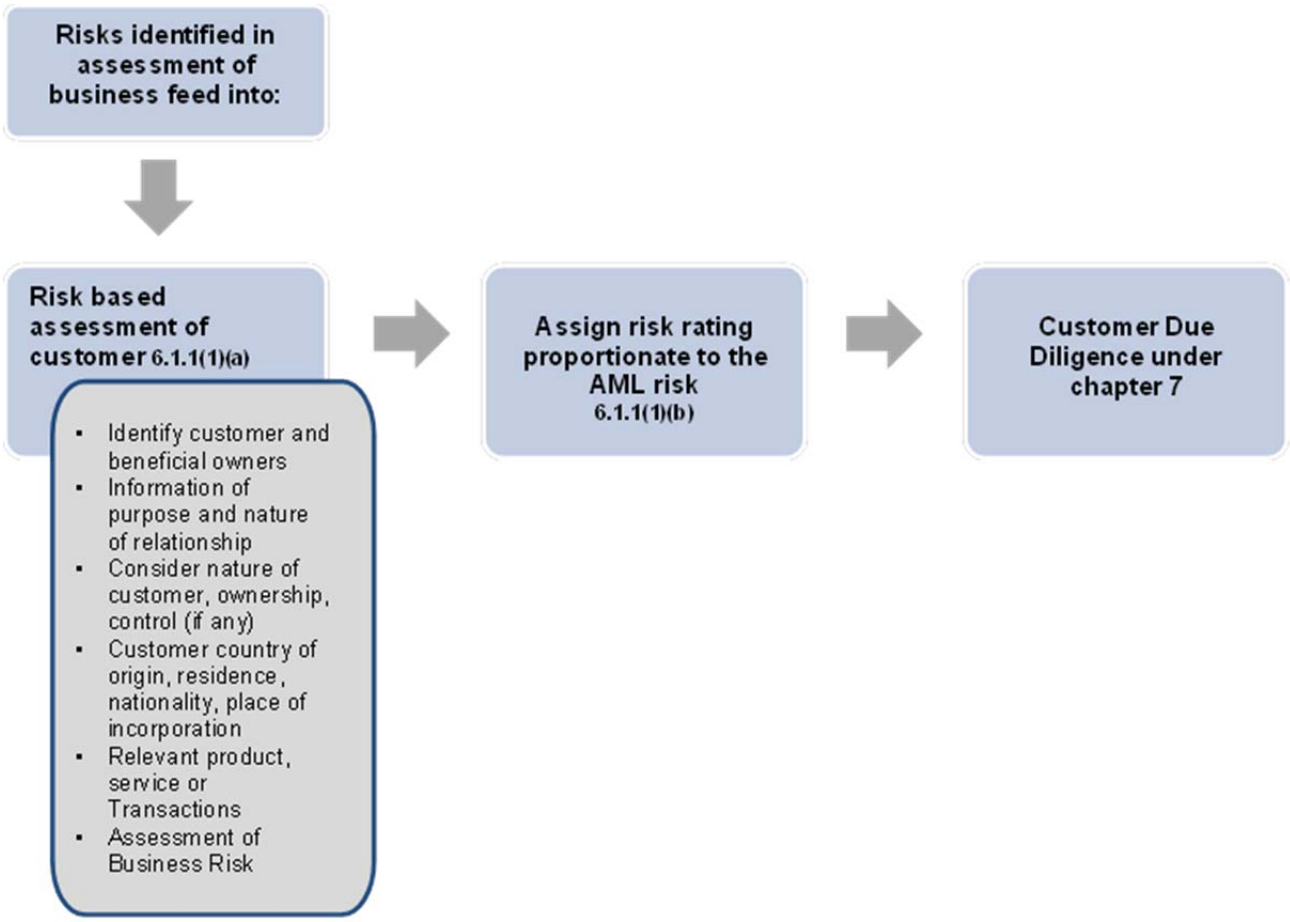
(c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and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

Guidance

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.

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. Examples of such relevant information include information on the source of funds or wealth or 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) A Relevant Person may assign a low risk rating to a Prescribed Low Risk Customer without the need to undertake the risk-based assessment of the customer under (1)(a).

