

Appendix 3

In this Appendix underlining indicates new text and striking through indicates deleted text.



The DFSA Rulebook

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

(AML)

1 INTRODUCTION

1.1 Application

1.1.1 This module (AML) applies to:

- (a) every Relevant Person in respect of all its activities carried on in or from the DIFC;
- (b) the persons specified in Rule 1.2.1 as being responsible for a Relevant Person's compliance with this module; and
- (c) a Relevant Person, which is a DIFC entity, to the extent required by Rule 14.1.

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

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

- (a) an Authorised Firm other than a Credit Rating Agency;
- (b) an Authorised Market Institution;
- (c) a DNFBP; or
- (d) a Registered Auditor.

[This Rule is not being amended but the text is included for reference]

...

3 INTERPRETATION AND TERMINOLOGY

3.1 Interpretation

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

Guidance

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

3.2 Glossary for AML

Guidance

1. ~~A Relevant Person should note that,~~ In order to make this module easier to read, some of the defined terms in this module have not had the initial letter of each word capitalised in the same way as in other Rulebook modules.
2. Some of the defined terms and abbreviations in this module may also be found in the DFSA’s Glossary module (GLO). Where a defined term in this module does not appear in Rule 3.2.1, a Relevant Person should look in GLO to find the meaning. In addition, Rule 9.3.2 of this module sets out definitions relevant to section 9.3 (Electronic fund transfers).
3. In accordance with the interpretation provisions in the Regulatory Law, a reference to legislation includes a reference to the legislation as amended or re-enacted from time to time.

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

...	...
Authorised Person	Means an Authorised Firm or an Authorised Market Institution.
beneficial owner	<p>Means, in relation to a customer a natural person:</p> <p>(a) who ultimately controls, directly or indirectly, a customer;</p> <p>(b) who, in relation to a customer which is a legal person or arrangement, exercises (whether directly or indirectly) ultimate effective control over the person or arrangement, or the management of such person or arrangement;</p> <p>(c) who ultimately owns or has an ownership interest in the customer, whether legally or beneficially, directly or indirectly;</p> <p>(d) on whose behalf or for whose benefit a transaction is being conducted; or</p>

	<p>(e) — on whose instructions the signatories of an account, or any intermediaries instructing such signatories, are for the time being accustomed to act.</p> <p>A person not falling into (a) or (b) is not a beneficial owner by reason of (c) or (d) if, having regard to a risk-based assessment of the customer, the ownership interest is small and in the circumstances poses no or negligible risk of money laundering.</p> <p>In (a) to (e), a reference to a “customer” includes a customer account, customer assets and the underlying legal person or arrangements which constitute or make up the customer, customer account or customer assets.</p>
<u>Beneficial Owner</u>	<p><u>(1) In relation to a customer, means a natural person who ultimately owns or controls the customer or a natural person on whose behalf a transaction is conducted or a business relationship is established, and includes:</u></p> <p><u>(a) in relation to a body corporate, a person referred to in Rule 7.3.3 (2) or (4);</u></p> <p><u>(b) in relation to a foundation, a person referred to in Rule 7.3.5 (2) or (3); and</u></p> <p><u>(c) in relation to a trust or other similar legal arrangement, a person referred to in Rule 7.3.6 (2) or (3).</u></p> <p><u>(2) In relation to a beneficiary of a life insurance or other similar policy, means a natural person who ultimately owns or controls the beneficiary.</u></p>
<u>body corporate</u>	<p><u>Any body corporate, including a limited liability partnership, whether constituted under the law of the DIFC, an Emirate, the State or any other country or territory.</u></p>
Branch	<p>Means a place of business within the DIFC:</p> <p>(a) which has no separate legal personality;</p> <p>(b) which forms a legally dependant part of a Relevant Person whose principal place of business and head office is in a jurisdiction other than the DIFC; and</p> <p>(c) through which the Relevant Person carries on business in or from the DIFC.</p>
Cabinet Resolution No. 38 of 2014	<p>Means Federal Cabinet Resolution No. 38 of 2014 on the Implementing Regulations of Federal Law No. 4 of 2002.</p>
Client	<p>Has the meaning in chapter 2 of the Conduct of Business module.</p>
company service provider	<p>Means a person, not falling into parts (1)(a) to (e) or (g) of the definition of a DNFBP that, by way of business, provides any of the following services to a customer:</p>

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

	<ul style="list-style-type: none"> (a) acting as a formation agent of legal persons; (b) acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; (c) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; or (d) acting as (or arranging for another person to act as) a nominee shareholder for another person.
Contract of Insurance	Has the meaning in GEN Rule A4.1.1.
CTF	Means counter-terrorist financing.
customer	<p>Unless otherwise provided, means:</p> <ul style="list-style-type: none"> (a) a person where, in relation to a business relationship between the person and a Relevant Person, there is a firm intention or commitment by each party to enter into a contractual relationship or where there is a firm commitment by each party to enter into a transaction, in connection with a product or service provided by the Relevant Person; (b) a Client of an Authorised Firm; (c) a Member or prospective Member of, or an applicant for admission of Securities to trading on, an Authorised Market Institution; (d) in relation to a Single Family Office, a member of the Single Family; or (e) a person with whom a Relevant Person is otherwise establishing or has established a business relationship.
Customer Due Diligence (CDD)	Has the meaning in Rule 7.3.1. <u>Means the measures referred to in section 7.3.</u>
...	...
Enhanced Customer Due Diligence	Means undertaking Customer Due Diligence and the enhanced measures under Rule 7.4.1.
FATF	Means the Financial Action Task Force.
FATF Recommendations	Means the publication entitled the "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation" as published and amended from time to time by FATF.
Federal AML	Means all U.A.E Federal Laws and their implementing

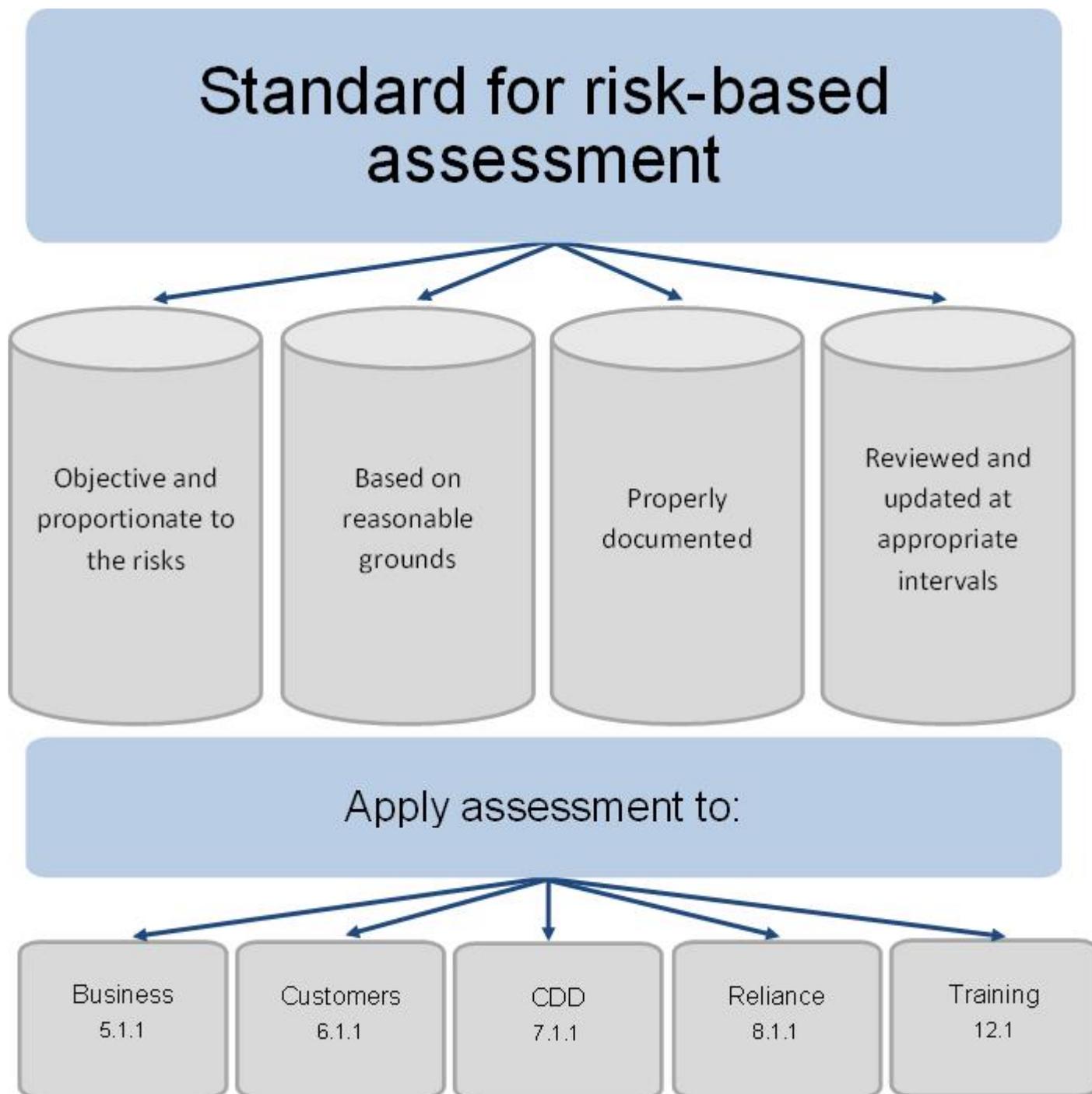
legislation	regulations relating to money laundering, terrorist financing and the financing of unlawful organisations, as well as sanctions compliance, including Federal Law No. 4 of 2002, Federal Law No. 7 of 2014 and Cabinet Resolution No. 38 of 2014.
Federal Law No. 4 of 2002	Means U.A.E Federal Law No. 4 of 2002 on Combating Money Laundering and Terrorist Financing.
Federal Law No. 7 of 2014	Means U.A.E Federal Law No. 7 of 2014 on Combating Terrorism Offences.
...	...
<u>foundation</u>	<u>Means a foundation established under the DIFC Foundations Law 2018 or under any other law.</u>
Governing Body	Means the board of directors, partners, committee of management or other governing body of: (a) a Body Corporate or Partnership; or (b) an unincorporated association carrying on a trade or business, with or without a view to profit.
Group	Means a Group of entities which includes an entity (the 'first entity') and: (a) any parent of the first entity; and (b) any subsidiaries (direct or indirect) of the parent or parents in (a) or the first entity; or (c) for a legal person which is not a body corporate, refers to that person and any other associated legal persons who are in an equivalent relationship to that in (a) and (b).
<u>IMF</u>	<u>The International Monetary Fund.</u>
International Organisation	Means an organisation established by formal political agreement between member countries, where the agreement has the status of an international treaty, and the organisation is recognised in the law of countries which are members.
Law	Means the Regulatory Law.
<u>legal arrangement</u>	<u>Means an express trust or any other similar legal arrangement.</u>
legal person	Means any entity other than a natural person that can establish a customer relationship with a Relevant Person or otherwise own property. This can include companies, bodies corporate or unincorporate, trusts , foundations, anstalten, partnerships, associations, states and governments and other relevantly similar entities.

