FINANCIAL SERVICES REGULATORY AUTHORITY
سلطة تنظيم الخدمات المالية

Anti-Money Laundering and Sanctions Rules and Guidance (AML)

ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

TABLE OF CONTENTS

The contents of the AML Rulebook are divided into the following Chapters and sections:

1. INTRODUCTION 1

1.1 Jurisdiction 1
1.2 Application 1
1.3 Responsibility for compliance with the AML Rulebook 2
1.4 Application table 3

2. OVERVIEW AND PURPOSE OF THE AML RULEBOOK 4

3. INTERPRETATION AND TERMINOLOGY 7

3.1 Interpretation 7
3.2 Glossary for AML 7

4. GENERAL COMPLIANCE REQUIREMENTS 8

4.1 General requirements 8
4.2 Co-operation with regulators 9

5. APPLYING A RISK-BASED APPROACH TO AML 10

5.1 The risk-based approach 10

6. BUSINESS RISK ASSESSMENT 11

6.1 Assessing business AML risks 11
6.2 AML systems and controls 12

7. CUSTOMER RISK ASSESSMENT 14

7.1 Customer risk-based assessment 14
7.2 Assessing Customer AML risks 15

8. CUSTOMER DUE DILIGENCE 20

8.1 Requirement to undertake Customer Due Diligence 20
8.2 Timing of Customer Due Diligence 23
8.3 Customer Due Diligence requirements 25

8.4 Enhanced Customer Due Diligence 38
8.5 Simplified Customer Due Diligence 40
8.6 On-going Customer Due Diligence 41
8.7 Failure to conduct or complete Customer Due Diligence 42

9. RELIANCE AND OUTSOURCING OF AML COMPLIANCE 44

9.1 Reliance on a third party 44
9.2 Business partner identification 45
9.3 Outsourcing 48
9.4 Record Keeping and Data Protection 48

10. CORRESPONDENT BANKING, WIRE TRANSFERS, ANONYMOUS ACCOUNTS AND AUDIT 50

10.1 Application 50
10.2 Correspondent banking 50
10.3 Wire transfers 51
10.4 Audit 52
10.5 Anonymous and nominee accounts 53

11. SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS 54

11.1 Sanctions and Other International Obligations 54
11.2 Government, regulatory and international findings 55

12. MONEY LAUNDERING REPORTING OFFICER 57

12.1 Appointment of a MLRO 57
12.2 Qualities of a MLRO 58
12.3 Responsibilities of a MLRO 58
12.4 Reporting 59

13. AML TRAINING AND AWARENESS 61

13.1 Training and awareness 61
13.2 Frequency 62
13.3 Record-keeping 62

14. SUSPICIOUS ACTIVITY REPORTS 63

14.1 Application and definitions 63
14.2 Internal reporting requirements 63
14.3 External Suspicious Activity Report 65
14.4 Suspension of Transaction and No Tipping-off Requirement 66
14.5 Record-keeping 66

15. GENERAL OBLIGATIONS 67

15.1 Groups, Branches and subsidiaries 67
15.2 Group policies 67
15.3 Notifications 68
15.4 Record keeping 69
15.5 Annual AML Return 71
15.6 Communication with the Regulator 71
15.7 Employee disclosures 71

1. INTRODUCTION

1.1 Jurisdiction

1.1.1 (1) The AML Rulebook is made in recognition of the application in the Abu Dhabi Global Market ("**ADGM**") of Federal Law No. 4 of 2002 regarding 'Criminalisation of Money Laundering', Federal Decree Law No. 1 of 2004 regarding 'Combating Terrorism Offences', and Federal Law No. 7 of 2014 regarding 'Combating Terrorist Crimes'.

(2) A reference in the AML Rulebook to money laundering is to be taken to include terrorist financing unless the context otherwise provides.

(3) Nothing in the AML Rulebook affects the operation of:

(a) Federal Law No. 4 of 2002 regarding 'Criminalisation of Money Laundering';

(b) Federal Law No. 1 of 2004 regarding 'Combating Terrorism Offences';

(c) Federal Law No. 7 of 2014 regarding 'Combating Terrorist Crimes';

(d) the Penal Code of the United Arab Emirates; or

(e) any other Federal Law that is applicable in the Abu Dhabi Global Market in relation to money laundering.

1.2 Application

1.2.1 (1) The AML Rulebook applies to:

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

(b) the Persons specified in Rule 1.3.3 as being responsible for a Relevant Person's compliance with the AML Rulebook,

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 7 to 9 of the AML Rulebook 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.

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

(a) an Authorised Person;

(b) a Recognised Body; or

(c) any Licensed Person who is not an Authorised Person or Recognised Body and who falls within any of the categories of business in Rule 1.2.3.

1.2.3 A Person falls within this Rule if it carries on any of the following business:

(1) A real estate developer or agency which carries out Transactions with a Customer involving the buying or selling of real property;

(2) A dealer in precious stones or precious metals;

(3) A dealer in any saleable item of a price equal to or greater than USD 15,000;

(4) A law firm, notary firm or other independent legal business;

(5) An accounting firm, audit firm or insolvency firm; or

(6) A Company Service Provider.

1.3 Responsibility for compliance with the AML Rulebook

1.3.1 A Relevant Person's Governing Body is responsible for establishing, maintaining and monitoring the Relevant Person's AML policies, procedures, systems and controls and compliance with applicable AML legislation.

1.3.2 A Relevant Person's Governing Body must ensure the policies, procedures, systems and controls referred to in Rule 1.3.1 are effective to meet the obligations of the Relevant Person.

1.3.3 (1) Responsibility for a Relevant Person's compliance with the AML Rulebook lies with every member of the Governing Body and its Senior Management unless a senior officer is acting as the Money Laundering Reporting Officer ("**MLRO**") of the Relevant Person in his/her capacity as a Recognised Person.

(2) In carrying out their responsibilities under the AML Rulebook every member of a Relevant Person's Governing Body and its Senior Management or the MLRO (as the case may be) must exercise due skill, care and diligence.

(3) Nothing in this Rule precludes the Regulator 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 the AML Rulebook:

(a) a Relevant Person;

(b) members of a Relevant Person's Senior Management; or

(c) an Employee of a Relevant Person.

1.4 Application table

Guidance

- Partially applicable. Relevant Persons should consider these Chapters and determine which provisions apply.

Relevant Person	Applicable Chapters			
Authorised Person and Recognised Body	1 - 15			
Representative Office	1 - 6	11 - 15		
Real estate developer or agency	1 - 9	11 - 15		
Law firm, notary firm, or other independent legal business	1 - 9	11 - 15		
Accounting firm, audit firm or insolvency firm	1 - 9	11 - 15		
Company service provider	1 - 9	11 - 15		
Dealer in precious metals or precious stones	1 - 9	13	14*	15
Dealer in high-value goods	1 - 9	13	14*	15

2. OVERVIEW AND PURPOSE OF THE AML RULEBOOK

Guidance

1. The AML Rulebook has been designed to provide a single reference point for all Persons and entities (collectively called "**Relevant Persons**") who are supervised by the Regulator for Anti-Money Laundering and Sanctions compliance. Accordingly it applies to Relevant Persons, but in different degrees as provided in Rule 1.4. The AML Rulebook takes into consideration the fact that Relevant Persons have differing AML risk profiles. A Relevant Person should familiarise itself with the AML Rulebook, and assess the extent to which the Chapters and sections apply to it.

2. The AML Rulebook is not intended to 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 ("**UNSC**") Resolutions which apply in the ADGM, and 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 the AML Rulebook contains an application table which should assist a Relevant Person to navigate through the AML Rulebook and to determine which Chapters are applicable to it. Chapter 1 also specifies who is ultimately responsible for a Relevant Person's compliance with AML. The Regulator expects the Senior Management of a Relevant Person to establish a robust and effective AML and Sanctions compliance culture for the business.

4. Chapter 2 provides an overview of the AML Rulebook and Chapter 3 sets out the key definitions in the AML Rulebook. Note that not all definitions used in the AML Rulebook are capitalised.

5. Chapter 4 outlines the general compliance requirements.

6. Chapter 5 explains the meaning of the risk-based approach ("**RBA**"), which should be applied when complying with the AML Rulebook. The RBA requires a risk-based assessment of a Relevant Person's business (in Chapter 6) and its Customers (in Chapter 7). 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 Rulebook 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 Regulator expects the RBA to determine the breadth and depth of the Customer Due Diligence ("**CDD**") which is undertaken for a particular Customer under Chapter 8, though the Regulator understands that there is an inevitable overlap between the risk-based assessment of the Customer in Chapter 7 and CDD in Chapter 8. This overlap may occur at the initial stages of Client on-boarding but may also occur when undertaking on-going CDD.

7. Chapter 9 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 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.

8. Chapter 10 sets out certain obligations in relation to correspondent banking, wire transfers and other matters which are limited to Authorised Persons and Recognised Bodies, and, in particular, to banks.

9. Chapter 11 sets out a Relevant Person's obligations in relation to UNSC resolutions and Sanctions, and government, regulatory and international findings (in relation to AML, terrorist financing and the financing of weapons of mass destruction).

10. Chapter 12 sets out the obligation for a Relevant Person to appoint an MLRO and the responsibilities of such a Person.

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

12. Chapter 14 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.

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

The U.A.E. criminal law

14. Under section 7(6) of the Financial Services and Markets Regulations 2015 (the "**FSMR**"), the Regulator has jurisdiction for the regulation of AML in the ADGM. The AML Rulebook sets out the requirements imposed by the Regulator under section 7(6) of the FSMR. The U.A.E. criminal law applies in the ADGM and, therefore, Persons in the ADGM 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, Federal Law No. 7 of 2014, and the Penal Code of the United Arab Emirates. The Rules in the AML Rulebook 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 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 Standards

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 Regulator 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 the AML Rulebook, 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.

Basel Committee Standards

19. The Basel Committee on Banking Supervision has published a set of guidelines for banks (Sound Management of Risks related to Money Laundering and Financing of Terrorism, January 2014) which are intended to supplement FATF Recommendations. Banks operating in ADGM should read the Basel Committee guidelines in conjunction with FATF Recommendations and in complying with these Rules.

20. In the event that any of the Basel Committee guidelines conflict with a Rule in the AML Rulebook, the relevant Rule takes precedence.

Sanctions

21. The U.A.E., as a member of the United Nations, is required to comply with Sanctions issued and passed by the UNSC. These UNSC obligations apply in the ADGM and their importance is emphasised by specific obligations contained in the AML Rulebook requiring Relevant Persons to establish and maintain effective systems and controls to make appropriate use of UNSC Sanctions and resolutions (see Chapter 11).

22. 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.

23. 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 ("**OFAC**")), the Regulator 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 the AML Rulebook to "money laundering" in lower case includes a reference to terrorist financing unless the context provides or implies otherwise.