(4) Where a Relevant Person has assigned a customer a low risk rating under (3) and the customer ceases to meet the criteria to be a Prescribed Low Risk Customer the Relevant Person must undertake the risk-based assessment of the customer under (1)(a).

(5) 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) 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; and

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

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

Guidance on the customer risk assessment

1. In assessing the nature of a customer, a Relevant Person should consider such factors as the legal structure of the customer, the customer's business or occupation, the location of the customer's business and the commercial rationale for the customer's business model.

2. In assessing the customer business relationship, a Relevant Person should consider how the customer is introduced to the Relevant Person and how the customer is serviced by the Relevant Person, including for example, whether the Person will be a private banking client, will open a bank account or whether the business relationship will be purely advisory.

3. 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.

4. 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, such as those in part (i) of the definition of a Prescribed Low Risk Customer, or may be a long-standing customer of a Group company who has been introduced to the Relevant Person.

5. In Rule 6.1.2, 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"

6. 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 client agreement or the acceptance of terms of business.

7. 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).

8. 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.

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

Guidance on high risk customers

10. In complying with Rule 6.1.1, the DFSA considers that a Relevant Person should consider the following factors, which may indicate that a customer poses a higher risk of money laundering:

    a. the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the location of the Relevant Person and the customer);

    b. legal persons or arrangements that are personal investment vehicles;

    c. companies that have nominee shareholders or directors or shares in bearer form;

d. businesses that are cash-intensive;

e. the ownership structure of the legal person appears unusual or excessively complex given the nature of the legal person's business or activities;

f. countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML systems;

g. countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations Security Council or identified by credible sources as having significant levels of corruption or other criminal activity;

h. countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;

i. a person not meeting the definition of a PEP but whose high profile or influence poses an elevated risk of corruption;

j. anonymous transactions (which may include cash);

k. private banking relationships;

l. non-face-to-face business relationships or transactions;

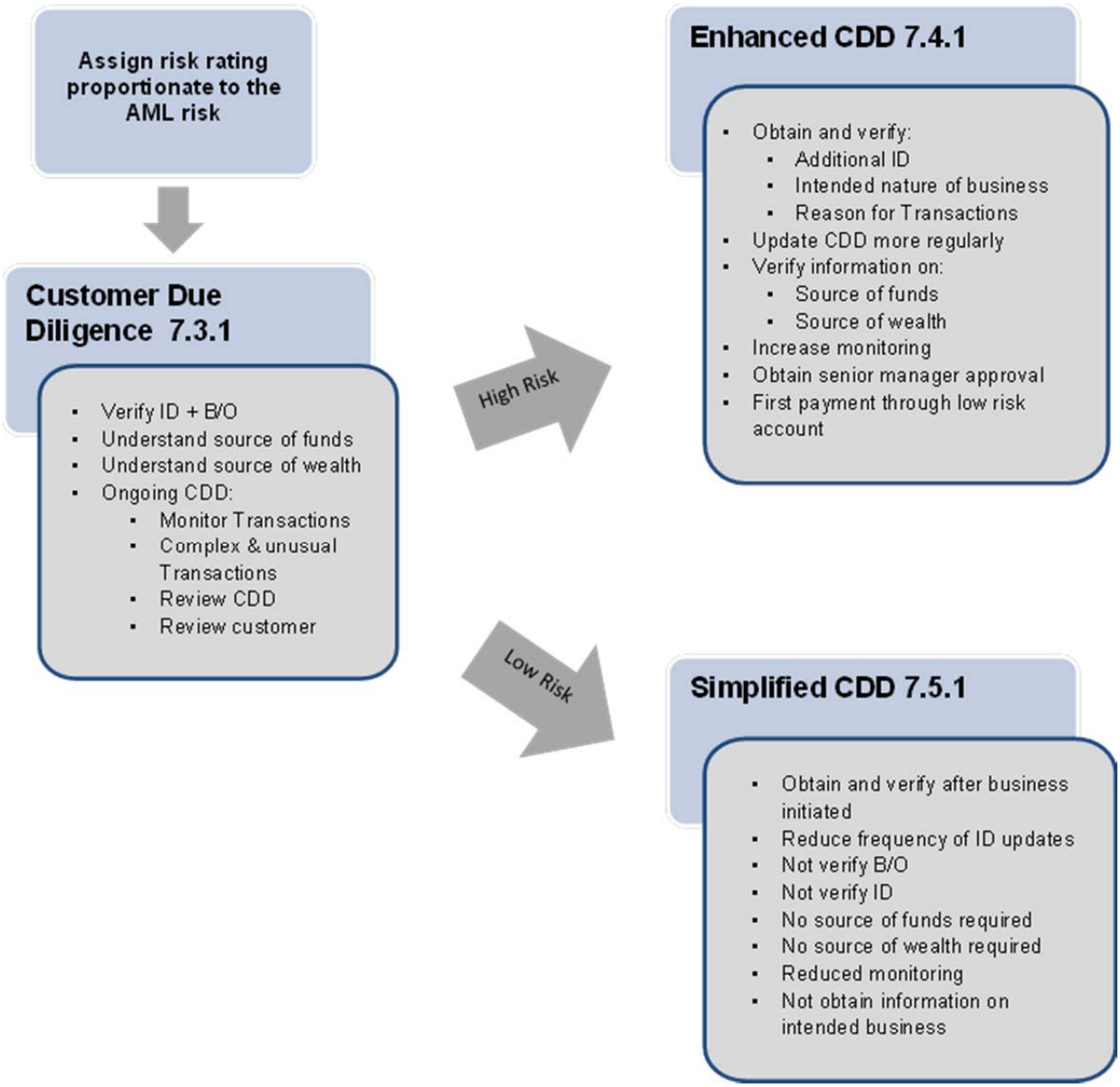
m. payment received from unknown or un-associated third parties;