Member	A person admitted as a member of an Authorised Market Institution in accordance with its Business Rules.
<u>MENAFATF</u>	<u>The Middle East and North Africa Financial Action Task Force.</u>
Money Laundering Reporting Officer (MLRO)	Means the person appointed by a Relevant Person pursuant to Rule 11.2.1(1).
natural person	Means an individual.
<u>OECD</u>	<u>The Organisation for Economic Co-operation and Development.</u>
person	Means a natural or legal person.
Politically Exposed Person (PEP)	Means a natural person (and includes, where relevant, a family member or close associate) who is or has been entrusted with a prominent public function, whether in the State or elsewhere, including but not limited to a head of state or of government, senior politician, senior government, judicial or military official, ambassador, senior person in an International Organisation, senior executive of a state owned corporation, an important political party official, or a member of senior management or an individual who has been entrusted with similar functions such as a director or a deputy director. This definition does not include middle ranking or more junior individuals in the above categories.
Public Listed Company	Has the meaning given in Schedule 1 to the Regulatory Law.
Registered Auditor	Has the meaning given to that term in the Regulatory Law.
Regulated Exchange	Means an exchange regulated by a Financial Services Regulator.
Regulated Financial Institution	A person who does not hold a Licence but who is authorised in a jurisdiction other than the DIFC to carry on any financial service by another Financial Services Regulator.
Relevant Person	Has the meaning given to that term in Rule 1.1.2.
senior management	Means: <u>(1)</u> , in relation to a Relevant Person every member of the Relevant Person's executive management and includes: (a) for a DIFC entity, every member of the Relevant Person's Governing Body; (b) for a Branch, the person or persons who control the

	<p>day to day operations of the Relevant Person in the DIFC and would include, at a minimum, the <u>SEO senior executive officer</u> or equivalent <u>officer</u>, such as the managing director; or</p> <p>(c) for a Registered Auditor, every member of the Relevant Person's executive management in the U.A.E.</p> <p>(2) <u>In relation to a customer that is a body corporate, every member of the body corporate's Governing Body and the person or persons who control the day-to-day operations of the body corporate, including its senior executive officer, chief operating officer and chief financial officer.</u></p>
Shell Bank	A bank that has no physical presence in the country in which it is incorporated or licensed and which is not affiliated with a regulated financial group that is subject to effective consolidated supervision.
Simplified Customer Due Diligence	Means Customer Due Diligence as modified under Rule 7.5.1.
Single Family	Has the meaning given to that term in the DIFC Single Family Office Regulations.
Single Family Office	Has the meaning given to that term in the DIFC Single Family Office Regulations.
source of funds	Means the origin of customer's funds which relate to a transaction or service and includes how such funds are connected to a customer's <u>the source of wealth of a customer or Beneficial Owner.</u>
source of wealth	Means how the customer's global wealth or net worth <u>of a customer or Beneficial Owner</u> is or was acquired or accumulated.
...	...

4 APPLYING A RISK-BASED APPROACH

Figure 1. The Risk-Based Approach (RBA)



4.1 The risk-based approach

4.1.1 A Relevant Person must:

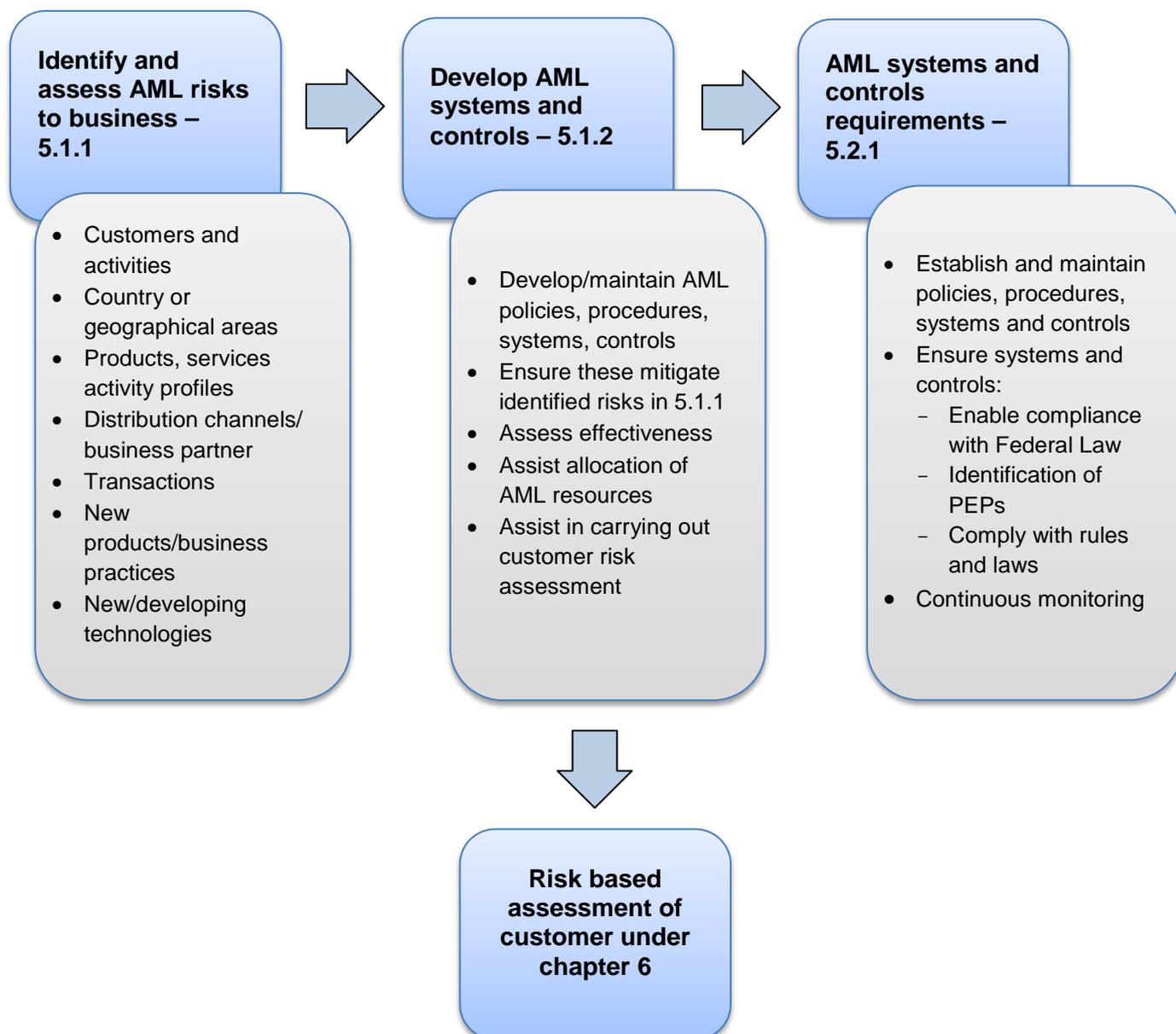
- (a) assess and address its AML risks under this module by reviewing the risks to which the person is exposed as a result of the nature of its business, customers, products, services and any other matters which are relevant in the context of money laundering and then adopting a proportionate approach to mitigate those risks; and
- (b) ensure that, when undertaking any risk-based assessment for the purposes of complying with a requirement of this module, such assessment is:
 - (i) objective and proportionate to the risks;
 - (ii) based on reasonable grounds;
 - (iii) properly documented; and
 - (iv) reviewed and updated at appropriate intervals.

Guidance

1. Rule 4.1.1 requires a Relevant Person to adopt an approach to AML which is proportionate to the risks. This is called the “risk-based approach” (“RBA”) and is illustrated in figure 1 above. The DFSA expects the RBA to be a key part of the Relevant Person’s money laundering compliance culture and to cascade down from the senior management to the rest of the organisation. Embedding the RBA within its business allows a Relevant Person to make decisions and allocate AML resources in the most efficient and effective way.
2. In implementing the RBA, a Relevant Person is expected to have in place processes to identify and assess money laundering risks. After the risk assessment, the Relevant Person is expected to monitor, manage and mitigate the risks in a way that is proportionate to the Relevant Person’s exposure to those money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted.
3. The RBA discourages a “tick-box” approach to AML. Instead a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks. The outcome of using the RBA is akin to using a sliding scale, where the type of CDD undertaken on each customer will ultimately depend on the outcome of the risk-based assessment made of such customer under this chapter.
4. The Rules regarding record-keeping for the purposes of this module are in section 14.4. These Rules apply in relation to Rule 4.1.1(b)(iii).

5 BUSINESS RISK ASSESSMENT

Figure 2. Business risk-based assessment



5.1 Assessing business AML risks

5.1.1 A Relevant Person must:

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

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (i) its type of customers and their activities;
 - (ii) the countries or geographic areas in which it does business;
 - (iii) its products, services and activity profiles;
 - (iv) its distribution channels and business partners;
 - (v) the complexity and volume of its transactions;
 - (vi) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
 - (vii) the use of new or developing technologies for both new and pre-existing products;
- (c) take appropriate measures to ensure that any risk identified as part of the assessment in (a) is taken into account in its day-to-day operations, including in relation to:
- (i) the development of new products, business practices and technologies referred to in Rule 5.1.3;
 - (ii) the taking on of new customers; and
 - (iii) changes to its business profile.

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

- (a) develop and maintain its AML policies, procedures, systems and controls required by Rule 5.2.1;
- (b) ensure that its AML policies, procedures, systems and controls adequately mitigate the risks identified as part of the assessment in Rule 5.1.1;
- (c) assess the effectiveness of its AML policies, procedures, systems and controls as required by Rule 5.2.1(c);
- (d) assist in allocation and prioritisation of AML resources; and
- (e) assist in the carrying out of the customer risk assessment under chapter 6.

New products, business practices and technologies

- 5.1.3** (1) This Rule applies in relation to:
- (a) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and
 - (b) the use of new or developing technologies for both new and existing products.
- (2) Without limiting Rules 5.1.1 and 5.1.2, a Relevant Person must take reasonable steps to ensure that it has:

- (a) assessed and identified the money laundering risks relating to the product, business practice or technology; and
 - (b) taken appropriate steps to manage and mitigate the risks identified under (a),
- before it launches or uses the new product, practice or technology.