3.2 Glossary for AML

Guidance

The defined terms and abbreviations in the AML Rulebook can be found in the Regulator's Glossary Rulebook ("**GLO**").

4. GENERAL COMPLIANCE REQUIREMENTS

4.1 General requirements

4.1.1 (1) A Relevant Person must establish and maintain effective AML policies, procedures, systems and controls to prevent opportunities for Money Laundering, in relation to the Relevant Person and its activities.

(2) A Relevant Person's AML policies, procedures, systems and controls should:

(a) ensure compliance with U.A.E. Law No. 4 of 2002, U.A.E. Law No. 1 of 2004, Federal Law No. 7 of 2014, and any other relevant federal laws of the U.A.E. relating to Money Laundering;

(b) enable suspicious Customers and Transactions to be detected and reported;

(c) ensure the Relevant Person is able to provide an appropriate audit trail of a Transaction; and

(d) ensure compliance with any other obligation in these Rules.

(3) A Relevant Person must take reasonable steps to ensure that its Employees comply with the relevant requirements of its AML policies, procedures, systems and controls.

(4) A Relevant Person must review the effectiveness of its AML policies, procedures, systems and controls at least annually.

(5) The review process may be undertaken:

(a) internally by its internal audit or compliance function; or

(b) by a competent firm of independent auditors or compliance professionals.

(6) The review process required under Rule 4.1.1(4) must cover at least the following:

(a) a sample testing of "Know Your Customer" arrangements;

(b) an analysis of all Suspicious Activity Reports 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 Governing Body or Senior Management with the MLRO to ensure that their responsibility for implementing and maintaining adequate controls is satisfactory.

4.1.2 A Relevant Person which is a Domestic Firm must ensure that its AML policies, procedures, systems and controls apply to any Branch or Subsidiary operating in another jurisdiction.

4.1.3 If another jurisdiction's laws or regulations prevent or inhibit a Relevant Person from complying with U.A.E. Law No. 4 of 2002, U.A.E. Law No. 1 of 2004 or with these Rules, the Relevant Person must promptly inform the Regulator in writing.

4.2 Co-operation with regulators

4.2.1 A Relevant Person that receives a request for information from a Non-ADGM Financial Services Regulator or agency responsible for AML regarding enquiries into potential Money Laundering related to Regulated Activities carried on in or from the ADGM, must promptly inform the Regulator in writing.

5. APPLYING A RISK-BASED APPROACH TO AML

5.1 The risk-based approach

5.1.1 A Relevant Person must:

(a) assess and address its AML risks under the AML Rulebook 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 the AML Rulebook, 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 5.1.1 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 in A1.1. The Regulator 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 the AML Rulebook are in Rule 15.4. These Rules apply in relation to Rule 5.1.1(b)(iii).

5.1.2 A flowchart outlining the RBA standards and their application is contained in A1.1.

6. BUSINESS RISK ASSESSMENT

6.1 Assessing business AML risks

6.1.1 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; and

(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.

6.1.2 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 as required by Rule 6.2.1;

(b) ensure that its AML policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 6.1.1;

(c) assess the effectiveness of its AML policies, procedures, systems and controls as required by Rule 6.2.1(c);

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

(e) assist in the carrying out of the Customer risk assessment under Chapter 7.

Guidance

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

2. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its Customers under Chapter 7. 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.

6.2 AML systems and controls

6.2.1 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 ("**PEP**");

(iii) enable the Relevant Person to comply with these Rules, Federal Law No. 4 of 2002, Federal Law No. 1 of 2004, Federal Law No. 7 of 2014, and any other relevant Federal laws; and

(iv) the Penal Code of the United Arab Emirates; 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 6.2.1(c) the regularity of risk assessments will depend on the nature, size and complexity of the Relevant Person's business.

6.3 A flowchart outlining the business risk-based assessment process is contained in A1.2.

7. CUSTOMER RISK ASSESSMENT

7.1 Customer risk-based assessment

7.1.1 Generally, a Relevant Person is expected to take a risk-based approach when assessing any business relationship or Transaction with respect to its specific money laundering risk and the information and evidence that might be required or validated for this purpose. "Know Your Customer" procedures need to be established and managed according to the perceived money laundering risk.

7.1.2 (1) The Relevant Person should take specific and adequate measures necessary to compensate for the higher risk of money laundering which might arise, for example from the following products, services or Customers:

(a) non-face-to-face business relationships or Transactions, such as via mail, telephone or the internet;

(b) internet-based products;

(c) electronic money products;

(d) correspondent banking relationships;

(e) Customers from higher-risk countries; and

(f) PEPs.

(2) A Relevant Person should apply an intensified monitoring of Transactions and accounts in relation to these products, services and Customers.

7.1.3 While a Relevant Person should assess the money laundering risks posed by the products and services it offers and devise its products with due regard to those risks, an RBA does not release the Relevant Person from its overall obligation to comply with AML obligations.

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 8. Chapter 8 prescribes the requirements of CDD and of Enhanced Customer Due Diligence for high-risk Customers and Simplified Customer Due Diligence 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 on-going CDD requirements in Rule 8.6.1 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 Regulator 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.

7.2 Assessing Customer AML risks

7.2.1 (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 CDD 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), including its possible status as a Politically Exposed Person;

(d) take into consideration the nature of the Customer's 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 6.

7.2.2 A Relevant Person must not establish a business relationship with a 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 Customer 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 in A1.3, requires a Relevant Person to allocate an appropriate risk rating to every Customer. The Regulator 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 7.2.2, 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.

6. The geographical location of a Relevant Person's Customer may also affect the money laundering risk assessment. The Regulator recommends that where a Relevant Person has Customers located in countries:

   a. without adequate AML strategies;

   b. where cash is the normal medium of exchange;

c. which have a politically unstable regime with high levels of public or private sector corruption;

d. which are known to be drug producing or drug transit countries; or

e. which have been classified as countries with inadequacies in their AML regulations,

it should consider which additional "Know Your Customer" and monitoring procedures might be necessary to compensate for the enhanced risks of money laundering.

7. Such measures may encompass, for example, the following:

a. requiring additional documentary evidence;

b. taking supplementary measures to verify or certify the documents supplied;

c. requiring that the initial Transaction is carried out through an account opened in the Customer's name with a Financial Institution subject to AML or regulated in a FATF country;

d. performing direct mailing of account opening documentation to a Customer at an independently verified address; or

e. establishing telephone contact with a Customer prior to opening the account.

8. A Relevant Person should be able to aggregate and monitor significant balances and activity in accounts on a consolidated basis when Customers have multiple accounts with the same institution but in offices located in different countries.

Guidance on the term "Customer"

9. The point at which a Person becomes a Customer will vary from business to business. However, the Regulator 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.

10. The Regulator 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).

11. The Regulator considers that a counterparty would generally be a "Customer" for the purposes of the AML Rulebook 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.

12. A Representative Office should not have any Customers in relation to its ADGM operations.

Guidance on Restricted Scope Companies

13. The Restricted Scope Company is a corporate vehicle offering a greater degree of confidentiality than other forms of corporate entity in ADGM. Restricted Scope Companies are not required to file accounts and are not required to audit their accounts. Restricted Scope Companies must file an annual return, articles, and details of their registered offices, directors and secretary (if they have one) with the Registrar.

14. Relevant Persons will know that the Restricted Scope Company is subject to less onerous corporate disclosure requirements than other forms of corporate entity due to the requirement to have "(Restricted)" in the company's name. Given that only a Restricted Scope Company's constitution and details of its registered office will be available in a public register, Relevant Persons will be required to have a bilateral dialogue with the Restricted Scope Company in accordance with the RBA to obtain any other relevant information which is needed to assess the money laundering risks to which it is exposed.

15. Restricted Scope Companies should be forthcoming with regards to requests for information by other Persons and entities for the purpose of their compliance with AML. In such cases, Restricted Scope Companies should not have difficulty in establishing business relationships with other Persons and entities in ADGM. The fact that Restricted Scope Companies are not subject to strict standards of disclosure of corporate documentation to a public registry should not be interpreted by Restricted Scope Companies to prohibit their providing of any relevant information for AML purposes.

Guidance on high-risk Customers

16. In complying with Rule 7.2.1, the Regulator 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 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 unassociated third parties;

n. discretionary trusts; and

o. charitable trusts and waqfs.

17. The highest risk products or services in respect of money laundering are those where unlimited third party funds can be freely received, or where funds can regularly be paid to third parties, without evidence of the identity of the third parties being taken.

18. Money laundering risks are increased if a Person is able to hide behind corporate structures such as limited companies, trusts, special purpose vehicles and nominee arrangements. When devising its internal procedures, a Relevant Person should consider how its Customers and operational systems impact upon the capacity of its staff to identify suspicious Transactions. Generally, the lowest risk products in respect of money laundering are those where funds can only be received from a named Customer by way of payment from an account held in the Customer's name, and where the funds can only be returned to the named Customer.

7.3 A flowchart outlining the customer risk-based assessment process is contained in A1.3.

8. CUSTOMER DUE DILIGENCE

8.1 Requirement to undertake Customer Due Diligence

8.1.1 (1) A Relevant Person must:

(a) undertake CDD under Rule 8.3.1 for each of its Customers (including those it has assigned as low-risk) with or for whom the Relevant Person acts or proposes to act; and

(b) in addition to (a), undertake Enhanced Customer Due Diligence under Rule 8.4.1 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 8.5.1 by modifying CDD under Rule 8.3.1 for any Customer falling within the following categories:

(a) Authorised Person;

(b) Recognised Body;

(c) a Credit Institution; or

(d) other Financial Institution (including publically listed companies in or outside of ADGM) covered by equivalent identification requirements as set out in Guidance 4 below.

8.1.2 (1) The obligations must, subject to Rule 8.1.2(3), be fulfilled before the Relevant Person effects any Transaction on behalf of the Customer.

(2) It is a Relevant Person's responsibility when it next has contact with a Customer who was an existing Customer, prior to the Relevant Person's authorisation by the Regulator, to assess whether it has performed the identification of that Customer which would have been required had these Rules been applicable when the Customer became a Customer, and to obtain without delay any missing information or evidence about the true identity of all relevant parties.

(3) A Relevant Person does not have to fulfil the obligations under Rules 8.1.2(1) and 8.1.2(2) before effecting a Transaction for a Customer where it has, on reasonable grounds, established that:

(a) following a preliminary risk assessment, the proposed Transaction presents a low-risk in relation to Money Laundering and terrorist financing;

(b) doing so would interrupt or delay the normal course of business in respect of effecting the Transaction; and

(c) the Transaction is in respect of electronic money, Investment Business or Insurance Business.