n. discretionary trusts; and

o. charitable trusts and waqfs.

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 Rule 7.3.1 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 Rule 7.3.1 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 Rule 7.3.1. However, for high risk customers, additional Enhanced CDD measures should also be undertaken under Rule 7.4.1. For low risk customers, Rule 7.3.1 may be modified according to the risks in accordance with Rule 7.5.1.

7.2 Timing of customer due diligence

7.2.1 (1) A Relevant Person must:

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

(b) undertake the appropriate Customer Due Diligence under Rule 7.3.1(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.

(3) 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 (4), 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.

(4) Where a Relevant Person is not reasonably able to comply with the 30 day requirement in (3)(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 (3) as soon as possible; and

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

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

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 7.2.1(3)(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 7.2.1(3)(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

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

(a) verify the identity of the customer and any beneficial owner on the basis of original or properly certified documents, data or information issued by or obtained from a reliable and independent source;

(b) understand the customer's source of funds;

(c) understand the customer's source of wealth; and

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

(2) In complying with (1)(a) for life insurance or other similar policies, a Relevant Person must:

(a) verify the identity of any named beneficiaries of the insurance policy; and

(b) verify the identity of the persons in any class of beneficiary, or where these are not identifiable, ensure that it obtains sufficient information to be able to verify the identity of such persons at the time of payout of the insurance policy.

(3) Where a customer, or a beneficial owner of the customer, is a Politically Exposed Person, a Relevant Person must ensure that, in addition to (1) it also:

(a) increases 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; and

(b) obtains the approval of senior management to commence a business relationship with the customer,

unless the customer is a Prescribed Low Risk Customer.

Guidance on CDD

1. A Relevant Person should, in complying with Rule 7.3.1(1)(a), and adopting the RBA, obtain, verify and record, for every customer who is a natural person, the following identification information:

a. full name (including any alias);

b. date of birth;

c. nationality;

d. legal domicile; and

e. current residential address (not a P.O. box).

2. Items (a) to (c) above should be obtained by sighting a current valid passport or, where a customer does not own 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.

3. A Relevant Person should, in complying with Rule 7.3.1(1)(a), and adopting the RBA, obtain, verify and record, for every customer which is a legal person, the following identification information:

a. full business name and any trading name;

b. registered or business address;

c. date of incorporation or registration;

d. place of incorporation or registration;

e. a valid commercial or professional licence;

f. the identity of the directors, partners, trustees or equivalent persons with executive authority of the legal person; and

g. for a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust and documentary evidence of the appointment of the current trustees.