Guidance

1. Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, and the nature of the products and services sold.
2. Using the RBA, a Relevant Person should assess its own vulnerabilities to money laundering and take all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers under chapter 6. ~~For instance, if a Relevant Person reasonably concludes that a particular business line poses a negligible risk of money laundering, it may decide, using the RBA, that all its customers in that business line should be treated as posing a lower risk of money laundering, and it may apply Simplified Customer Due Diligence.~~

5.2 AML systems and controls

5.2.1 A Relevant Person must:

- (a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Relevant Person and its activities;
- (b) ensure that its systems and controls in (a):
 - (i) include the provision to the Relevant Person's senior management of regular management information on the operation and effectiveness of its AML systems and controls necessary to identify, measure, manage and control the Relevant Person's money laundering risks;
 - (ii) enable it to determine:
 - (A) whether a customer or a Beneficial Owner is a Politically Exposed Person (PEP); and
 - (B) if it provides a customer with a life insurance or other similar policy, whether a beneficiary of the policy, or a Beneficial Owner of the beneficiary, is a PEP; and
 - (iii) enable the Relevant Person to comply with these Rules and Federal AML legislation; and
- (c) ensure that regular risk assessments are carried out on the adequacy of the Relevant Person's AML systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risk adequately, and are comprehensive and proportionate to the nature, scale and complexity of its activities.

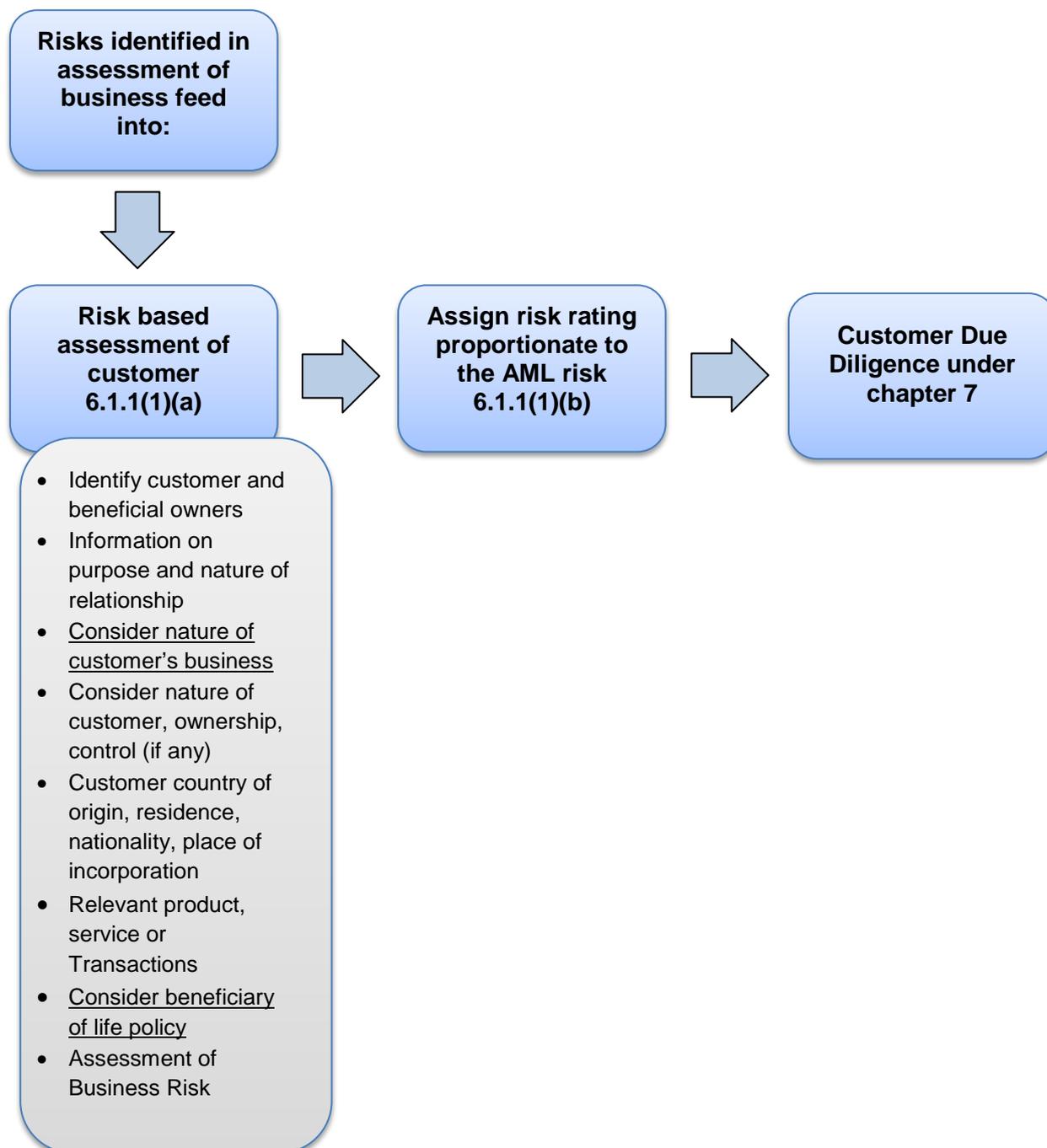
Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

Guidance

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

6 CUSTOMER RISK ASSESSMENT

Figure 3. Customer risk-based assessment



Guidance

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

chapter prescribes the requirements of CDD and of Enhanced CDD for high risk customers and Simplified CDD for low risk customers.

2. CDD in the context of AML refers to the process of identifying a customer, verifying such identification and monitoring the customer's business and money laundering risk on an ongoing basis. CDD is required to be undertaken following a risk-based assessment of the customer and the proposed business relationship, transaction or product.
3. Relevant Persons should note that the ongoing CDD requirements in Rule 7.6.1 require a Relevant Person to ensure that it reviews a customer's risk rating to ensure that it remains appropriate in light of the AML risks.
4. The DFSA is aware that in practice there will often be some degree of overlap between the customer risk assessment and CDD. For example, a Relevant Person may undertake some aspects of CDD, such as identifying a ~~B~~beneficial ~~O~~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~~ An example of such relevant information ~~include information on the source of funds or wealth or is~~ information on the ownership and control structure of the customer. Where information obtained as part of CDD of a customer affects the risk rating of a customer, the change in risk rating should be reflected in the degree of CDD undertaken.

6.1 Assessing customer AML risks

- 6.1.1** (1) A Relevant Person must:
- (a) undertake a risk-based assessment of every customer; and
 - (b) assign the customer a risk rating proportionate to the customer's money laundering risks.
- (2) The customer risk assessment in (1) must be completed prior to undertaking Customer Due Diligence for new customers, and whenever it is otherwise appropriate for existing customers.
- (3) When undertaking a risk-based assessment of a customer under (1)(a) a Relevant Person must:
- (a) identify the customer and any ~~B~~beneficial ~~O~~owner;
 - (b) obtain information on the purpose and intended nature of the business relationship;
 - (c) obtain information on, and take into consideration, the nature of the customer's business;
 - (ca) take into consideration the nature of the customer, its ownership and control structure, and its ~~B~~beneficial ~~O~~ownership (if any);
 - (d) take into consideration the nature of the customer business relationship with the Relevant Person;
 - (e) take into consideration the customer's country of origin, residence, nationality, place of incorporation or place of business;
 - (f) take into consideration the relevant product, service or transaction; and
-

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (fa) if it is providing a customer with a life insurance or other similar policy, take into consideration the beneficiary of the policy and any Beneficial Owner of the beneficiary; and
- (g) take into consideration the outcomes of business risk assessment under chapter 5.

Factors that may indicate higher money laundering risk

- 6.1.2** (1) When assessing if there is a high risk of money laundering in a particular situation, a Relevant Person must take into account, among other things:
- (a) customer risk factors, including whether:
 - (i) the business relationship is conducted in unusual circumstances;
 - (ii) the customer is resident, established or registered in a geographical area of high risk (as set out in paragraph (c));
 - (iii) the customer is a legal person or legal arrangement that is a vehicle for holding personal assets;
 - (iv) the customer is a company that has nominee shareholders or shares in bearer form;
 - (v) the customer is a business that is cash intensive, such as a business that receives a majority of its revenue in cash; and
 - (vi) the corporate structure of the customer is unusual or excessively complex given the nature of the business;
 - (b) product, service, transaction or delivery channel risk factors, including whether:
 - (i) the service involves private banking;
 - (ii) the product, service or transaction is one that might favour anonymity;
 - (iii) the situation involves non face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
 - (iv) payments will be received from unknown or unassociated third parties;
 - (v) new products and new business practices are involved, including new delivery mechanisms or the use of new or developing technologies for both new and pre-existing products; and
 - (vi) the service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in another country; and
 - (c) geographical risk factors, including:
 - (i) countries identified in reports by credible sources, such as mutual evaluations, detailed assessment reports or follow-up reports, as:

- (A) not having effective systems to counter money laundering; or
- (B) not implementing requirements to counter money laundering that are consistent with FATF Recommendations;
 - (ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism, money laundering or the production and supply of illicit drugs;
 - (iii) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations or the State;
 - (iv) countries providing funding or support for terrorism; and
 - (v) countries that have organisations operating within their territory that have been designated by the State, other countries or International Organisations as terrorist organisations.
- (2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.
- (3) When assessing the risk factors referred to in (1), Relevant Persons must bear in mind that the presence of one or more risk factors may not always indicate a high risk of money laundering in a particular situation.