(4) Where the Relevant Person is unable to establish and verify the identity of the Customer referred to in Rule 8.1.2(3) including, where applicable, any beneficiaries, Beneficial Owners or trustees, within the 30 days following receipt of the Customer's instruction, it must:

(a) consider the circumstances and determine whether to make an internal Suspicious Activity Report to the MLRO;

(b) where it has determined that it is unnecessary to make such a report, return to the Customer any monies associated with the Transaction, excluding any reasonable costs incurred by the Relevant Person;

(c) where it has determined to make such a report, not return any monies or provide any Investments to the Customer, unless instructed to do so by the MLRO and otherwise act in accordance with instructions issued by the MLRO; and

(d) not establish any further business relationship with that Customer until the verification process has been completed for that Customer in accordance with these Rules.

8.1.3 (1) A Relevant Person must:

(a) undertake periodic reviews to ensure that the information and documentation concerning a Customer's identity remains appropriate, accurate and up-to-date; and

(b) conduct on-going due diligence on its business relationship with, and on-going scrutiny of Transactions undertaken by, a Customer throughout the course of the relationship.

(2) If, at any time, a Relevant Person becomes aware that it lacks sufficient information or documentation concerning a Customer's identification, or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify the Customer's identity.

Guidance

1. A Relevant Person should undertake CDD in a manner proportionate to the Customer's money laundering risks identified under Rule 7.2.1(1). This means that all Customers are subject to CDD under Rule 8.3.1. However, for high-risk Customers, additional Enhanced Customer Due Diligence measures should also be undertaken under Rule 8.4.1. For low-risk Customers, Rule 8.3.1 may be modified according to the risks in accordance with Rule 8.5.1.

2. Subject to the exception for Simplified Customer Due Diligence, in establishing and verifying a Customer's true identity, a Relevant Person must obtain sufficient and satisfactory evidence of that identity, having considered its risk assessment in respect of the Customer and a Relevant Person must update, as appropriate, any Customer identification policies, procedures, systems and controls.

3. Subject to the exception for Simplified Customer Due Diligence, whenever a Relevant Person comes into contact with a Customer with or for whom it acts or proposes to act, it must establish whether the Customer is acting on his own behalf or on behalf of another Person, and a Relevant Person must establish and verify the identity of both the Customer and any other Person on whose behalf the Customer is acting, including that of the Beneficial Owner of the relevant funds, which may be the subject of a Transaction to be considered, and must obtain sufficient and satisfactory evidence of their identities. A Relevant Person should obtain a statement from a prospective Customer to the effect that he is, or is not, acting on his own behalf. In cases where the Customer is acting on behalf of third parties, it is recommended that the Relevant Person obtain a written statement, confirming the statement made by the Customer, from the parties, including the Beneficial Owner.

4. An institution falls within Rule 8.1.1(2)(c) if it is:

   a. a Credit Institution or other Financial Institution whose entire operations are subject to regulation, including AML, by:

      i. a Non-ADGM Financial Services Regulator in a FATF country; or

      ii. another relevant authority in a FATF country; or

      iii. is publically listed in or outside of ADGM; or

   b. a Subsidiary of a Credit Institution or other Financial Institution referred to in a., provided that the Parent Credit Institution or other Financial Institution ensures that the Subsidiary also observes the same provisions.

5. A Relevant Person must take reasonable steps to determine whether or not a Customer falls within the exceptions under Rule 8.1.2(3), and, if applicable, must keep records of the basis on which a Customer was considered to fall within an exception.

6. A Relevant Person is required to be satisfied that a prospective Customer is who he claims to be and to obtain evidence to prove this. "Know Your Customer" and knowing the Persons with or for whom the Customer acts or proposes to act, consists of several aspects:

   a. personal details: a Relevant Person should obtain and verify details which include the true full name or names used and the current permanent address;

   b. the nature and level of business to be conducted: a Relevant Person should ensure that sufficient information is obtained regarding the nature of the business that the Customer expects to undertake, and any expected or predictable pattern of Transactions. This information should include the purpose and reason for opening the account or establishing the business relationship, the anticipated level and nature of the activity that is to be undertaken and the various relationships of signatories to the account and the underlying Beneficial Owners;

   c. the origin of funds: a Relevant Person should identify how all payments were made, from where and by whom. All payments should be recorded to provide an audit trail; and

d. the Source of Wealth: a Relevant Person should establish a Source of Wealth or income, including how the funds were acquired, to assess whether the actual Transaction pattern is consistent with the expected Transaction pattern and whether this constitutes any grounds for suspicion of money laundering.

7. It is important for a Relevant Person to obtain such information because this process should allow the risk of being exploited for the purpose of money laundering to be reduced to a minimum. It should also enable suspicious Transactions to be detected because they are incompatible with the information received.

8. Any unusual facts of which a Relevant Person becomes aware during the identification process may be an indication of money laundering and should prompt the Relevant Person to request supplementary information and evidence.

9. The Regulator expects a Relevant Person to establish the full identity of all relevant parties to the business relationship. Further, a Relevant Person should apply adequate measures to enable it to understand the relationship between the counterparties involved. The following list includes some identification checks for particular relationships:

a. joint account holders and joint applicants: identification should be performed and evidence obtained for all applicants and account holders;

b. pooled accounts which are managed by professional intermediaries such as mutual funds, pension funds, money funds, lawyers and stockbrokers on behalf of entities or other Persons: all Beneficial Owners of the account held by the intermediary should be identified;

c. power of attorney: identification and evidence should be obtained for the applicants and account holders as well as for the holder of the power of attorney; and

d. minors: an account for a minor should be opened by a family member or guardian whose identification evidence should be obtained in addition to the birth certificate or passport of the minor.

8.2 Timing of Customer Due Diligence

8.2.1 (1) A Relevant Person must:

(a) undertake the appropriate CDD under Rule 8.3.1(a) to (c) when it is establishing a business relationship with a Customer; and

(b) undertake the appropriate CDD under Rule 8.3.1(d) after establishing a business relationship with a Customer.

(2) A Relevant Person must also conduct appropriate CDD 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 CDD;

(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 8.3.1 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 in accordance with Rule 15.5.

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

Guidance

1. For the purposes of Rule 8.2.1(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 8.2.1(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 8.2.1, a Relevant Person should also, where relevant, consider Rule 8.7.1 regarding failure to conduct or complete CDD and Chapter 14 regarding Suspicious Activity Reports and tipping off.

4. For the purposes of Rule 8.2.1(3)(d), the Regulator 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.

8.3 Customer Due Diligence requirements

8.3.1 (1) In undertaking the CDD required by Rule 8.1.1(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 8.6.1.

(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) A Relevant Person must have systems and controls in place to determine whether a Customer, or a Beneficial Owner of the Customer, is a PEP. If so, 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.

8.3.2 Subject to Rule 8.3.3, a Relevant Person is not required to establish:

(1) whether a Customer is acting on its own behalf; or

(2) the Beneficial Owner(s) of the relevant funds,

if the Relevant Person's Customer is a Person falling within Rule 8.1.1.

8.3.3 (1) Rules 8.1.1(2) and 8.3.2 do not apply where the Relevant Person:

(a) knows or suspects; or

(b) has reasonable grounds to know or suspect,

that a Customer or a Person on whose behalf the Customer is acting, is engaged in Money Laundering.

(2) The Relevant Person will be taken to have the knowledge or suspicion or to have reasonable grounds to have the knowledge or suspicion referred to in paragraph (1) if:

(a) any Employee handling the Transaction or potential Transaction; or

(b) anyone managerially responsible for it,

knows or suspects, or has reasonable grounds to know or suspect, that a Customer or a Person on whose behalf the Customer is acting is engaged in Money Laundering.

Guidance on CDD

1. A Relevant Person is expected to establish to its satisfaction the true identity of a Customer and any other Person on whose behalf the Customer is acting, including that of the Beneficial Owner of the relevant funds which may be the subject of a Transaction to be considered. The Relevant Person should verify that it is dealing with a true and existing Person. It also should obtain evidence of verification that is sufficient to establish that the Person is indeed who he claims to be.

   Because of the high degree of risk sensitivity needed to comply with CDD, the following (which is not meant to be exhaustive) sets out Guidance regarding the type of information and evidence which should be obtained by a Relevant Person to establish and verify the identity of a Customer. The standard of verification, taking into account the risk-based approach and circumstances where there are no original documents, is also set out below.

Individuals

2. A Relevant Person should, in complying with Rule 8.3.1(1)(a), and adopting the RBA, obtain, verify and record, for every Customer who is a Natural Person, the following identification information in either documentary (hard copy) or electronic form:

   a. true full name (or names) used;

   b. date and place of birth;

   c. nationality;

d. complete current permanent address, including all relevant details with regard to country of residence; and

e. telephone and email address.

3. Items 2a. to 2c. 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.

4. The following additional information may be requested depending on the facts and the nature and size of the transaction or the business relationship:

   a. occupation or profession, name of employer and location of activity;

   b. information regarding the nature of the business to be conducted;

   c. information regarding the origin of the funds;

   d. legal domicile or fiscal residence; and

   e. information regarding the Source of Wealth or income.

5. The concept of domicile referred to at item 4d. above 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.

6. The address of a prospective Customer should enable a Relevant Person to physically locate the Customer. If P.O. Box numbers are customary to a country, additional methods of physically locating the Customer should be applied.

7. Documentary evidence of identity:

   a. current, signed passport;

   b. current, signed ID card; or

   c. other identification documentation that is customary in the country of residence, such as a driving licence, including a clear photograph of the prospective Customer.

8. A Relevant Person should ensure that any documents used for the purpose of identification are original documents.

9. Where personal identity documents, such as a passport, ID card or other identification documentation cannot be obtained in original form, for example because a Relevant Person has no physical contact with the Customer, the identification documentation provided should be certified as a true copy of the original document by any one of the following:

   a. a registered lawyer;

   b. a registered notary;

c. a chartered accountant;

d. a government ministry;

e. a post office;

f. a police officer; or

g. an embassy or consulate.

The individual or authority undertaking the certification should be contactable if necessary.

Where a copy of an original identification document is made by a Relevant Person, the copy should be dated, signed and marked with 'original sighted'.

10. Documentary evidence of address:

a. record of home visit;

b. confirmation from an electoral register search that a Person of such a name lives at that address;

c. tenancy agreement;

d. utility bill; or

e. local authority tax bill.

Unincorporated businesses or partnerships

11. Evidence to be obtained in either documentary or electronic form:

a. true full name or names;

b. complete current registered and trading address, including relevant details with regard to country of establishment;

c. telephone number and email address;

d. fiscal residence;

e. business activity;

f. information on the nature of the business to be conducted;

g. trading licence, with renewal date;

h. a list of authorised signatories of the business or partnership;

i. regulatory body, if applicable;

j. information regarding the origin of funds; and

k. information regarding the Source of Wealth/income.

12. Documentary evidence of identity:

a. the latest annual report and accounts, audited where applicable; and

b. a certified copy of the partnership deed, to ensure that it has a legitimate purpose and to ascertain the nature of the business or partnership.