4. In complying with Rule 7.3.1(1)(a), 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(1)(a). 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.

5. For higher risk situations the DFSA would expect identification information to be independently verified, using both public and non-public sources. For lower risk situations, not all of the relevant identification information would need to be verified.

6. In complying with Rule 7.3.1(1) (b) and (c), a Relevant Person is required to "understand" a customer's source of funds and wealth. This would mean obtaining information from the customer or from a publicly-available source on the source of funds and wealth. For a public company, this might be achieved by looking at their published accounts. For a natural or legal person, this might involve including a question on source of funds and wealth in an application form or client questionnaire. Understanding a customer's source of funds and wealth is also important for the purposes of undertaking ongoing due diligence under Rule 7.3.1(1)(d).

7. An insurance policy which is similar to a life policy would include life-related protection, or a pension, or investment product which pays out to the policy holder or beneficiary upon a particular event occurring or upon redemption.

Guidance on verification of beneficial owner

8. In determining whether an individual meets the definition of a beneficial owner or controller, 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 "small" ownership interest for the purposes of the definition of a beneficial owner will depend on the individual circumstances of the customer. The DFSA considers that the question of whether an ownership interest is small 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.

9. When verifying beneficial owners under Rule 7.3.1(1)(a), 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.

10. 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.

11. 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.

12. Where a Relevant Person carries out identification and verification in respect of actual and potential beneficial owners of a trust, this should include the trustee, settlor, the protector, the enforcer, beneficiaries, other persons with power to appoint or remove a trustee and any person entitled to receive a distribution, whether or not such person is a named beneficiary.

Guidance on politically exposed persons

13. 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. It does, however, put the customer into a higher risk category.

14. 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.

15. 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 Law No. 4 of 2002. 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.

16. 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.

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) verify information on:

(i) the customer's source of funds;

(ii) the customer's source of wealth;

(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; and

(e) obtain the approval of senior management to commence 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 a Prescribed Low Risk Customer of type (a), (c) or (d).

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 or by a committee of senior managers appointed to consider high risk customers. It may also be outsourced within the Group.

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, where there is a beneficial owner, verification of 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.

6. The DFSA considers that verification of 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.

7. 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.

8. 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.

9. 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 Prescribed Low Risk Customer of type (a), (c) or (d) 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 (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 a beneficial owner;

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

(e) not enquiring as to a customer's source of funds or source of wealth;

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

(g) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but infering 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. For example, for customers where the money laundering risks are very low, a Relevant Person may decide to simply identify the customer and verify such information only to the extent that this is commercially necessary. On the other hand, a low risk customer which is undertaking a complex transaction might require more comprehensive Simplified CDD.

3. 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.

4. 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.

7.6 Ongoing customer due diligence

7.6.1 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) periodically 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) periodically 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.

Guidance

1. In complying with Rule 7.6.1(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 (d) and (e) particularly 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.

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(d).

Guidance

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

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 Article 16 of the Federal Law No. 4 of 2002; or