Factors that may indicate lower money laundering risk

- 6.1.3** (1) When assessing if there is a low risk of money laundering in a particular situation, a Relevant Person must take into account, among other things:
- (a) customer risk factors, including whether the customer is:
 - (i) a public body or a publicly owned enterprise;
 - (ii) resident, established or registered in a geographical area of lower risk (as set out in paragraph (c));
 - (iii) an Authorised Person;
 - (iv) a Regulated Financial Institution that is subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations that are equivalent to the standards set out in the FATF Recommendations;
 - (v) a Subsidiary of a Regulated Financial Institution referred to in (iv), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent;
 - (vi) a company whose Securities are listed by the DFSA, another Financial Services Regulator or a Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules;

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (vii) a law firm, notary firm or other legal business that carries on its business in or from the DIFC; and
 - (viii) an accounting firm, insolvency firm, Registered Auditor or other audit firm that carries on its business in or from the DIFC;
 - (b) product, service, transaction or delivery channel risk factors, including whether the product or service is:
 - (i) a Contract of Insurance that is non-life insurance;
 - (ii) a Contract of Insurance that is a life insurance product with no investment return or redemption or surrender value;
 - (iii) an insurance policy for a pension scheme that does not provide for an early surrender option and cannot be used as collateral;
 - (iv) a Contract of Insurance which is a reinsurance contract that is ceded by an insurer who is a Regulated Financial Institution;
 - (v) a pension, superannuation or similar scheme that satisfies the following conditions:
 - (A) the scheme provides retirement benefits to employees;
 - (B) contributions to the scheme are made by way of deductions from wages; and
 - (C) the scheme rules do not permit the assignment of a member's interest under the scheme; and
 - (vi) a product where the risks of money laundering are adequately managed by other factors such as transaction limits or transparency of ownership; and
 - (c) geographical risk factors, including whether:
 - (i) a country has been identified by credible sources as having effective systems to counter money laundering;
 - (ii) a country is identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism, money laundering, or the production and supply of illicit drugs; and
 - (iii) on the basis of reports by credible sources, such as mutual evaluations, detailed assessment reports or follow-up reports, a country:
 - (A) has requirements to counter money laundering that are consistent with the FATF Recommendations; and
 - (B) effectively implements those Recommendations.
- (2) For the purposes of (1)(c), a credible source includes, but is not limited to, FATF, the IMF, the World Bank, the OECD and other International Organisations.
- (3) When assessing the risk factors referred to in (1), Relevant Persons must bear in mind that the presence of one or more risk factors may not always indicate a low risk of money laundering in a particular situation.

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

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

Shell Banks

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

Anonymous or fictitious accounts

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

Use of numbered or abbreviated accounts for internal purposes

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

- (a) such an account is used only for internal purposes;
- (b) it has undertaken the same Customer Due Diligence procedures in relation to the account holder as are required for other account holders;
- (c) it maintains the same information in relation to the account and account holder as is required for other accounts and account holders; and
- (d) staff performing AML functions, including staff responsible for identifying and monitoring transactions for suspicious activity, and staff performing compliance and audit functions, have full access to information about the account and the account holder.

Guidance on the customer risk assessment

- ~~1. In assessing the nature of a customer, a Relevant Person should consider such factors as the legal structure of the customer, the customer's business or occupation, the location of the customer's business and the commercial rationale for the customer's business model.~~
- ~~2. In assessing the customer business relationship, a Relevant Person should consider how the customer is introduced to the Relevant Person and how the customer is serviced by the Relevant Person, including for example, whether the Person will be a private banking customer, will open a bank account or whether the business relationship will be purely advisory.~~
13. The risk assessment of a customer, which is illustrated in figure 3 above, requires a Relevant Person to allocate an appropriate risk rating to every customer. The DFSA would expect risk ratings to be either descriptive, such as "low", "medium" or "high", or a sliding numeric scale such as 1 for the lowest risk to 10 for the highest. Depending on the outcome of a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

to what degree CDD will need to be performed. For a high risk customer, the Relevant Person will need to undertake Enhanced CDD under section 7.4 as well as the normal CDD set out in section 7.3. For a low risk customer, the Relevant Person may be able to undertake Simplified CDD in accordance with section 7.5. For any other customer, the Relevant Person will be required to undertake the normal CDD set out in section 7.3.

24. Using the RBA, a Relevant Person could, when assessing two customers with near identical risk profiles, consider that one is high risk and the other low risk. This may occur, for example, where both customers may be from the same high risk country, but one customer may be a customer in relation to a low risk product or may be a long-standing customer of a Group company who has been introduced to the Relevant Person.
35. In Rule 6.1.42, ownership arrangements which may prevent the Relevant Person from identifying one or more Beneficial Owners include bearer shares and other negotiable instruments in which ownership is determined by possession.

Guidance on the term “customer”

46. The point at which a person becomes a customer will vary from business to business. However, the DFSA considers that it would usually occur at or prior to the business relationship being formalised, for example, by the signing of a customer agreement or the acceptance of terms of business.
57. The DFSA does not consider that a person would be a customer of a Relevant Person merely because such person receives marketing information from a Relevant Person or where a Relevant Person refers a person who is not a customer to a third party (including a Group member).
68. The DFSA considers that a counterparty would generally be a “customer” for the purposes of this module and would therefore require a Relevant Person to undertake CDD on such a person. However, this would not include a counterparty in a transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ordinary business services, for consumption by the Relevant Person such as cleaning, catering, stationery, IT or other similar services.
79. A Representative Office should not have any customers in relation to its DIFC operations.

Guidance on high risk customers

10. ~~In complying with Rule 6.1.1, the DFSA considers that a Relevant Person should consider the following factors, which may indicate that a customer poses a higher risk of money laundering:~~
 - a. ~~the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the location of the Relevant Person and the customer);~~
 - b. ~~legal persons or arrangements that are personal investment vehicles;~~
 - c. ~~companies that have nominee shareholders or directors or shares in bearer form;~~
 - d. ~~businesses that are cash intensive;~~
 - e. ~~the ownership structure of the legal person appears unusual or excessively complex given the nature of the legal person’s business or activities;~~
 - f. ~~countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow up reports, as not having adequate AML systems;~~

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- ~~g. countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations Security Council or identified by credible sources as having significant levels of corruption or other criminal activity;~~
- ~~h. countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;~~
- ~~i. a person not meeting the definition of a PEP but whose high profile or influence poses an elevated risk of corruption;~~
- ~~j. anonymous transactions (which may include cash);~~
- ~~k. private banking relationships;~~
- ~~l. non face to face business relationships or transactions;~~
- ~~m. payment received from unknown or un-associated third parties;~~
- ~~n. discretionary trusts; and~~
- ~~o. charitable trusts and waqfs.~~

Guidance on low risk customers

11. In complying with Rule 6.1.1, the DFSA considers that the following types of customers may pose a lower risk of money laundering:
- ~~a. an Authorised Firm;~~
 - ~~b. an Authorised Market Institution;~~
 - ~~c. a Regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF recommendations;~~
 - ~~d. a Subsidiary of a Regulated Financial Institution referred to in (c), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent;~~
 - ~~e. a law firm, notary firm, or other independent legal business that carries on its business in or from the DIFC;~~
 - ~~f. an accounting firm, Registered Auditor or other audit firm or insolvency firm that carries on its business in or from the DIFC;~~
 - ~~g. a person carrying on a business in another jurisdiction that is equivalent to the businesses specified in (e) or (f) if:

 - ~~(i) the jurisdiction has AML regulations which are equivalent to the standards set out in the FATF Recommendations; and~~
 - ~~(ii) the person's entire operations are subject to AML regulation and supervision by a competent authority;~~~~
 - ~~h. a company whose Securities are listed on a Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules;~~
 - ~~i. a government body or a non-commercial government entity in the State or a FATF member country; and~~

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- ~~j. a customer where the business relationship is limited to providing one or more of the following products or services:

 - ~~(i) a Contract of Insurance which is non life insurance;~~
 - ~~(ii) a Contract of Insurance which is a life insurance product with no investment return or redemption or surrender value;~~
 - ~~(iii) a Contract of Insurance which is life insurance where the annual premium is no more than \$1,000 or where a single premium of no more than \$2,500 is paid;~~
 - ~~(iv) a Contract of Insurance for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral;~~
 - ~~(v) a Contract of Insurance which is a reinsurance contract not falling into (i) to (iv) which is ceded by an insurer who is a Regulated Financial Institution;~~
 - ~~(vi) a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an Employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme; or~~
 - ~~(vii) arbitration, litigation or advice on litigation prospects.~~~~
- ~~12. The assignment of a low risk customer AML rating should not be automatic and should be applied only after an assessment of a customer's actual AML risk as required in AML Rule 6.1.1. In conducting this assessment, however, Relevant Persons may wish to make use of, and build upon, the risk assessments it has conducted under Rule 5.1.1.~~

Guidance on Shell Banks

- ~~813. Rule 6.1.35 prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank. A Shell Bank is a bank that has no physical presence in the country in which it is incorporated or licensed, and is not affiliated with a regulated financial Group that is subject to effective consolidated supervision. The DFSA does not consider that the existence of a local agent or low level staff constitutes physical presence.~~

Guidance on fictitious and anonymous accounts

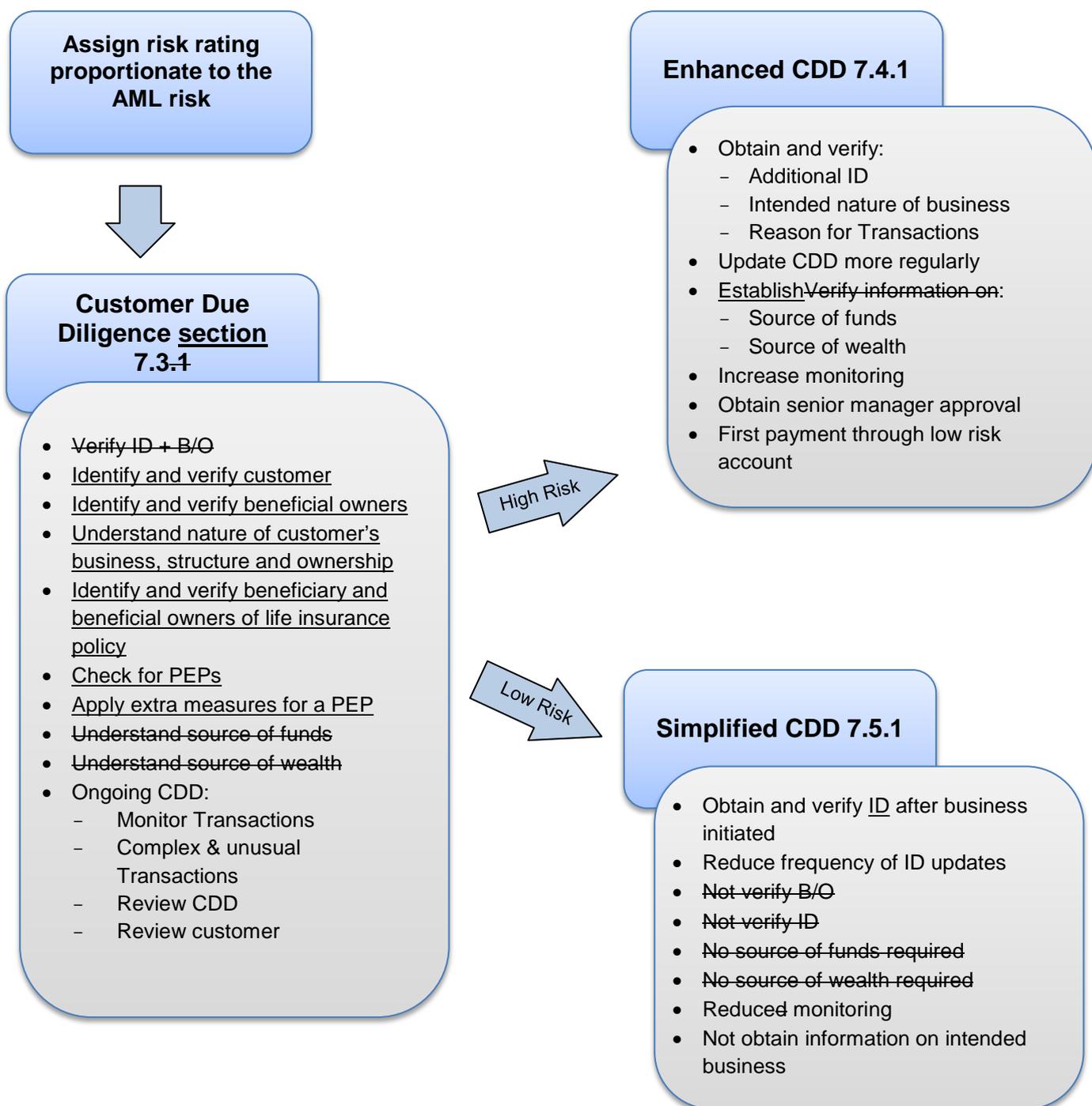
- ~~914. A Relevant Person should note that, in addition to the prohibition in Rule 6.1.46 against establishing anonymous or fictitious accounts or accounts for unknown persons, the Federal AML legislation also prohibits the opening of accounts held under borrowed, mock or fake names or with numbers without the names of account holders.~~
- ~~15. A Relevant Person may internally use a numbered account or an account with an abbreviated name. However, it must ensure that the account holder is subject to the same customer due diligence procedures as apply to all other account holders. Also, it should ensure that the identity of the account holder is known to a sufficient number of its staff, and that staff performing AML, compliance, audit and other oversight functions have full access to information about the account holder. Finally, a numbered account or an account with an abbreviated name should only be used for internal purposes.~~