13. Evidence of the trading address of the business or partnership should be obtained and may be verified with a visit to the place of business.

Guidance on Restricted Scope Companies

14. The Restricted Scope Company is a corporate vehicle offering a greater degree of confidentiality than other forms of corporate entity in ADGM. Restricted Scope Companies are not required to file accounts and are not required to audit their accounts. Restricted Scope Companies must file an annual return, articles, and details of their registered offices, directors and secretary (if they have one) with the Registrar.

15. Relevant Persons will know that the Restricted Scope Company is subject to less onerous corporate disclosure requirements than other forms of corporate entity due to the requirement to have "(Restricted)" in the company's name. Given that only a Restricted Scope Company's constitution and details of its registered office will be available in a public register, Relevant Persons will be required to have a bilateral dialogue with the Restricted Scope Company in accordance with the RBA to obtain any other relevant information which is needed to assess the money laundering risks to which it is exposed.

16. Evidence to be obtained in either documentary or electronic form:

a. true full name or names;

b. registered address;

c. telephone number and email address;

d. fiscal residence;

e. business activity;

f. information regarding the origin of funds;

g. information regarding the Source of Wealth/income; and

h. the latest annual report and accounts, audited where applicable.

Corporate entities including Financial Institutions or Credit Institutions that are not covered by an exemption, including Financial Institutions or Credit Institutions that are not regulated by the Regulator or regulated in a FATF country

17. Evidence to be obtained in either documentary or electronic form:

a. registered corporate name and any trading names used;

b. complete current registered address and any separate principal trading addresses, including all relevant details with regard to country of residence;

c. telephone number and email address;

d. date and place of incorporation;

e. corporate registration number;

f. fiscal residence;

g. business activity;

h. regulatory body, if applicable;

i. name and address of Group, if applicable;

j. legal form;

k. name of external auditor;

l. information regarding the nature and level of the business to be conducted;

m. information regarding the origin of the funds; and

n. information regarding the Source of Wealth/income.

18. Documentary evidence of identity:

a. copy of the extract of the register of the regulator or exchange, or state law or edict creating the entity, in case of regulated, listed or state-owned companies;

b. certified copy of the articles of association or statutes;

c. certified copy of either the certificate of incorporation or the trade register entry and the trading licence, including the renewal date;

d. latest annual report, audited and published if applicable;

e. certified copies of the list of authorised signatories specifying who is authorised to act on behalf of the Customer account and of the board resolution authorising the signatories to operate the account;

f. certified copies of the identification documentation of the authorised signatories;

g. names, country of residence, nationality of Directors or partners and of the members of the Governing Body; and

h. list of the main shareholders holding more than 5% of the issued capital.

19. If the applying Customer is not obliged to publish an audited annual report, adequate information about the financial accounts should be obtained.

20. A Relevant Person should verify that the applying Customer is active and has not been, or is not in the process of being dissolved, wound-up or terminated.

Trusts, nominees and fiduciaries

21. In addition to the identification documentation listed under 'corporate entities' (Paragraphs 17 to 20 above), the following information and documentation should be obtained:

    a. identity of any settlor, the trustee and any principal controller who has the power to remove the trustee, as well as the identity of the Beneficial Owner;

    b. a certified copy of the trust deed, to ascertain the nature and purpose of the trust; and

    c. documentary evidence of the appointment of the current trustees.

22. A Relevant Person should ensure that it is advised about any changes concerning the individuals who have control over the funds, and concerning the Beneficial Owners.

23. Where a trustee, principal controller or Beneficial Owner who has been identified is about to be replaced, the identity of the new trustee, principal controller or Beneficial Owner should be verified before they are allowed to exercise control over the funds.

Authorised Persons and Recognised Bodies regulated by the Regulator or Financial Institutions or Credit Institutions regulated in a FATF country

24. Pursuant to the exception under Simplified Customer Due Diligence, identification evidence is generally not required for Customers of a firm who are themselves Authorised Persons, Auditors, Recognised Clearing Houses or Recognised Investment Exchanges registered or regulated by the Regulator or are Financial Institutions or Credit Institutions regulated by any FATF country's relevant Non-ADGM Financial Services Regulator or other relevant regulatory authority or regulator.

25. However, the confirmation of the existence of such a relevant firm or institution and its regulatory status, including the application of AML applying in the ADGM or equivalent AML provisions, should be verified by the Relevant Person prior to entering into a Customer relationship. Regular professional and commercial checks and due diligence investigations should still be performed. The Relevant Person should verify the regulatory status of the firm or institution by one of the following means:

    a. requesting confirmation from the relevant Non-ADGM Financial Services Regulator or other relevant regulatory authority, regulator, body, or home country Central Bank; or

    b. requesting a certified copy of a relevant licence or authorisation to conduct financial or banking business from the firm or institution.

Clubs, cooperative, charitable, social or professional societies

26. A Relevant Person should take steps to satisfy itself as to the legitimate purpose of clubs and societies by, for example, obtaining a certified copy of the constitution of the organisation.

27. The identity of the principal signatories and controllers should be verified in accordance with the requirements for private individuals. The capacity of the signatories to act on behalf of the club or society and the identity of Beneficial Owners of the funds should be established and verified.

28. A Relevant Person should consider the following items while completing the Customer identification requirements for a Client which is a charitable society:

    a. whether the charity is licensed or permitted by a regulatory authority, regulator or government entity in its home country. (Note: charities in the U.A.E. are required to obtain from the U.A.E. Minister of Labour and Social Affairs a certificate which confirms their identity, permits them to open bank accounts and states whether they are permitted to collect donations and make financial transfers outside the U.A.E. through such bank accounts);

    b. the type and quality of regulation to which the charity is subject in its home state;

    c. the structure and overall character of management and trustees;

    d. whether the charity allows donors to specify beneficiaries. If yes, then it would be prudent to ensure that such charities are closely regulated;

    e. the pattern of beneficiaries: a small number of targeted beneficiaries could indicate potential risks;

    f. whether the charity and its functioning is dominated by a few large donors and the pattern of donors; and

    g. whether it is a private foundation as, if it is, it is more likely to be dominated by a single donor and linked to a small number of beneficiaries which will necessitate scrutiny of both the donor and the beneficiaries.

29. The Regulator may, from time to time:

    a. review the relevant guidance in light of changing money laundering legislation issued by the U.A.E. Central Bank, money laundering trends and techniques and according to international standards, in order to keep the guidance current; and

    b. provide such other guidance as it deems appropriate regarding Customer identification obligations.

30. The Regulator expects that a Relevant Person will take these changes into account by amending, as appropriate, its policies, procedures, systems and controls.

31. Sound "Know Your Customer" arrangements have particular relevance to the safety and soundness of a Relevant Person, in that:

a. they help to protect its reputation and the integrity of the ADGM by reducing the likelihood of Relevant Persons becoming a vehicle for, or a victim of, financial crime and suffering consequential reputational damage; and

b. they constitute an essential part of sound risk management, for example by providing the basis for identifying, limiting and controlling risk exposures to assets and liabilities, including assets under management.

Risk-Based Approach

32. Any inadequacy of "Know Your Customer" standards can expose Relevant Persons to serious business operation and control risks.

33. In complying with Rule 8.3.1(1)(a), a Relevant Person should adopt an RBA for the Customer identification and verification process. Depending on the money laundering risk assessment regarding the Relevant Person's Customer, the Relevant Person should decide to what level of detail the Customer identification and verification process will need to be performed. The risk assessment regarding a Customer should be recorded in the Customer file.

34. The RBA does not release a Relevant Person from its overall obligation to identify fully and obtain evidence of Customer identification to the Regulator's satisfaction.

35. A Relevant Person is advised that in cases of doubt it should adopt a stricter rather than a moderate approach in its judgement concerning the risk level and the level of detail to which Customer identification is performed and evidence obtained.

No Original Documents

36. In complying with Rule 8.3.1(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 Regulator 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 8.3.1(1)(a). The Regulator 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.

37. For higher risk situations the Regulator 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.

38. In complying with Rule 8.3.1(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 on-going due diligence under Rule 8.3.1(1)(d).

39. 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

40. 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 Regulator 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.

41. When verifying Beneficial Owners under Rule 8.3.1(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 focuses 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 Regulator does not set explicit ownership or control thresholds in defining the Beneficial Owner because the Regulator considers that the applicable threshold to adopt will ultimately depend on the risks associated with the Customer, and so the Regulator 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 5.1.1. 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.

42. The Regulator 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 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.

43. For a retail investment fund which is widely-held and where the investors invest via pension contributions, the Regulator 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 Regulator 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 Regulator would not expect a Relevant Person to identify the Beneficial Owners.

44. 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, the settlor, the protector, the enforcer, the 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 and corruption

45. 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. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the Customer into a higher risk category.

46. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such Person, if he were committing money laundering, would attempt to place his money offshore where he 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.

47. Due diligence to uncover information about PEPs can be time consuming and difficult, requiring close fact checking of the names, dates of birth, photographs and identification numbers of individuals against reputable PEP lists. However, despite the development of such lists by certain vendors, as well as the United Nations' compilation of a list of heads of states which fall within the FATF definition of PEPs, there is no "official" centralised global PEP list. It is therefore left to each Relevant Person to determine whether they would like to internally develop their own database or list of PEPs as a due diligence tool.

48. Where a Customer relationship is maintained with a PEP, detailed monitoring and due diligence procedures should include:

    a. analysis of any complex structures, for example involving trusts or multiple jurisdictions;

    b. appropriate measures to establish the Source of Wealth;

    c. development of a profile of expected activity for the business relationship in order to provide a basis for Transaction and account monitoring;

    d. initial screening and due diligence prior to the account opening;

    e. Senior Management approval for the account opening;

f. regular oversight of the relationship with a PEP by Senior Management; and

g. ongoing and periodical screening of accounts opened by PEPs.

49. A Relevant Person is advised that Customer relationships with family members or close associates of PEPs involve similar risks to those with PEPs themselves.

50. 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 Federal Law No. 4 of 2002.

51. The Regulator 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.

Guidance on Insurers

52. With regard to Insurers, the following "Know Your Customer" verification and identification set out in this section should be taken into account.

53. An Insurer undertaking verification should establish to its satisfaction that every verification subject exists. All verification subjects of joining applicants for Insurance Business should normally be verified. In the case of arrangements such as trusts, nominee companies and front companies, verification should include an assessment of the substance of the arrangement, for example in relation to settlors, trustees and beneficiaries.

54. An Insurer should carry out verification in respect of the parties entering into the Contract of Insurance. On some occasions there may be underlying principals and, if this is the case, the true nature of the relationship between principals and the policyholders should be established and appropriate enquiries performed about the former, especially if the policyholders are accustomed to acting on their instructions. 'Principal' should be understood in its widest sense to include, for example, Beneficial Owners, settlors, controlling shareholders, Directors and major beneficiaries.