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

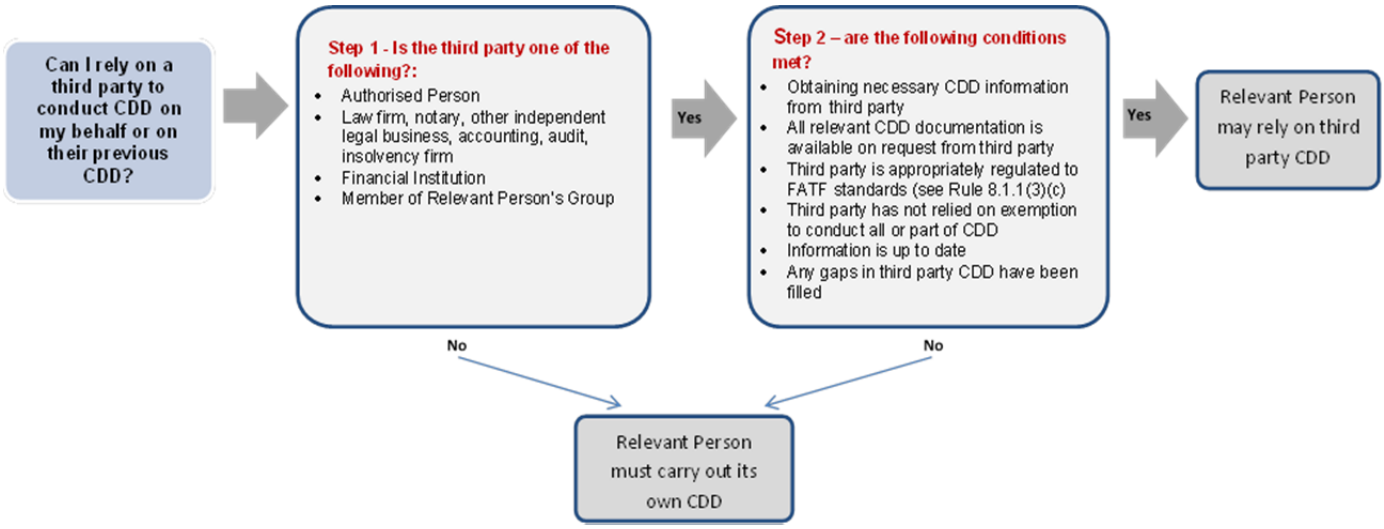
Guidance

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) the person in (1)(b) to (d) is subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;

(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 and record keeping which is equivalent to the standards set by FATF; and

(b) where the effective implementation of those Customer Due Diligence and record keeping requirements and AML programmes are supervised at Group level by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to 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.

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. However, compliance can be achieved by having the information sent in an email or other appropriate means. For the avoidance of doubt, it does not necessarily require a Relevant Person to immediately obtain the underlying certified documents used by the third party to undertake its CDD because under Rule 8.1.1(3)(b), these need only be available on request without delay.

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.

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.

9 CORRESPONDENT BANKING, WIRE TRANSFERS, ANONYMOUS ACCOUNTS AND AUDIT

9.1 Application

9.1.1 This chapter applies only to an Authorised Person other than a Representative Office.

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

A shell bank would be a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated 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.

9.3 Wire transfers

9.3.1 In this section:

(a) "beneficiary" means the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer;

(b) "originator" means the account holder who instructs the wire transfer from the relevant account, or where there is no account, the natural or legal person that places the order with the ordering Financial Institution to perform the wire transfer; and

(c) "wire transfer" includes any value transfer arrangement.

9.3.2 (1) An Authorised Person must:

(a) when it sends or receives funds by wire transfer on behalf of a customer, ensure that the wire transfer and any related messages contain accurate originator and beneficiary information;

(b) ensure that, while the wire transfer is under its control, the information in (a) remains with the wire transfer and any related message throughout the payment chain; and

(c) monitor wire transfers for the purpose of detecting those wire transfers that do not contain originator and beneficiary information and take appropriate measures to identify any money laundering risks.

(2) The requirement in (1) does not apply to an Authorised Person which transfers funds to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

(3) An Authorised Person must ensure that information accompanying all wire transfers contains at a minimum:

(a) the name of the originator;

(b) the originator account number where such an account is used to process the transaction;

(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the transaction.

Guidance

1. In the absence of an account number, a unique transaction reference number should be included which permits traceability of the transaction.

2. The DFSA considers that concealing or removing in a wire transfer any of the information required by Rule 9.3.2(3) would be a breach of the requirement to ensure that the wire transfer contains accurate originator and beneficiary information.

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.

9.5 Anonymous and nominee accounts

9.5.1 An Authorised Person must not establish or maintain:

(a) an anonymous account or an account in a fictitious name; or

(b) 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 Authorised Person.

10 SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

10.1 Application

10.1.1 This chapter does not apply to a person meeting part (1) (b) or (c) of the definition of a DNFBP.

10.2 Relevant United Nations resolutions and sanctions

10.2.1 (1) A Relevant Person must establish and maintain effective systems and controls to obtain and make appropriate use of relevant resolutions or sanctions issued by the United Nations Security Council.