Guidance on Tax Issues

1046. A Relevant Person should, when carrying out a customer risk assessment, consider and assess the tax crime risk associated with the customer and factor such risks into the overall risk assigned to that customer. Many of the factors described in ~~Guidance item 10~~ Rule 6.1.2 on higher risk customers could also be an indicator of potential tax crimes. For example, the use of complex or unusual corporate structures, the customer's business not being located where the customer lives (without adequate explanation), unusual customer interface, or reluctance by the customer to communicate directly with the Relevant Person ~~or the customer being unable or unwilling to disclose the source of funds and wealth.~~
1147. If it is justified based on the risk assessment and where concerns arise, a Relevant Person may wish to seek comfort from its customers by obtaining disclosures or declarations to ascertain if a legitimate explanation exists for the concerns and therefore to allay those concerns.

7 CUSTOMER DUE DILIGENCE

Figure 4. CDD



7.1 Requirement to undertake customer due diligence

- 7.1.1** (1) A Relevant Person must:
- (a) undertake Customer Due Diligence under section 7.3 ~~Rule 7.3.1~~ for each of its customers; and
 - (b) in addition to (a), undertake Enhanced Customer Due Diligence under Rule 7.4.1 in respect of any customer it has assigned as high risk.
- (2) A Relevant Person may undertake Simplified Customer Due Diligence in accordance with Rule 7.5.1 by modifying Customer Due Diligence under section 7.3 ~~Rule 7.3.1~~ for any customer it has assigned as low risk.

Guidance

A Relevant Person should undertake CDD in a manner proportionate to the customer's money laundering risks identified under Rule 6.1.1(1). This means that all customers are subject to CDD under section 7.3 ~~Rule 7.3.1~~. However, for high risk customers, additional Enhanced CDD measures should also be undertaken under section 7.4 ~~Rule 7.4.1~~. For low risk customers, section 7.3 ~~Rule 7.3.1~~ may be modified according to the risks in accordance with section 7.5 ~~Rule 7.5.1~~.

7.2 Timing of customer due diligence

- 7.2.1** (1) A Relevant Person must, except as otherwise provided in Rule 7.2.2 or in section 7.3:
- (a) undertake the appropriate Customer Due Diligence under Rule 7.3.1(1)(a) to (c) and section 7.3 when it is establishing a business relationship with a customer; and
 - (b) undertake the appropriate Customer Due Diligence under Rule 7.3.1(1)(d) after establishing a business relationship with a customer.
- (2) A Relevant Person must also undertake appropriate Customer Due Diligence if, at any time:
- (a) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of Customer Due Diligence;
 - (b) it suspects money laundering in relation to a person; or
 - (c) there is a change in risk-rating of the customer, or it is otherwise warranted by a change in circumstances of the customer.

Establishing a business relationship before verification

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

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (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 (24), 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.
- (24) Where a Relevant Person is not reasonably able to comply with the 30 day requirement in (13)(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 (13) as soon as possible; and
 - (c) record the non-compliance event in its annual AML Return.
- (35) The DFSA may specify a period within which a Relevant Person must complete the verification required by (13) failing which the DFSA may direct the Relevant Person to cease any business relationship with the customer.
- (4) A Relevant Person must ensure that its AML systems and controls referred to in Rule 5.2.1 include risk management policies and procedures concerning the conditions under which business relationships may be established with a customer before completing verification.

Guidance

1. For the purposes of Rule 7.2.1(2)(a), examples of situations which might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained could be where there is a suspicion of money laundering in relation to that customer, where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Relevant Person that a person other than the customer is the real customer.
2. In Rule 7.2.24(31)(a), situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period or executing a time critical transaction, which if not executed immediately, would or may cause a customer to incur a financial loss due to price movement or loss of opportunity or when a customer seeks immediate insurance cover.
3. When complying with Rule 7.2.1, a Relevant Person should also, where relevant, consider Rule 7.7.1 regarding failure to conduct or complete CDD and chapter 13 regarding SARs and tipping off.

4. For the purposes of Rule 7.2.24(31)(d), the DFSA considers that in most situations as soon as reasonably practicable would be within 30 days after the establishment of a business relationship. However, it will depend on the nature of the customer business relationship.

7.3 Customer due diligence requirements

- 7.3.1** ~~(1) In undertaking Customer Due Diligence required by Rule 7.1.1(1)(a) a Relevant Person must:~~
- ~~(a) verify the identity of the customer and any beneficial owner on the basis of original or properly certified documents, data or information issued by or obtained from a reliable and independent source;~~
 - ~~(b) understand the customer's source of funds;~~
 - ~~(c) understand the customer's source of wealth; and~~
 - ~~(d) undertake on-going due diligence of the customer business relationship under Rule 7.6.1.~~
- ~~(2) In complying with (1)(a) for life insurance or other similar policies, a Relevant Person must:~~
- ~~(a) verify the identity of any named beneficiaries of the insurance policy; and~~
 - ~~(b) verify the identity of the persons in any class of beneficiary, or where these are not identifiable, ensure that it obtains sufficient information to be able to verify the identity of such persons at the time of payout of the insurance policy.~~
- ~~(3) Where a customer, or a beneficial owner of the customer, is a Politically Exposed Person, a Relevant Person must ensure that, in addition to (1) it also:~~
- ~~(a) increases the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious ; and~~
 - ~~(b) obtains the approval of senior management to commence a business relationship with the customer.~~

Undertaking customer due diligence

- 7.3.1** (1) In undertaking Customer Due Diligence required by Rule 7.1.1(1)(a) a Relevant Person must:
- (a) identify the customer and verify the customer's identity;
 - (b) identify any Beneficial Owners of the customer and take reasonable measures to verify the identity of the Beneficial Owners, so that the Relevant Person is satisfied that it knows who the Beneficial Owners are;

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (c) if the customer is a legal person or legal arrangement, take reasonable measures to understand the nature of the customer's business and its ownership and control structure; and
 - (d) undertake on-going due diligence of the customer business relationship under Rule 7.6.1.
 - (2) If a person ("A") purports to act on behalf of the customer, the Relevant Person must, in addition to (1)(a):
 - (a) verify that A is authorised to act on the customer's behalf; and
 - (b) identify A and verify A's identity.
 - (3) The verification under (1) and (2) must be based on reliable and independent source documents, data or information.

Identifying and verifying the customer

7.3.2

- (1) For the purposes of Rule 7.3.1(1)(a), a Relevant Person must identify a customer and verify the customer's identity in accordance with this Rule.
 - (2) If a customer is a natural person, a Relevant Person must obtain and verify information about the person's:
 - (a) full name (including any alias);
 - (b) date of birth;
 - (c) nationality;
 - (d) legal domicile; and
 - (e) current residential address (other than a post office box).
 - (3) If a customer is a body corporate, the Relevant Person must obtain and verify:
 - (a) the full name of the body corporate and any trading name;
 - (b) the address of its registered office and, if different, its principal place of business;
 - (c) the date and place of incorporation or registration;
 - (d) a copy of the certificate of incorporation or registration;
 - (e) the articles of association or other equivalent governing documents of the body corporate; and
 - (f) the full names of its senior management.
 - (4) If a customer is a foundation, the Relevant Person must obtain and verify:
 - (a) a certified copy of the charter and by-laws of the foundation or any other documents constituting the foundation; and
 - (b) documentary evidence of the appointment of the guardian or any other person who may exercise powers in respect of the foundation.
-

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (5) If a customer is an express trust or other similar legal arrangement, the Relevant Person must obtain and verify:
- (a) a certified copy of the trust deed or other documents that set out the nature, purpose and terms of the trust or arrangement; and
 - (b) documentary evidence of the appointment of the trustee or any other person exercising powers under the trust or arrangement.

Identifying and verifying beneficial owners: body corporate

- 7.3.3** (1) If a customer is a body corporate, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.
- (2) The Relevant Person must identify:
- (a) the natural persons who ultimately have a controlling ownership interest in the body corporate, whether legal or beneficial, direct or indirect; and
 - (b) if there is any doubt about whether the natural persons identified under (a) exert control through ownership interests, or if no natural person exerts control through ownership interests, the natural persons exercising control of the body corporate through other means.
- (3) A Relevant Person does not have to identify an ownership interest under (2)(a) if, having regard to a risk-based assessment of the customer, it is reasonably satisfied that the ownership interest is minor and in the circumstances poses no or negligible risk of money laundering.
- (4) If a Relevant Person has exhausted all possible means but has not been able to identify the Beneficial Owners under (2), and provided it has no grounds for suspecting money laundering, it must treat the senior management of the body corporate as the Beneficial Owners.
- (5) If (4) applies, the Relevant Person must keep a record in writing of all the actions it has taken to identify the Beneficial Owners of the body corporate.