Guidance on electronic money

55. The following factors will increase the risk of electronic money products being used for money laundering or terrorist financing:

a. high, or no, Transaction or purse limits: the higher the value and frequency of Transactions, and the higher the purse limit, the greater the risk, particularly where Customers are permitted to hold multiple purses;

b. frequent cross-border Transactions, unless within a single scheme, can give rise to difficulties with information sharing: dependence on counterparty systems increases the risk;

c. funding of purses by unverified parties presents a higher risk of money laundering, whether it is the Customer who is unverified or a third party;

d. funding of purses using cash offers little or no audit trail of the source of the funds and hence presents a higher risk of money laundering;

e. funding of purses using electronic money products that have not been verified may present a higher risk of money laundering;

f. the non-face-to-face nature of many products gives rise to increased risk;

g. the ability of consumers to hold multiple purses (for example, open multiple accounts or purchase a number of cards) without verification of identity increases the risk;

h. cash access, for example by way of ATMs, as well as an allowance for the payment of refunds in cash for purchases made using electronic money, will increase the risk;

i. increased product functionality may, in some instances, give rise to a higher risk of money laundering (product functionality includes Person-to-business, Person-to-Person, and business-to-business transfers);

j. products that feature multiple cards linked to the same account increase the utility provided to the user, but may also increase the risk of money laundering, particularly where the Customer is able to pass on linked 'partner' cards to anonymous third parties;

k. segmentation of the business value chain, including use of multiple agents and outsourcing, in particular to overseas locations, may give rise to a higher risk; and

l. the technology adopted by the product may give rise to specific risks that should be assessed.

56. Electronic money issuers should address the risks that are inherent in payments in a similar manner to other retail products: by putting in place systems and controls that prevent money laundering and terrorist financing by detecting unusual Transactions and predetermined patterns of activity.

57. The systems and controls electronic money issuers put in place must be commensurate with the money laundering and terrorist financing risk to which they are exposed. The detail of electronic money issuers' systems and controls will therefore vary. Examples include those that:

a. place limits on purse storage values, cumulative turnover or amounts transacted;

b. can detect money laundering Transaction patterns;

c. will detect anomalies to normal Transaction patterns;

d. can identify multiple purses held by a single individual or group of individuals, such as the holding of multiple accounts or the 'stockpiling' of pre-paid cards;

e. can look for indicators of accounts being opened with different electronic money issuers as well as attempts to pool funds from different sources;

f. can identify discrepancies between submitted and detected information, for example between country of origin submitted information and the electronically-detected IP address;

g. deploy sufficient resources to address money laundering risks, including, where necessary, specialist expertise for the detection of suspicious activity;

h. allow collaboration with merchants that accept electronic money to identify and prevent suspicious activity; and

i. restrict funding of electronic money products to funds drawn on accounts held in the ADGM.

8.4 Enhanced Customer Due Diligence

8.4.1 Where a Relevant Person is required to undertake Enhanced Customer Due Diligence under Rule 8.1.1(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 CDD information which it holds on the Customer and any Beneficial Owners;

(c) verify information on:

(i) the Customer's Source of Funds; and

(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.

Guidance

1. In Rule 8.4.1 Enhanced Customer Due Diligence 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 8.4.1(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 Customer Due Diligence, 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 Regulator 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 Regulator 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 8.4.1, 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 include:

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

b. as an alternative measure, where one of the measures in Rule 8.4.1 (a) to (e) cannot be carried out.

8.5 Simplified Customer Due Diligence

8.5.1 (1) Where a Relevant Person is permitted to undertake Simplified Customer Due Diligence under Rule 8.1.1(2), modification of Rule 8.3.1 may include:

(a) verifying the identity of the Customer and any Beneficial Owners after the establishment of the business relationship under Rule 8.2.1(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 inferring such purpose and nature from the type of Transactions or business relationship established.

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

Guidance

1. Rule 8.5.1(1) provides examples of Simplified Customer Due Diligence 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 Customer Due Diligence.

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.

8.6 On-going Customer Due Diligence

8.6.1 An Authorised Person must ensure that the information and evidence concerning a Customer's identity is accurate and up-to-date. When undertaking on-going CDD under Rule 8.3.1(1)(d), a Relevant Person must, using the RBA:

(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 CDD 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 7.2.1(1)(b) remains appropriate for the Customer in light of the money laundering risks.

8.6.2 A Relevant Person should apply an intensified and on-going monitoring programme with respect to higher risk Transactions and accounts.

Guidance

1. The Customer identification process does not end at the point of application. Following the start of the Customer relationship, a Relevant Person should ensure that all relevant evidence and information is kept up-to-date including, for example, the list of authorised signatories who can act on behalf of a corporate Client.

2. In complying with Rule 8.6.1(d), a Relevant Person should undertake a periodic review to ensure that non-static Customer identity documentation is accurate and up-to-date. A Relevant Person is expected to ensure that the information and the evidence obtained from a Customer is valid and has not expired, for example when obtaining copies of identification documentation such as a passport or identification card. 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.

3. A Relevant Person should undertake a review under Rule 8.6.1(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.

4. The degree of the on-going due diligence to be undertaken will depend on the Customer risk assessment carried out under Rule 7.2.1.

5. 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.

8.6.3 A Relevant Person must review its Customers, their business, and Transactions, against Sanctions Lists when complying with Rule 8.6.1(d).

8.7 Failure to conduct or complete Customer Due Diligence

8.7.1 (1) Where, in relation to any Customer, a Relevant Person is unable to conduct or complete the requisite CDD in accordance with Rule 8.1.1 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 CDD necessitates the making of a Suspicious Activity Report under Rule 14.3.1(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 Federal Law No. 4 of 2002; or

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

Guidance

1. In complying with Rule 8.7.1(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 8.7.1 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 ADGM) have not been subject to CDD at an equivalent standard to that required by the AML Rulebook, 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 8.7.1.

8.8 A diagram outlining the Customer due diligence process is contained in A1.4.

9. RELIANCE AND OUTSOURCING OF AML COMPLIANCE

9.1 Reliance on a third party

9.1.1 (1) A Relevant Person may rely on the following third parties ("**qualified professionals**") to conduct one or more elements of CDD on its behalf:

(a) an Authorised Person or Recognised Body;

(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;

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

(e) other specialised utilities for the provision of outsourced AML services.

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

(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 CDD 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 CDD 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 Non-ADGM 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 CDD 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 is subject to policies and requirements equivalent to FATF standards, either:

(i) where the Group applies and implements a Group-wide policy on CDD and record keeping which is equivalent to the standards set by FATF; or

(ii) where the effective implementation of those CDD and record keeping requirements and AML programmes are supervised at Group level by a Non-ADGM 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;

(b) no exception from identification obligations has been applied in the original identification process; and

(c) a written statement is received from the introducing member of the Relevant Person's Group confirming that:

(i) the Customer has been identified in accordance with the relevant standards under (4)(a) and (b);

(ii) any identification evidence can be accessed by the Relevant Person without delay; and

(iii) the identification evidence will be kept for at least 10 years.

(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 CDD 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 CDD requirements in the AML Rulebook.

9.2 Business partner identification

9.2.1 (1) (a) Prior to establishing the business relationship, a Relevant Person must establish and verify its business partners' identities in accordance with Rule 8.1.3 by obtaining sufficient and satisfactory evidence of the identity of any business partner it relies upon in carrying on its Regulated Activities.

(b) A Relevant Person must maintain accurate and up-to-date information and conduct on-going due diligence on its business partners, throughout the course of the business relationship.

(c) If at any time a Relevant Person becomes aware that it lacks sufficient information or documentation concerning a business partner's identification, or develops a concern about the accuracy of its current information or documentation, it must promptly obtain appropriate material to verify such business partner's identity.

(2) In the context of this Rule, a 'business partner' includes:

(a) a qualified professional as specified in Rule 9.1.1(1);

(b) a member of the Relevant Person's Group;

(c) a Correspondent Bank; or

(d) any other service provider.

(3) A Relevant Person that establishes, operates or maintains a Correspondent Account for a Correspondent Banking Client must ensure that it has arrangements to:

(a) conduct due diligence in respect of the opening of a Correspondent Account for a Correspondent Banking Client, including measures to identify:

(i) its ownership and management structure;

(ii) its major business activities and Customer base;

(iii) its location; and

(iv) the intended purpose of the Correspondent Account;

(b) identify third parties that will use the Correspondent Account; and

(c) monitor Transactions processed through a Correspondent Account that has been opened by a Correspondent Banking Client, in order to detect and report any suspicion of Money Laundering.

9.2.2 A Relevant Person must not:

(1) establish a correspondent banking relationship with a Shell Bank;

(2) establish or keep anonymous accounts or accounts in false names; or

(3) maintain a nominee account which is held in the name of one Person, but controlled by or held for the benefit of another Person whose identity has not been disclosed to the Relevant Person.

Guidance

1. In complying with Rule 9.1.1(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 9.1.1(3)(b), these need only be available on request without delay.

2. The Regulator would expect a Relevant Person, in complying with Rule 9.1.1(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 Regulator 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 have undertaken 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 9.1.1(3)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

5. The requirement to identify the business partner is meant to cover only those business partners who may pose any relevant money laundering risk to the Relevant Person. Hence, a Relevant Person would be not required to establish and verify the identity of, for example, its maintenance or cleaning service.

6. The Regulator may take into account the identity of a Relevant Person's business partner and the nature of their relationship in considering the fitness and propriety of a Relevant Person.

7. "Know your business partner" is as important as "Know Your Customer". A Relevant Person is therefore required to verify the identity of a prospective business partner and to obtain evidence of it. The same documentation that is used to identify Customers should be obtained from the business partner prior to conducting any business.

8. Before entering into a business relationship, a Relevant Person should conduct a due diligence investigation, which includes ensuring that the business partner is an existing Person authorised to conduct the kind of business in question and, if applicable, verifying that this Person is duly regulated by a Non-ADGM Financial Services Regulator or other relevant regulatory authority or regulator. In accordance with "The Wolfsberg Anti-Money Laundering Principles for Correspondent Banking", the Relevant Person should take into account, and verify the nature of:

    a. the business to be conducted and the major business activities;

    b. the jurisdiction where the business partner is located as well as that of the parent; and

    c. the transparency and the nature of the ownership and the management structure.

9. A Relevant Person may also gather information about the reputation of the business partner, including whether it has been subject to investigation or regulatory action in relation to money laundering or terrorist financing.

10. A Relevant Person should adopt a risk-based approach when verifying its business partners' identities. Depending on the money laundering risk assessment of the Relevant Person's business partner, the Relevant Person should decide the level of detail to which the business partner identification and verification process will need to be performed.

11. A Relevant Person should verify whether any secrecy or data protection law exists in the country of incorporation of the business partner that would prevent access to relevant data.