(2) A Relevant Person must immediately notify the DFSA when it becomes aware that it is:

(a) carrying on or about to carry on an activity;

(b) holding or about to hold money or other assets; or

(c) undertaking or about to undertake any other business whether or not arising from or in connection with (a) or (b);

for or on behalf of a person, where such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the United Nations Security Council.

(3) A Relevant Person must ensure that the notification stipulated in (2) above includes the following information:

(a) a description of the relevant activity in (2) (a), (b) or (c); and

(b) the action proposed to be taken or that has been taken by the Relevant Person with regard to the matters specified in the notification.

Guidance

1. In relation to the term "make appropriate use" in Rule 10.2.1, this 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 a person.

2. Relevant 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.

10.3 Government, regulatory and international findings

10.3.1 (1) A Relevant Person must establish and maintain systems and controls to obtain and make appropriate use of any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions 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. or the AMLSCU;

(c) FATF;

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

(e) 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, including any assessment of material deficiency against relevant countries in adopting international standards; and

(b) 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.

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. A Relevant Person should examine and pay special attention to any transactions or business relationship with persons located in countries or jurisdictions mentioned by the persons in Rule 10.3.1(a) to (e).

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.

4. The Relevant Person's MLRO is not obliged to report all transactions from these countries or jurisdictions to the AMLSCU if they do not qualify as suspicious under Federal Law No. 4 of 2002. 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 financial sanctions in the European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Assets Control (OFAC) of the United States Department of Treasury.

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 relation to the term "make appropriate use" in Rule 10.3.1, this 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. The DFSA encourages Relevant Persons to perform checks against their customer databases and records for any names appearing on such lists and databases as well as to monitor transactions accordingly.

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

11.1.1 This chapter does not apply to a person meeting part (1) (b) or (c) of the definition of a DNFBP.

11.2 Appointment of a MLRO

11.2.1 (1) A Relevant Person must appoint an individual as MLRO, with responsibility for implementation and oversight of its compliance with the Rules in this module, who has an appropriate level of seniority and independence to act in the role.

(2) The MLRO in (1) and Rule 11.2.5 must be resident in the U.A.E.

11.2.2 The individual appointed as the MLRO of a Representative Office must be the same individual who holds the position of Principal Representative of that 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.

11.2.3 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 has:

(a) direct access to its senior management;

(b) 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;

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

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

Guidance

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.

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, in accordance with Federal Law No. 4 of 2002, Suspicious Activity Reports;

(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 Law No. 4 of 2002, Federal Law No. 1 of 2004 and any other relevant Federal laws;

(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 In this chapter, a person meeting part (1) (b) or (c) of the definition of a DNFBP is only required to comply with Rule 13.3.4 and section 13.4.

13.1.2 In this chapter:

(a) "money laundering" means the criminal offence defined in Federal Law No 4 of 2002; and

(b) "terrorist financing" means the criminal offence defined in Federal Law No 1 of 2004.

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's refusal 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) investigates 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 Law No. 4 of 2002 a Suspicious Activity Report must be made to the AMLSCU and documents such determination;

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

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

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.

13.3.4 When a person meeting part (1) (b) or (c) of the definition of a DNFBP 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, it must make a Suspicious Activity Report to the AMLSCU as soon as practicable and notify the DFSA of the making of such report immediately following its submission to the AMLSCU.

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 U.A.E.

2. SARs under Federal Law No. 4 of 2002 should be emailed or faxed to the AMLSCU. The dedicated email address and fax numbers, and the template for making a SAR are available on the DFSA website.

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 AMLSCU, the AMLSCU 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 AMLSCU on how to proceed, the Relevant Person should immediately contact the AMLSCU for further instructions.

13.4 Tipping-off

Guidance

1. Relevant Persons are reminded that in accordance with Article 16 of the Federal Law No. 4 of 2002, Relevant Persons or any of their Employees must not tip-off any person, that is, inform any person that he is being scrutinised for possible involvement in suspicious activity related to money laundering, or that any other competent authority is investigating his possible involvement in suspicious activity relating to money laundering.

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.

14 GENERAL OBLIGATIONS

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) The requirement in (1) does not apply if the Relevant Person can satisfy the DFSA that the relevant branch, Subsidiary or Group entity is subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance with such regulations.