Guidance

1. In exceptional circumstances, a Relevant Person may not be able to identify any natural person as the ultimate owner or controller of a body corporate. In such a case, provided it has exhausted all other means of identifying the owner or controller and it has no grounds for suspecting money laundering, it can treat each of the members of the senior management of the body corporate as the Beneficial Owners (see Rule 7.3.3(4)). However, in such a case the Relevant Person will need to keep records of all the actions it has taken to identify the Beneficial Owners (see Rule 7.3.3(5)).
2. If the ownership or control arrangements of a customer are of such a nature that the Relevant Person is prevented from identifying the Beneficial Owners (for example, if Beneficial Owners hold bearer shares or other negotiable instruments and there is no effective system for recording the current holder of the shares or instruments), the Relevant Person is prohibited from establishing a business relationship with the customer under Rule 6.1.4.
3. For more detailed Guidance on identifying and verifying Beneficial Owners, see the guidance on CDD at the end of section 7.3.

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

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

- (a) a body corporate that:
 - (i) has its Securities listed by the DFSA, another Financial Services Regulator or a Regulated Exchange; and
 - (ii) is subject to disclosure requirements which ensure that adequate information about its business, structure and beneficial ownership is publicly available; or
- (b) a majority-owned subsidiary of a body corporate referred to in (a).

Identifying and verifying beneficial owners: foundations

- 7.3.5** (1) If a customer is a foundation, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.
- (2) The Relevant Person must identify the founder, guardian, contributors, qualified recipients, other persons entitled to receive any property or income from the foundation and any other natural person who exercises ultimate effective control of the foundation.
- (3) If the qualified recipients, or other persons entitled to receive property or income from a foundation, are designated by characteristics or by class, the Relevant Person must obtain sufficient information to satisfy itself that it will be able to establish the identity of the qualified recipient or other person before it makes any payment or transfer of property to the recipient or person.
- (4) The Relevant Person must verify the identity of a qualified recipient or other person referred to in (3) before it makes any payment, or transfers any property, from the foundation to that recipient or person.

Identifying and verifying beneficial owners: trusts and similar arrangements

- 7.3.6** (1) If a customer is a legal arrangement, a Relevant Person must identify and verify the Beneficial Owners under Rule 7.3.1(1)(b) in accordance with this Rule.
- (2) The Relevant Person must identify:
- (a) for a trust, the settlor, trustee, protector, enforcer, beneficiaries and any other natural person who exercises ultimate effective control over the trust; and
 - (b) for other types of legal arrangements, persons in equivalent or similar positions to those persons referred to in (a).
- (3) If the beneficiaries of a trust or arrangement are designated by characteristics or by class, the Relevant Person must obtain sufficient information about the beneficiaries to satisfy itself that it will be able to establish the identity of a beneficiary:
- (a) before it makes a distribution to the beneficiary; or
 - (b) when the beneficiary intends to exercise vested rights.

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

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

Identifying and verifying beneficiary of a life insurance policy

- 7.3.7**
- (1) This Rule applies if a Relevant Person is providing a customer with a life insurance or other similar policy.
- (2) The Relevant Person must, in addition to complying with Rule 7.3.1:
- (a) if a beneficiary is specifically named in the policy, record the name of that person; and
- (b) if the beneficiaries of the policy are designated by characteristics or by class, obtain sufficient information to satisfy itself that it will be able to establish the identity of the beneficiaries when any payment is due to be made under the policy.
- (3) The Relevant Person must undertake the measures referred to in (2) as soon as the beneficiary of the policy is identified or designated.
- (4) The Relevant Person must verify the identity of beneficiaries and any Beneficial Owners of a beneficiary before it makes a payout under the policy.

Guidance

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

Politically Exposed Persons: other measures

- 7.3.8**
- (1) A Relevant Person must take reasonable measures to determine:
- (a) if a customer, or a Beneficial Owner of a customer, is a Politically Exposed Person (PEP); and
- (b) for a life insurance or other similar policy, if a beneficiary of the policy, or a Beneficial Owner of a beneficiary, is a PEP.
- (2) If a customer, or a Beneficial Owner of a customer, is a PEP, a Relevant Person must:
- (a) obtain the approval of senior management to commence or continue the business relationship with the customer;
- (b) take reasonable measures to establish the source of wealth and source of funds of the customer or Beneficial Owner; and
- (c) increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (3) If a beneficiary of a life insurance or other similar policy, or a Beneficial Owner of a beneficiary, is a PEP, a Relevant Person must:
- (a) obtain the approval of senior management to make any payout under the policy;
 - (b) take reasonable measures to establish the source of wealth and source of funds of the beneficiary or Beneficial Owner of the beneficiary; and
 - (c) increase the degree and nature of monitoring of its business relationship with the policyholder, to determine whether the customer's transactions or activities appear unusual or suspicious.
- (4) A Relevant Person must carry out the additional Customer Due Diligence referred to in (3) before it makes any payout under the policy.

Guidance on CDD

1. ~~A Relevant Person should, in complying with Rule 7.3.1(1)(a), and adopting the RBA, obtain, verify and record, for every customer who is a natural person, the following identification information:~~
 - a. ~~full name (including any alias);~~
 - b. ~~date of birth;~~
 - c. ~~nationality;~~
 - d. ~~legal domicile; and~~
 - e. ~~current residential address (not a P.O. box).~~
12. Items (a) to (c) ~~in Rule 7.3.2(2) above~~ should be obtained from a current valid passport or, where a customer does not possess a passport, an official identification document which includes a photograph. The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties or which is his place of origin.
3. ~~A Relevant Person should, in complying with Rule 7.3.1(1)(a), and adopting the RBA, obtain, verify and record, for every customer which is a legal person, the following identification information:~~
 - a. ~~full business name and any trading name;~~
 - b. ~~registered or business address;~~
 - c. ~~date of incorporation or registration;~~
 - d. ~~place of incorporation or registration;~~
 - e. ~~a copy of the certificate of incorporation or registration;~~
 - f. ~~a valid commercial or professional licence;~~
 - g. ~~the identity of the directors, partners, trustees or equivalent persons with executive authority of the legal person; and~~

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- h. ~~for a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust and documentary evidence of the appointment of the current trustees.~~
24. Under Rule 7.3.1(3), a Relevant Person is required to verify the identity of a person based on reliable and independent source documents, data or information. A Relevant Person should generally have sight of original identification documents and retain a copy of the identification document. However in complying with Rule 7.3.1(4)(a), it may not always be possible to obtain original documents. Where identification documents cannot be obtained in original form, for example, because a Relevant Person has no physical contact with the customer, the Relevant Person should obtain a copy certified as a true copy by a person of good standing such as a registered lawyer or notary, a chartered accountant, a bank manager, a police officer, an Employee of the person's embassy or consulate, or other similar person. The DFSA considers that downloading publicly-available information from an official source (such as a regulator's or other official government website) is sufficient to satisfy the requirements of Rule 7.3.1(4)(a). The DFSA also considers that CDD information and research obtained from a reputable company or information-reporting agency may also be acceptable as a reliable and independent source as would banking references and, on a risk-sensitive basis, information obtained from researching reliable and independent public information found on the internet or on commercial databases.
35. For higher risk situations the DFSA would expect identification information to be independently verified, using both public and non-public sources. For lower risk situations, not all of the relevant identification information would need to be verified.
6. ~~In complying with Rule 7.3.1(1)(b), a Relevant Person is required to "understand" a customer's source of funds. This process involves understanding where the funds for a particular service or transaction will come from (e.g. a specific bank account held with a specific financial institution) and whether that funding is consistent with the customer's source of wealth. The best way of understanding the source of funds is by obtaining information directly from the customer, which will usually be obtained during the on boarding process. The Relevant Person should keep appropriate evidence of how they were able to understand the source of funds, for example, a copy of the customer account opening form, customer questionnaire or a memo of a call with the relationship manager at a financial institution.~~
7. ~~In complying with Rule 7.3.1(1)(c), a Relevant Person is required to "understand" a customer's source of wealth. For a natural person, this might include questions about the source of wealth in an application form or customer questionnaire. The understanding may also be gained through interactions with the relationship manager at a financial institution. It could also be gained by obtaining information from a reliable and independent publicly available source, for example, from published accounts or a reputable news source. The understanding need not be a dollar for dollar account of the customer's global wealth, but it should provide sufficient detail to give the Relevant Person comfort that the customer's wealth is legitimate and also to provide a base line for subsequent ongoing due diligence. The understanding of the customer's source of wealth should be clearly documented.~~
8. ~~Understanding a customer's source of funds and wealth is also important for the purposes of undertaking ongoing due diligence under Rule 7.3.1(1)(d). Initial funding of an account or investments from an unknown or unexpected source may pose a money laundering risk. Similarly, a sound understanding of the customer's source of funds and wealth also provides useful information for a Relevant Person's transaction monitoring programme.~~
9. ~~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 identification and verification of Beneficial Owners

410. 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" "minor" ownership interest for the purposes of the definition of a Beneficial Owner in Rule

7.3.3 will depend on the individual circumstances of the customer. The DFSA considers that the question of whether an ownership interest is ~~small~~ minor should be considered in the context of the Relevant Person's knowledge of the customer and the customer risk assessment and the risk of money laundering.

544. When identifying Beneficial Owners, a Relevant Person is expected to adopt a substantive (as opposed to form over substance) approach to CDD for legal persons. Adopting a substantive approach means focusing on the money laundering risks of the customer and the product/service and avoiding an approach which focusses purely on the legal form of an arrangement or sets fixed percentages at which Beneficial Owners are identified (or not). It should take all reasonable steps to establish and understand a corporate customer's legal ownership and control and to identify the Beneficial Owner. The DFSA does not set explicit ownership or control thresholds in defining the Beneficial Owner because the DFSA considers that the applicable threshold to adopt will ultimately depend on the risks associated with the customer, and so the DFSA expects a Relevant Person to adopt the RBA and justify on reasonable grounds an approach which is proportionate to the risks identified. A Relevant Person should not set fixed thresholds for identifying the Beneficial Owner without objective and documented justification as required by Rule 4.1.1. An overly formal approach to defining the Beneficial Owner may result in a criminal "gaming" the system by always keeping his financial interest below the relevant threshold.
642. The DFSA considers that in some circumstances no threshold should be used when identifying Beneficial Owners because it may be important to identify all underlying Beneficial Owners in order to ensure that they are not associated or connected in some way. This may be appropriate where there are a small number of investors in an account or fund, each with a significant financial holding and the customer-specific risks are higher. However, where the customer-specific risks are lower, a threshold can be appropriate. For example, for a low-risk corporate customer which, combined with a lower-risk product or service, a percentage threshold may be appropriate for identifying "control" of the legal person for the purposes of the definition of a Beneficial Owner.
743. For a retail investment fund which is widely-held and where the investors invest via pension contributions, the DFSA would not expect the manager of the fund to look through to any underlying investors where there are none with any material control or ownership levels in the fund. However, for a closely-held fund with a small number of investors, each with a large shareholding or other interest, the DFSA would expect a Relevant Person to identify and verify each of the Beneficial Owners, depending on the risks identified as part of its risk-based assessment of the customer. For a corporate health policy with defined benefits, the DFSA would not expect a Relevant Person to identify the Beneficial Owners.
14. ~~Where a Relevant Person carries out identification and verification in respect of actual and potential beneficial owners of a trust, this should include the trustee, settlor, the protector, the enforcer, beneficiaries, other persons with power to appoint or remove a trustee and any person entitled to receive a distribution, whether or not such person is a named beneficiary.~~
845. Under Federal AML legislation, if the customer is a legal person, the Relevant Person must obtain information identifying the names and addresses of partners and shareholders who each hold more than 5% of the capital of the legal person i.e. it applies a specified threshold. This does not affect the approach that should be taken under Rule 7.3.1(1)(a**b**) and Rule 7.3.3 for verifying the identity of Beneficial Owners, where no threshold is specified (see Guidance items ~~404~~ to ~~447~~ above). As a result, under the Federal AML legislation a Relevant Person will need to obtain information identifying partners and shareholders who hold more than 5% of the capital of the legal person. Then, in accordance with the risk-based approach in Guidance items ~~404~~ to ~~447~~, the Relevant Person should determine whether it is necessary also to identify other persons who may be Beneficial Owners, and verify their identity.