12. A Relevant Person should have in place specific arrangements to ensure that adequate due diligence and identification measures with regard to the business relationship are taken.

13. The Relevant Person should conduct regular reviews of the relationship with its business partners.

14. The Senior Management or Governing Body of a Relevant Person should give their approval before it establishes any new correspondent banking relationships.

15. A Relevant Person should also have arrangements to guard against establishing a business relationship with business partners who permit their accounts to be used by Shell Banks; further details on the definition of Shell Banks are set out in Guidance 2 to Rule 10.2.2.

9.3 Outsourcing

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

Guidance

Prior to appointing an outsourced service provider to undertake CDD, a Relevant Person should undertake 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.

9.4 Record Keeping and Data Protection

9.4.1 Where Customer identification records are kept by the Relevant Person or other Persons outside the ADGM, a Relevant Person must take reasonable steps to ensure that the records are held in a manner consistent with these Rules.

9.4.2 A Relevant Person must verify whether there is secrecy or data protection legislation that would restrict access without delay to such data by the Relevant Person, the Regulator or the law enforcement agencies of the U.A.E. Where such legislation exists, the Relevant Person must obtain without delay certified copies of the relevant identification evidence and keep these copies in a jurisdiction which allows access by all those Persons.

9.5 A diagram outlining the reliance and outsourcing of AML compliance requirements is contained in A1.5.

10. CORRESPONDENT BANKING, WIRE TRANSFERS, ANONYMOUS ACCOUNTS AND AUDIT

10.1 Application

10.1.1 This Chapter applies only to an Authorised Person or Recognised Body other than a Representative Office.

10.2 Correspondent banking

10.2.1 An Authorised Person proposing to have a correspondent banking relationship with a respondent bank must:

(a) undertake CDD 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 as to 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 Person'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 Person, the respondent bank:

(i) has undertaken CDD (including on-going CDD) at least equivalent to that in Rule 8.3.1 in respect of each Customer; and

(ii) is able to provide the relevant CDD information in (i) to the Authorised Person upon request; and

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

10.2.2 An Authorised Person 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

1. The rules and guidance set out in Rule 9.2 above also applies to correspondent banking business partners. This Rule provides further details on specific requirements applicable to a correspondent banking business relationship.

2. With regard to Correspondent Banking Clients and, if applicable, other qualified professionals, specific care should be taken to assess their AML arrangements regarding Customer identification, Transaction monitoring, terrorist financing and other relevant elements, and to verify that these business partners comply with the same or equivalent AML requirements as the Relevant Person. Information on applicable laws and regulations regarding the prevention of money laundering should be obtained. A Relevant Person should ensure that a Correspondent Banking Client does not use the Relevant Person's products and services to engage in business with Shell Banks. 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 Regulator does not consider that the existence of a local agent or low level staff constitutes physical presence.

3. If applicable, information on distribution networks and delegation of duties should be obtained.

10.3 Wire transfers

10.3.1 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.

10.3.2 (1) An Authorised Person and Recognised Body 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 or Recognised Body which (a) provides Financial Institutions with messages or other support systems for transmitting funds; or (b) 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 and Recognised Body 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. 'FATF Special Recommendation Number 16' seeks to ensure that national or international electronic payment and message systems, including fund or wire transfer systems such as SWIFT, are not misused as a means to break the money laundering audit trail. Therefore, the information about the Customer as the originator of the fund transfer should remain with the payment instruction through the payment chain.

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

3. Relevant Persons should monitor for, and conduct enhanced scrutiny of, suspicious activities, including incoming fund transfers that do not contain complete originator information, including name, address and account number or unique reference number.

4. The Regulator considers that concealing or removing in a wire transfer any of the information required by Rule 10.3.2(3) would be a breach of the requirement to ensure that the wire transfer contains accurate originator and beneficiary information.

10.4 Audit

10.4.1 An Authorised Person and Recognised Body must ensure that its audit function includes regular reviews and assessments of the effectiveness of the Authorised Person or Recognised

Body's money laundering policies, procedures, systems and controls, and its compliance with its obligations in the AML Rulebook.

Guidance

1. The review and assessment undertaken for the purposes of Rule 10.4.1 may be undertaken:

   a. internally by the Authorised Person or Recognised Body'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 10.4.1 should cover at least the following:

   a. sample testing of compliance with the Authorised Person or Recognised Body's CDD arrangements;

   b. an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced; and

   c. a review of the nature and frequency of the dialogue between the Senior Management and the MLRO.

10.5 Anonymous and nominee accounts

10.5.1 An Authorised Person and Recognised Body 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 or Recognised Body.

11. SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

11.1 Sanctions and Other International Obligations

11.1.1 (1) A Relevant Person must establish and maintain effective systems and controls to obtain and make appropriate use of resolutions or Sanctions which it is required to comply with, under the laws of ADGM or any other jurisdiction.

(2) A Relevant Person must immediately notify the Regulator 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 any Sanctions which the Relevant Person is required to comply with, under the laws of ADGM or any other jurisdiction.

(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 11.1.1, 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 11.1.1 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. a Recognised Investment Exchange or Recognised Clearing House 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.

11.2 Government, regulatory and international findings

11.2.1 (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) The Basel Committee on Banking Supervision;

(e) U.A.E. enforcement agencies;

(f) the Regulator; and

(g) any other jurisdiction which promulgates Sanctions to which it is subject,

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 risks to stakeholders.

2. A Relevant Person should examine and pay special attention to any Transactions or business relationships with Persons located in countries or jurisdictions mentioned by the Persons in Rule 11.2.1(1)(a) to (f).

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 Regulator 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 14 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 Regulator may, from time to time, publish U.A.E., FATF or other findings, guidance, directives or Sanctions. However, the Regulator 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, and OFAC.

7. In addition, the systems and controls mentioned in Rule 11.2.1 should be established and maintained by a Relevant Person taking into account its risk assessment under Chapters 6 and 7. In relation to the term "make appropriate use" in Rule 11.2.1, 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 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 Regulator 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 Regulator may require Relevant Persons to take any special measures it may prescribe with respect to certain types of Transactions or accounts where the Regulator reasonably believes that any of the above may pose a money laundering risk to the ADGM.

12. MONEY LAUNDERING REPORTING OFFICER

12.1 Appointment of a MLRO

12.1.1 (1) A Relevant Person must appoint an individual as MLRO, with responsibility for implementation and oversight of its compliance with the Rules in the AML Rulebook, who has an appropriate level of seniority and independence to act in the role. It must do so by completing and filing with the Regulator the appropriate form specified by the Regulator.

(2) The MLRO in (1) and Rule 12.1.5 must be resident in the U.A.E.

12.1.2 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

The individual appointed as the MLRO of a Recognised Investment Exchange or Recognised Clearing House is the same individual who holds the position of MLRO of that Recognised Investment Exchange or Recognised Clearing House under the relevant REC Rule.

12.1.3 If the MLRO leaves the employment of the Relevant Person, the Relevant Person must designate a successor within 28 days. An Authorised Person, other than a Representative Office, must appoint an individual to act as a deputy MLRO of the Authorised Person to fulfil the role of the MLRO in his absence.

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

Guidance

1. The individual appointed as the deputy MLRO of an Authorised Person need not apply for Recognised Person status for performing the Recognised Function of MLRO, subject to Rules in GEN section 11.6.

2. A Relevant Person other than an Authorised Person should make adequate arrangements to ensure that it remains in compliance with the AML Rulebook 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.

12.1.5 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.

12.2 Qualities of a MLRO

12.2.1 A Relevant Person must ensure that its MLRO has:

(a) direct access to the Governing Body and its Senior Management;

(b) sufficient and up-to-date qualifications and experience to fulfil the role;

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

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

(e) timely and unrestricted access to information the Relevant Person has about the financial and business circumstances of a Customer or any Person on whose behalf the Customer is or has been acting sufficient to enable him to carry out his responsibilities in Rule 12.3.1; and

(f) unrestricted access to relevant information about the features of the Transaction which the Relevant Person has entered into or may have contemplated entering into with or for the Customer or a Person on whose behalf a Customer is or has been acting.

Guidance

The Regulator 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.

12.3 Responsibilities of a MLRO

12.3.1 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 14.2.2;

(c) taking appropriate action under Rule 14.3.1 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 Regulator regarding money laundering issues;

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

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11; and

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under Chapter 13.

12.4 Reporting

12.4.1 The MLRO must report at least annually to the Governing Body or Senior Management of the Relevant Person on the following matters:

(a) the results of the review under Rule 4.1.1(4);

(b) the Relevant Person's compliance with applicable AML laws including these Rules;

(c) the quality of the Relevant Person's AML policies, procedures, systems and controls;

(d) any relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions and how the Relevant Person has taken them into account;

(e) any internal Suspicious Activity Reports made by the Relevant Person's Employees and action taken in respect of those reports, including the grounds for all decisions;

(f) any external Suspicious Activity Reports made by the Relevant Person and action taken in respect of those reports including the grounds for all decisions; and

(g) any other relevant matters related to Money Laundering as it concerns the Relevant Person's business.

12.4.2 A Relevant Person must ensure that its Governing Body or Senior Management promptly:

(a) assess the report provided under Rule 12.4.1;

(b) take action, as required, subsequent to the findings of the report, in order to resolve any identified deficiencies; and

(c) make a record of their assessment pursuant to paragraph (a) and the action taken pursuant to paragraph (b).

12.4.3 (1) The report provided under Rule 12.4.1 and the records of the assessment and actions pursuant to Rule 12.4.2 must be documented in writing.

(2) A complete copy of each document referred to in paragraph (1) must be provided to the Regulator within two months of the end of the Relevant Person's financial year.

13. AML TRAINING AND AWARENESS

13.1 Training and awareness

13.1.1 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) know the identity, and understand the responsibilities, of the Relevant Person's MLRO and his deputy;

(ii) understand the relevant legislation relating to money laundering, including Federal Law No. 1 of 2004, Federal Law No. 4 of 2002, Federal Law No. 7 of 2014, and any other relevant Federal laws;

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

(iv) recognise and deal with Transactions, risks, trends, techniques and other activities which may be related to money laundering;

(v) 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 14.2.2;

(vi) understand its arrangements regarding the making of a notification to the MLRO under Rule 14.2.2;

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

(viii) 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

(ix) understand the relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Chapter 11;

(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 and the 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); and

(d) ensure that its AML training is up-to-date with money laundering trends and techniques.

13.2 Frequency

13.2.1 A Relevant Person must conduct AML training sessions for all Employees at least once every 12 months.

13.3 Record-keeping

13.3.1 All relevant details of the Relevant Person's AML training must be recorded, including:

(a) dates when the training was given;

(b) the nature of the training; and

(c) the names of the Employees who received the training.