(3) Where the law of another jurisdiction does not permit the implementation of policies, procedures, systems and controls consistent with those of the Relevant Person, 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) understands the policies and procedures covering the sharing of information between Group entities, particularly when sharing Customer Due Diligence information;

(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 any a significant breach of a Rule in this module or breach of Federal Law No. 4 of 2002 or Federal Law No. 1 of 2004 by the Relevant Person or any of its Employees.

14.4 Record keeping

14.4.1 A Relevant Person must, where relevant, maintain the following records:

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

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

(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 AMLSCU; and

(f) the documents in Rule 14.4.2,

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.

14.4.2 A Relevant Person must document, and provide to the DFSA 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, within an appropriate time, any regulatory enquiry or court order to disclose information.

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 available for inspection within a reasonable period of time.

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 which is:

(a) an Authorised Person;

(b) a real estate developer or agency;

(c) a law firm, notary firm, or other independent legal business;

(d) an accounting firm, audit firm or insolvency firm; or

(e) a company service provider,

must complete the AML Return form in AFN on an annual basis and submit such form to the DFSA within four 4 months of its financial year end.

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 AMLSCU or another financial intelligence unit, the police, or a Dubai or Federal ministry.

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 2004. The Regulatory Law 2004 gives the DFSA a power to supervise DNFBPs', compliance with relevant AML laws in the U.A.E. It 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 2004. The DFSA may also impose fines for breaches of the Law or the Rules.

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 2004 and outlines its policy for using these powers.

15.1 Registration and notifications

15.1.1 A DNFBP must register with the DFSA by way of a notification by completing and submitting the appropriate form in the AFN Sourcebook.

15.1.2 A DNFBP must promptly notify the DFSA of any change in its:

(a) name;

(b) legal status;

(c) address; or

(d) if applicable, its MLRO.

15.2 Withdrawal of registration

15.2.1 A DNFBP must notify the DFSA in writing when it proposes to cease carrying on its business activities in or from the DIFC.

15.2.2 A DNFBP which proposes to cancel its registration as a DNFBP must provide the DFSA with 14 days' written notice of such cancellation and provide written evidence of the basis of its withdrawal.

15.2.3 The DFSA may cancel the registration of a DNFBP:

(a) if the DNFBP notifies the DFSA of the cancellation in accordance with Rule 15.2.2;

(b) if the DNFBP's commercial licence is cancelled or expires and a reasonable time has passed without such licence being renewed;

(c) following a request by the ROC;

(d) in the event of the insolvency or the entering into administration of the DNFBP; or

(e) if the DFSA considers it necessary or desirable in the interests of the DIFC.

15.2.4 (1) The DFSA may only cancel the registration of a DNFBP under Rule 15.2.3 (b) to (e) if it has given the person an opportunity to make representations in relation to the proposed cancellation.

(2) If the DFSA cancels the registration of a DNFBP under Rule 15.2.3, the DFSA shall without delay inform the DNFBP in writing of:

(a) such decision;

(b) the reasons for the decision; and

(c) the date on which the decision shall be deemed to take effect.

15.2.5 A DNFBP may appeal to the DFSA's Regulatory Appeals Committee against any decision of the DFSA to cancel its registration under Rule 15.2.3 (b) to (e).

Guidance

1. A DNFBP may request a cancellation 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. The DFSA would expect to use the power to cancel the registration of a DNFBP under Rule 15.2.3(e) once its supervisory tools have been exhausted. Examples of when it might use this power include where a DNFBP commits serious or persistent breaches of the AML Rules which it fails to rectify, or where the DNFBP or its activities in or from the DIFC create risks to the DFSA's regulatory objectives.

3. Under Article 28 of the Regulatory Law, a person wishing to appeal to the Regulatory Appeals Committee a decision of the DFSA must submit a written notice of appeal within 30 days of the notification of the relevant decision. The form of submission that an appeal must take is specified in the rules of procedures of the Regulatory Appeals Committee. Information on the DFSA's Regulatory Appeals Committee can be found on the DFSA website.

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.

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 the date on which the Rules in this module came into force;

(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.