Guidance on politically exposed persons

946. 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

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

close associates. Politically Exposed Person (“PEP”) status itself does not, of course, incriminate individuals or entities. ~~It does, however, put the customer into a higher risk category.~~

1047. Generally, a foreign PEP presents a higher risk of money laundering because there is a greater risk that such person, if he was committing money laundering, would attempt to place his money offshore where the customer is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his home jurisdiction to confiscate or freeze his criminal property.

1148. Corruption-related money laundering risk increases when a Relevant Person deals with a PEP. Corruption may involve serious crimes and has become the subject of increasing global concern. Corruption offences are predicate crimes under the Federal AML legislation. A Relevant Person should note that customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves.

1249. The DFSA considers that after leaving office a PEP may remain a higher risk for money laundering if such person continues to exert political influence or otherwise pose a risk of corruption.

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

7.4 Enhanced customer due diligence

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

- (a) obtain and verify additional:
 - (i) identification information on the customer and any ~~B~~eneficial ~~O~~wner;
 - (ii) information on the intended nature of the business relationship; and
 - (iii) information on the reasons for a transaction;
- (b) update more regularly the Customer Due Diligence information which it holds on the customer and any ~~B~~eneficial ~~O~~wners;
- (c) take reasonable measures to establish ~~verify information on:~~
 - (i) ~~the customer's~~ source of funds; and
 - (ii) ~~the customer's~~ source of wealth,of the customer or, if applicable, of the Beneficial Owner;
- (d) increase the degree and nature of monitoring of the business relationship, in order to determine whether the customer’s transactions or activities appear unusual or suspicious;

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (e) obtain the approval of senior management to commence a business relationship with a customer; and
- (f) where applicable, require that any first payment made by a customer in order to open an account with a Relevant Person must be carried out through a bank account in the customer's name with:
 - (i) a Bank;
 - (ii) a Regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF recommendations; or
 - (iii) a Subsidiary of a Regulated Financial Institution referred to in (ii), if the law that applies to the Parent ensures that the Subsidiary also observes the same AML standards as its Parent.

Guidance

1. In Rule 7.4.1 Enhanced CDD measures are only mandatory to the extent that they are applicable to the relevant customer or the circumstances of the business relationship and to the extent that the risks would reasonably require it. Therefore, the extent of additional measures to conduct is a matter for the Relevant Person to determine on a case by case basis.
2. In Rule 7.4.1 (e), senior management approval may be given by an individual member of the Relevant Person's senior management or by a committee of senior managers appointed to consider high risk customers. It may also be outsourced within the Group.
3. For high risk customers, a Relevant Person should, in order to mitigate the perceived and actual risks, exercise a greater degree of diligence throughout the customer relationship and should endeavour to understand the nature of the customer's business and consider whether it is consistent and reasonable.
4. A Relevant Person should be satisfied that a customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.
5. For enhanced CDD, a Relevant Person has to take reasonable measures to establish the source of funds. That is, where the funds for a particular service or transaction will come from (e.g. a specific bank account held with a specific financial institution) and whether that funding is consistent with the source of wealth of the customer or, if applicable, of the Beneficial Owner.
65. For enhanced CDD, where there is a Beneficial Owner, ~~verification of establishing~~ the customer's source of funds and wealth may require enquiring into the Beneficial Owner's source of funds and wealth because the source of the funds would normally be the Beneficial Owner and not the customer.
76. The DFSA considers that taking reasonable measures to establish the ~~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.
87. The DFSA considers that verification of source of wealth includes obtaining independent corroborating evidence such as share certificates, publicly-available registers of ownership,

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

bank or brokerage account statements, probate documents, audited accounts and financial statements, news items from a reputable source and other similar evidence. For example:

- a. for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect its financial situation or the profitability of its business; and
- b. for a natural person, this might include documentary evidence which corroborates answers given to questions on the source of wealth in an application form or customer questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide sufficient bank or salary statements covering a number of years to draw up a picture of his source of wealth.

98. 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.

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

- a. where, following the use of other Enhanced CDD measures, the Relevant Person is not satisfied with the results of due diligence; or
- b. as an alternative measure, where one of the measures in Rule 7.4.1 (a) to (e) cannot be carried out.

7.5 Simplified customer due diligence

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

- (a) verifying the identity of the customer and ~~identifying~~ any Beneficial Owners after the establishment of the business relationship under Rule 7.2.1(3);
- (b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;
- ~~(c) deciding not to verify an identified beneficial owner;~~
- ~~(cd)~~ 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;~~
- ~~(df)~~ reducing the degree of on-going monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or
- ~~(eg)~~ not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business

relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

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

Guidance

1. Rule 7.5.1(1) provides examples of Simplified CDD measures. Other measures may also be used by a Relevant Person to modify CDD in accordance with the customer risks.
2. A Relevant Person should not use a "one size fits all" approach for all its low risk customers. Notwithstanding that the risks may be low for all such customers, the degree of CDD undertaken needs to be proportionate to the specific risks identified on a case by case basis. ~~For example, for customers where the money laundering risks are very low, a Relevant Person may decide to simply identify the customer and verify such information only to the extent that this is commercially necessary. On the other hand, a low risk customer which is undertaking a complex transaction might require more comprehensive Simplified CDD.~~
3. ~~For the avoidance of doubt, a~~ A Relevant Person is ~~always~~ not required to 'identify' or verify Bbeneficial Owners, ~~except~~ for retail investment funds which are widely held and for investment funds where the investor invests via pension contributions. ~~However, a Relevant Person may decide not to 'verify' beneficial owners of a low risk customer.~~
4. An example of circumstances where a Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates would be where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.
5. An example of where a Relevant Person might reasonably reduce the degree of on-going monitoring and scrutinising of transactions, based on a reasonable monetary threshold or on the nature of the transaction, would be where the transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the transaction is not material for money laundering purposes given the nature of the customer and the transaction type.
6. For the avoidance of doubt, a Relevant Person should not conduct Simplified CDD where there is any suspicion of money laundering.

7.6 Ongoing customer due diligence

- 7.6.1** (1) When undertaking ongoing Customer Due Diligence under Rule 7.3.1(1)(d), a Relevant Person must, using the risk-based approach:
- (a) monitor transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the Relevant Person's knowledge of the customer, his business and risk rating;
 - (b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;
 - (c) enquire into the background and purpose of the transactions in (b);
 - (d) ~~periodically~~ review the adequacy of the Customer Due Diligence information it holds on customers and Bbeneficial Owners to ensure

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

that the information is kept up to date, particularly for customers with a high risk rating; and

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

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

Guidance

1. In complying with Rule 7.6.1(1)(d), a Relevant Person should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up-to-date. Examples of non-static identity documentation include passport number and residential/business address and, for a legal person, its share register or list of partners.
2. A Relevant Person should undertake a review under Rule 7.6.1(1)(d) and (e), both periodically and at other appropriate times such as particularly when:
 - a. the Relevant Person changes its CDD documentation requirements;
 - b. an unusual transaction with the customer is expected to take place;
 - c. there is a material change in the business relationship with the customer; or
 - d. there is a material change in the nature or ownership of the customer.
3. The degree of the on-going due diligence to be undertaken will depend on the customer risk assessment carried out under Rule 6.1.1.
4. A Relevant Person’s transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination thereof, are one of the most important aspects of effective CDD. Whether a Relevant Person should undertake the monitoring by means of a manual or computerised system (or both) will depend on a number of factors, including:
 - a. the size and nature of the Relevant Person’s business and customer base; and
 - b. the complexity and volume of customer transactions.

Ongoing sanctions screening

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

Guidance

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

7.7 Failure to conduct or complete customer due diligence

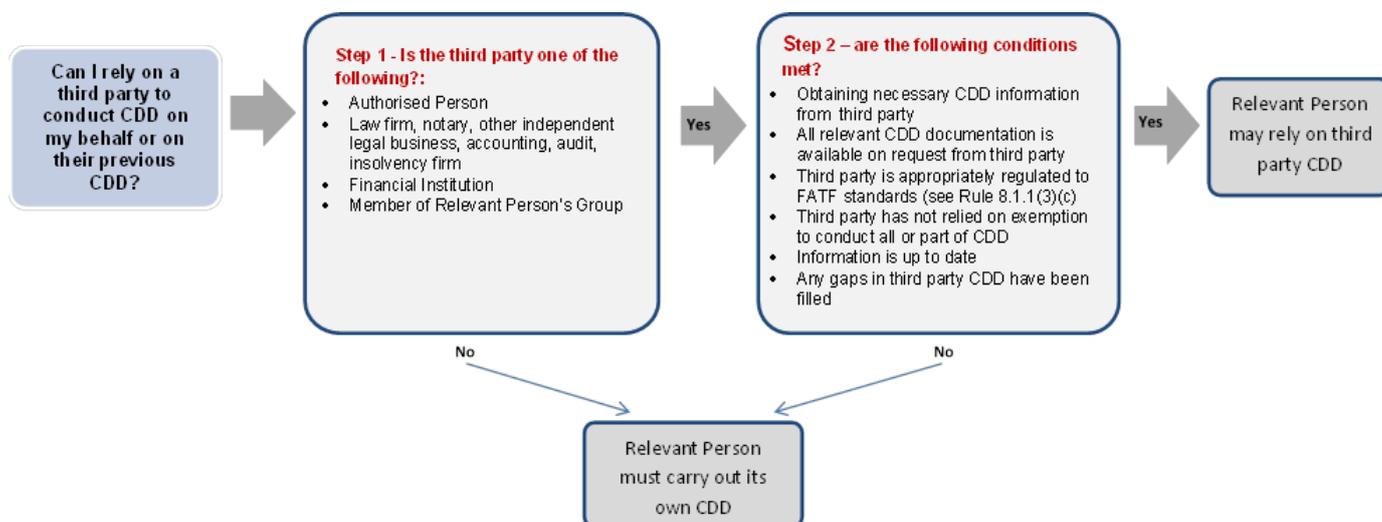
- 7.7.1** (1) Where, in relation to any customer, a Relevant Person is unable to conduct or complete the requisite Customer Due Diligence in accordance with Rule 7.1.1 it must, to the extent relevant:
- (a) not carry out a transaction with or for the customer through a bank account or in cash;
 - (b) not open an account or otherwise provide a service;
 - (c) not otherwise establish a business relationship or carry out a transaction;
 - (d) terminate or suspend any existing business relationship with the customer;
 - (e) return any monies or assets received from the customer; and
 - (f) consider whether the inability to conduct or complete Customer Due Diligence necessitates the making of a Suspicious Activity Report under Rule 13.3.1(c).