13.3.2 These records must be kept for at least 10 years from the date on which the training was given.

Guidance

1. The Regulator 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 an RBA to AML training. The Regulator 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 Person the Regulator 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.

14. SUSPICIOUS ACTIVITY REPORTS

14.1 Application and definitions

14.1.1 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.

14.2 Internal reporting requirements

14.2.1 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.

14.2.2 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 ("**Internal Suspicious Activity Report**").

14.2.3 A Relevant Person must have policies and procedures to ensure that disciplinary action can be taken against any Employee who fails to make such a report.

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. 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 Regulator 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.

14.3 External Suspicious Activity Report

14.3.1 A Relevant Person must ensure that where the Relevant Person's MLRO receives a notification under Rule 14.2.2, the MLRO, without delay:

(a) investigates and documents the circumstances in relation to which the notification made under Rule 14.2.2 was made;

(b) determines whether in accordance with Federal Law No. 4 of 2002 an external Suspicious Activity Report must be made to the AMLSCU and documents such determination;

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

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

14.3.2 The MLRO must document:

(a) the steps taken to investigate the circumstances in relation to which an Internal Suspicious Activity Report is made; and

(b) where no external Suspicious Activity Report is made to the AMLSCU, the reasons why no such report was made.

14.3.3 Where, following a notification to the MLRO under 14.2.2, no external Suspicious Activity Report is made, a Relevant Person must record the reasons for not making an external Suspicious Activity Report.

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

Guidance

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

2. Suspicious Activity Reports under Federal Law No. 4 of 2002 should be emailed to the AMLSCU. The dedicated email address and the template for making a Suspicious Activity Report are available on the Regulator's website.

3. In the preparation of a Suspicious Activity Report, 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.

14.4 Suspension of Transaction and No Tipping-off Requirement

14.4.1 A Relevant Person must not carry out Transactions which it knows or suspects or has reasonable grounds for knowing or suspecting to be related to Money Laundering until it has informed the AMLSCU and the Regulator pursuant to Rule 14.3.

Guidance

1. Relevant Persons are reminded that in accordance with Article 16 of 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 Suspicious Activity Report. Relevant Persons should ensure that their Employees are aware of and sensitive to these issues when considering the CDD measures.

14.5 Record-keeping

14.5.1 All relevant details of any internal or external Suspicious Activity Report pursuant to Rules 14.2 and 14.3 must be kept for at least 10 years from the date on which the report was made.

15. GENERAL OBLIGATIONS

15.1 Groups, Branches and subsidiaries

15.1.1 (1) A Relevant Person which is an ADGM Entity must ensure that its policies, procedures, systems and controls required by Rule 6.2.1 apply to:

(a) any of its Branches or Subsidiaries; and

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

(2) Where the regulator 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 Regulator 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 an ADGM 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.

15.1.2 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 15.1.1(2)(b) is met.

Guidance

In relation to an Authorised Person, if the Regulator 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 of the Authorised Person's Financial Services Permission that it must not operate a Branch or Subsidiary in that jurisdiction.

15.2 Group policies

15.2.1 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 CDD 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.

15.3 Notifications

15.3.1 A Relevant Person must inform the Regulator in writing as soon as possible if, in the course of its activities carried on in or from the ADGM 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 or Sanctions regarding enquiries into potential money laundering or terrorist financing or Sanctions breaches;

(b) becomes aware, or has reasonable grounds to believe, that the following has or may have occurred in or through its business:

(a) money laundering, contrary to Federal Law No. 4 of 2002 regarding 'Criminalisation of Money Laundering', Federal Decree Law No. 1 of 2004 regarding 'Combating Terrorism Offences', or Federal Law No. 4 of 2014 regarding 'Combating Terrorist Crimes';

(b) a breach of Sanctions; or

(c) acts amounting to bribery under the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions;

(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 the AML Rulebook 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.

15.3.2 A Relevant Person must inform the Regulator in writing as soon as possible if, in the course of its activities carried on in or from the ADGM, it suspects or becomes aware that another Person outside of its business is engaged in:

(a) money laundering, contrary to Federal Law No. 4 of 2002 regarding 'Criminalisation of Money Laundering', Federal Decree Law No. 1 of 2004 regarding 'Combating Terrorism Offences', or Federal Law No. 4 of 2014 regarding 'Combating Terrorist Crimes';

(b) a breach of Sanctions; or

(c) acts amounting to bribery under the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

This requirement does not apply to information or documents that are legally privileged or in the public domain.

15.4 Record keeping

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

(a) a copy of all documents and information obtained in undertaking initial and on-going CDD or business partners 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 14.2.2;

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

(e) any relevant communications with the AMLSCU;

(f) the documents in Rule 15.4.2; and

(g) the relevant details of any Transaction carried out by the Relevant Person with or for a Customer,

for at least 10 years from the date on which the notification or report was made, the business relationship ends or the Transaction is completed, whichever occurs last.

15.4.2 A Relevant Person must document, and provide to the Regulator on request, any of the following:

(a) the risk assessment of its business undertaken under Rule 6.1.1;

(b) how the assessment in (a) was used for the purposes of complying with Rule 7.2.1(1);

(c) the risk assessment of the Customer undertaken under Rule 7.2.1(1)(a); and

(d) the determination made under Rule 7.2.1(1)(b).

15.4.3 The records maintained by a Relevant Person must be kept in such a manner that:

(a) the Regulator or another competent third party is able to assess the Relevant Person's compliance with legislation applicable in the ADGM;

(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;

(d) all Internal and external Suspicious Activity Reports can be identified; and

(e) the Relevant Person can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

Guidance

1. The records required to be kept under Rule 15.4.1 may be kept in electronic format, provided that such records are readily accessible and available to respond promptly to any Regulator requests for information.

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 Regulator or another competent authority is able to assess the Relevant Person's compliance with legislation applicable in the ADGM;

    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.

15.4.4 Where the records referred to in Rule 15.4.1 are kept by the Relevant Person outside the ADGM, 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 Regulator, ensure that the records are available for inspection within a reasonable period of time.

15.4.5 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 15.4.1 by the Relevant Person, the Regulator 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).

15.4.6 A Relevant Person must be able to demonstrate that it has complied with the training and awareness requirements in Chapter 13 through appropriate measures, including the maintenance of relevant training records.

Guidance

The Regulator considers that "appropriate measures" in Rule 15.4.6 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.

15.5 Annual AML Return

15.5.1 A Relevant Person which is:

(a) an Authorised Person or Recognised Body; or

(b) an auditor,

must complete the AML Return form on an annual basis and retain the AML Return for inspection by the Regulator upon the Regulator's request.

15.6 Communication with the Regulator

15.6.1 A Relevant Person must:

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

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

15.7 Employee disclosures

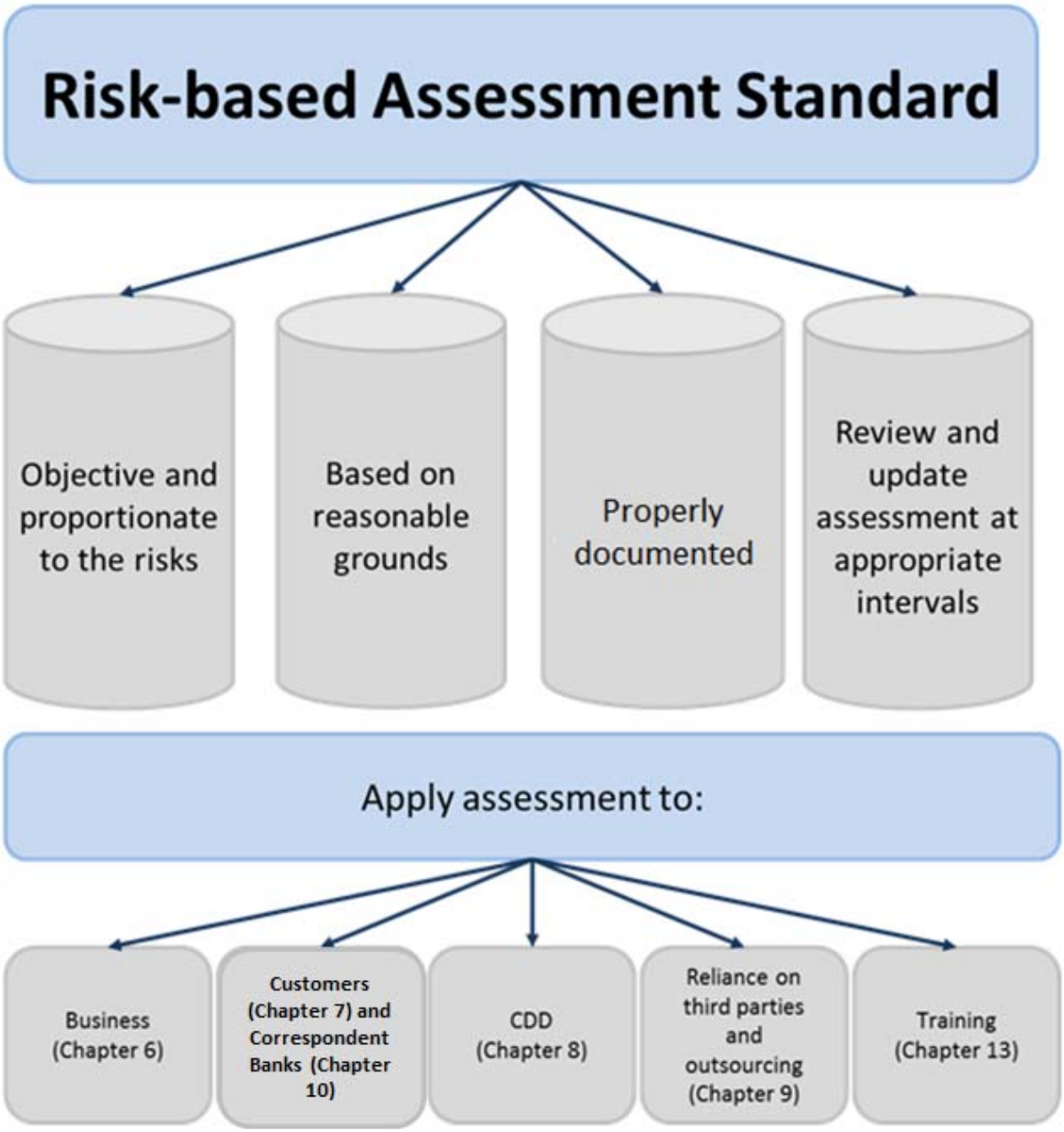
15.7.1 A Relevant Person must ensure that it does not prejudice an Employee who discloses any information regarding money laundering to the Regulator or to any other relevant body involved in the prevention of money laundering.

Guidance

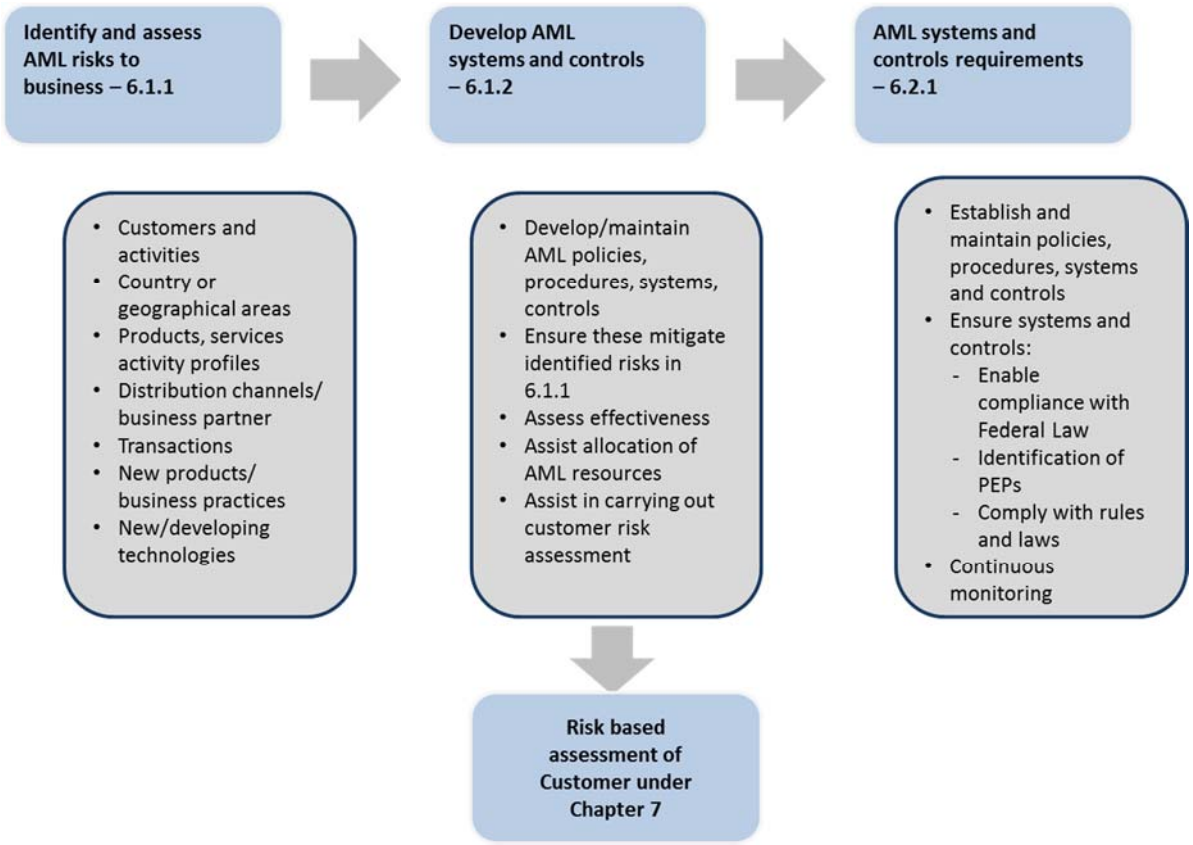
The Regulator considers that "relevant body" in Rule 15.7.1 would include the AMLSCU or another financial intelligence unit, the police, or an Abu Dhabi or Federal ministry.

APP 1 FLOWCHARTS

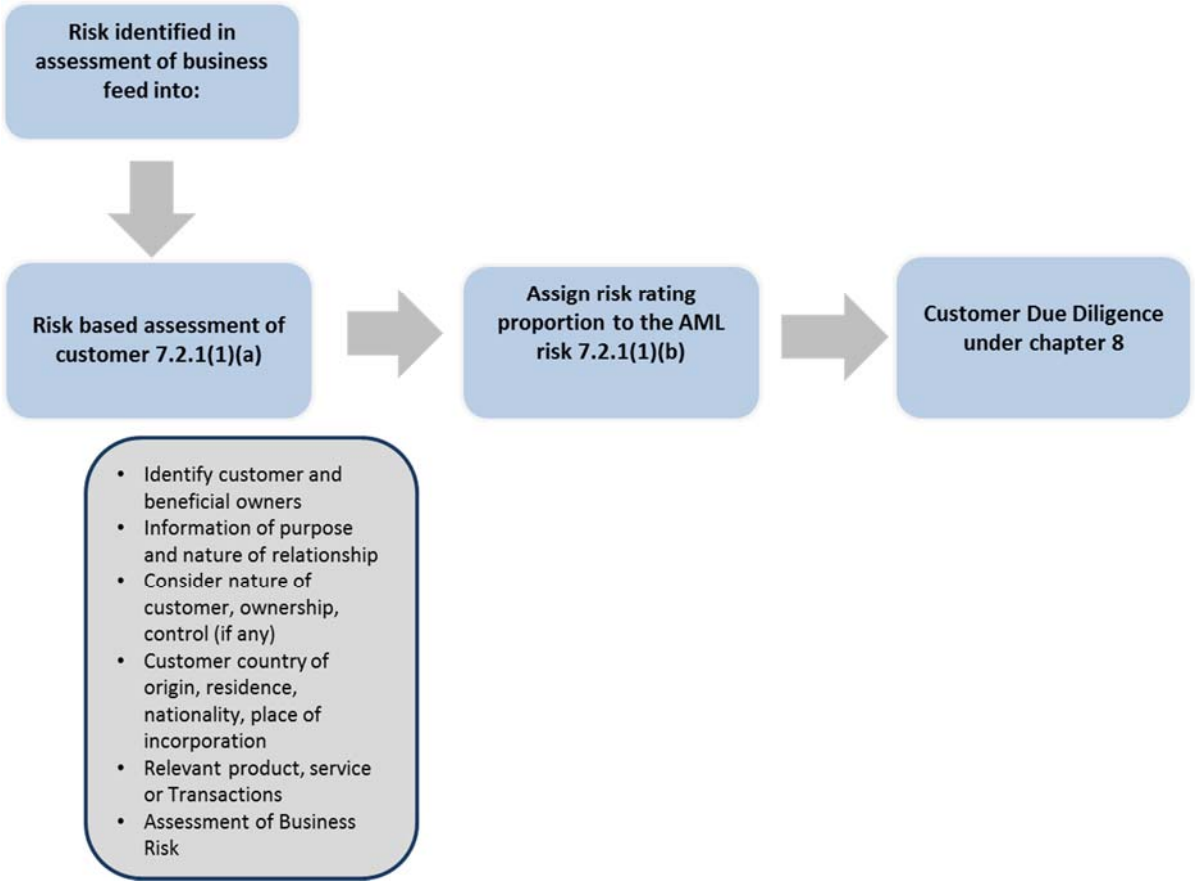
A1.1 Figure 1. The Risk-Based Approach



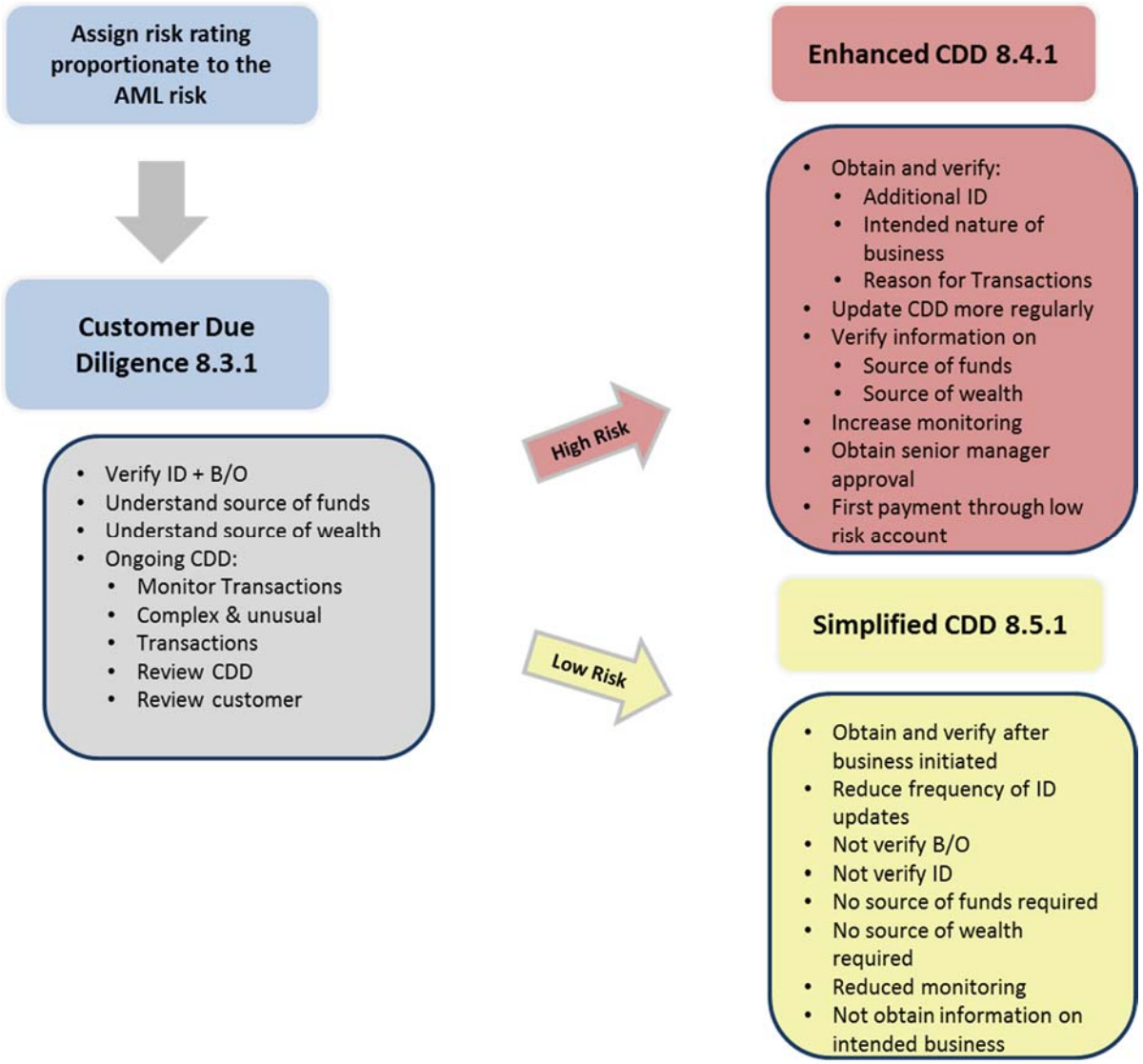
A1.2 Figure 2. Business risk-based assessment



A1.3 Figure 3. Customer risk-based assessment



A1.4 Figure 4. Customer due diligence



A1.5 Figure 5. Reliance and outsourcing of AML compliance.