.....

Guidance

1. In complying with Rule 7.7.1(1) a Relevant Person should apply one or more of the measures in (a) to (f) as appropriate in the circumstances. Where CDD cannot be completed, it may be appropriate not to carry out a transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD, such as identifying and verifying a Beneficial Owner cannot be conducted, a Relevant Person should not establish a business relationship with the customer.
2. A Relevant Person should note that Rule 7.7.1 applies to both existing and prospective customers. For new customers it may be appropriate for a Relevant Person to terminate the business relationship before a product or service is provided. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. Whichever route is taken, the Relevant Person should be careful not to tip off the customer.
3. A Relevant Person should adopt the RBA for CDD of existing customers. For example, if a Relevant Person considers that any of its existing customers (which may include customers which it migrates into the DIFC) have not been subject to CDD at an equivalent standard to that required by this module, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with Rule 7.7.1.

8 RELIANCE AND OUTSOURCING



8.1 Reliance on a third party

- 8.1.1** (1) A Relevant Person may rely on the following third parties to conduct one or more elements of Customer Due Diligence on its behalf:
- (a) an Authorised Person;
 - (b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;
 - (c) a Financial Institution; or
 - (d) a member of the Relevant Person's Group.
- (2) In (1), a Relevant Person may rely on the information previously obtained by a third party which covers one or more elements of Customer Due Diligence.
- (3) Where a Relevant Person seeks to rely on a person in (1) it may only do so if and to the extent that:
- (a) it immediately obtains the necessary Customer Due Diligence information from the third party in (1);
 - (b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of Customer Due Diligence will be available from the third party on request without delay;
 - (c) ~~the person in (1)(b) to (d) is subject to regulation, including AML regulation, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;~~

- (c) if a person in (1)(b) to (d) is in another country, the person is:
 - (i) subject to requirements in relation to customer due diligence and record keeping which meet the standards set out in the FATF Recommendations; and
 - (ii) supervised for compliance with those requirements in a manner that meets the standards for regulation and supervision set out in the FATF Recommendations;
 - (d) the person in (1) has not relied on any exception from the requirement to conduct any relevant elements of Customer Due Diligence which the Relevant Person seeks to rely on; and
 - (e) in relation to (2), the information is up to date.
- (4) Where a Relevant Person relies on a member of its Group, such Group member need not meet the condition in (3)(c) if:
- (a) the Group applies and implements a Group-wide policy on cCustomer dDue dDiligence, and—record keeping, Politically Exposed Persons and AML programmes which meets is equivalent to the standards set by out in the FATF Recommendations; and
 - (b) where the effective implementation of those Customer Due Diligence, and—record keeping and PEP requirements and AML programmes are supervised at Group level by a Financial Services Regulator or other competent authority in a country, the supervision and regulation meets the standards with AML regulations which are equivalent to the standards set out in the FATF Recommendations.
- (5) If a Relevant Person is not reasonably satisfied that a customer or Bbeneficial Qowner has been identified and verified by a third party in a manner consistent with these Rules, the Relevant Person must immediately perform the Customer Due Diligence itself with respect to any deficiencies identified.
- (6) Notwithstanding the Relevant Person's reliance on a person in (1), the Relevant Person remains responsible for compliance with, and liable for any failure to meet the Customer Due Diligence requirements in this module.

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

- (a) mutual evaluations, assessment reports or follow-up reports published by FATF, the IMF, the World Bank, the OECD or other International Organisations;
- (b) membership of FATF or other international or regional groups such as the MENAFATF or the Gulf Co-operation Council;
- (c) contextual factors such as political stability or the level of corruption in the jurisdiction;

- (d) evidence of recent criticism of the jurisdiction, including in:
 - (i) FATF advisory notices;
 - (ii) public assessments of the jurisdiction’s AML regime by organisations referred to in (a); or
 - (iii) reports by other relevant non-government organisations or specialist commercial organisations; and
 - (e) whether adequate arrangements exist for co-operation between the AML regulator in that jurisdiction and the DFSA.
- (2) A Relevant Person making an assessment under (1) must rely only on sources of information that are reliable and up-to-date.
- (3) A Relevant Person must keep adequate records of how it made its assessment, including the sources and materials considered.

Guidance

1. In complying with Rule 8.1.1(3)(a), “immediately obtaining the necessary CDD information” means obtaining all relevant CDD information, and not just basic information such as name and address. Compliance can be achieved by having that relevant information sent by email or other appropriate means. For the avoidance of doubt, a Relevant Person is not required automatically to obtain the underlying certified documents used by the third party to undertake its CDD. A Relevant Person must, however, under Rule 8.1.1(3)(b) ensure that the certified documents are readily available from the third party on request.
2. The DFSA would expect a Relevant Person, in complying with Rule 8.1.1(5), to fill any gaps in the CDD process as soon as it becomes aware that a customer or Beneficial Owner has not been identified and verified in a manner consistent with these Rules.
3. If a Relevant Person acquires another business, either in whole or in part, the DFSA would permit the Relevant Person to rely on the CDD conducted by the business it is acquiring but would expect the Relevant Person to have done the following:
 - a. as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD undertaken; and
 - b. to undertake CDD on all the customers to cover any deficiencies identified in (a) as soon as possible following the acquisition, prioritising high risk customers.
4. Where a particular jurisdiction’s laws (such as secrecy or data protection legislation) would prevent a Relevant Person from having access to CDD information upon request without delay as referred to in Rule 8.1.1(3)(b), the Relevant Person should undertake the relevant CDD itself and should not seek to rely on the relevant third party.
5. If a Relevant Person relies on a third party located in a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the Relevant Person must ensure that the foreign jurisdiction has AML regulations that are equivalent to the standards in the FATF Recommendations (see Rule 8.1.1(3)(c) and Rule 8.1.2).
6. ~~When assessing if AML regulations in another jurisdiction are equivalent to FATF standards, a Relevant Person may consider a number of factors including, but not limited to: FATF membership, FATF Mutual Evaluation reports, FATF style or IMF/World Bank evaluations, membership of an international or regional ‘group’ such as the MENAFATF or the Gulf Cooperation Council, contextual factors such as political stability or the level of corruption,~~

~~evidence of relevant criticism of a jurisdiction including FATF advisory notices or independent and public assessments of the jurisdiction's overall AML regime such as IMF/World Bank or other reports by reputable NGOs or specialised commercial agencies. A Relevant Person should, in making its assessment, rely only on sources that are up to date and that include the latest AML developments from a reliable and competent source. The assessment may also take into account whether adequate arrangements exist for co-operation between the AML regulator in that jurisdiction and the DFSA. The DFSA expects a Relevant Person to keep sufficient records of the sources and materials considered when undertaking this AML assessment.~~

8.2 Outsourcing

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

Guidance

1. Prior to appointing an outsourced service provider to undertake CDD, a Relevant Person should undertake appropriate due diligence to assure itself of the suitability of the outsourced service provider and should ensure that the outsourced service provider's obligations are clearly documented in a binding agreement.
2. An Authorised Person should be mindful of its obligations regarding outsourcing set out in GEN Rules 5.3.21 and 5.3.22.

9 CORRESPONDENT BANKING, WIRE ELECTRONIC FUND TRANSFERS AND AUDIT

9.1 Application

9.1.1 This chapter applies only to an Authorised Person.

9.2 Correspondent banking

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

- (a) undertake appropriate Customer Due Diligence on the respondent bank;
- (b) as part of (a), gather sufficient information about the respondent bank to understand fully the nature of the business, including making appropriate enquiries on its management, its major business activities and the countries or jurisdictions in which it operates;
- (c) determine from publicly-available information the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or relevant regulatory action;
- (d) assess the respondent bank's AML controls and ascertain if they are adequate and effective in light of the FATF Recommendations;
- (e) ensure that prior approval of the Authorised Firm's senior management is obtained before entering into a new correspondent banking relationship;
- (f) ensure that the respective responsibilities of the parties to the correspondent banking relationship are properly documented; and
- (g) be satisfied that, in respect of any customers of the respondent bank who have direct access to accounts of the Authorised Firm, the respondent bank:
 - (i) has undertaken Customer Due Diligence (including ongoing Customer Due Diligence) at least equivalent to that in Rule 7.3.1 in respect of each customer; and
 - (ii) is able to provide the relevant Customer Due Diligence information in (i) to the Authorised Firm upon request; and
- (h) document the basis for its satisfaction that the requirements in (a) to (g) are met.

9.2.2 An Authorised Firm must:

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

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

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

Guidance

Rule 9.2.2 prohibits an Authorised Firm from entering into a correspondent banking relationship with a Shell Bank or a bank which is known to permit its accounts to be used by Shell Banks. See the Guidance after Rule 6.1.47 for more information about what constitutes a Shell Bank.

9.3 Wire Electronic fund transfers

9.3.1 In this section:

- (a) ~~“beneficiary” means the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer;~~
- (b) ~~“originator” means the account holder who instructs the wire transfer from the relevant account, or where there is no account, the natural or legal person that places the order with the ordering Financial Institution to perform the wire transfer; and~~
- (c) ~~“wire transfer” includes any value transfer arrangement.~~

9.3.2 (1) An Authorised Person must:

- (a) ~~when it sends or receives funds by wire transfer on behalf of a customer, ensure that the wire transfer and any related messages contain accurate originator and beneficiary information;~~
 - (b) ~~ensure that, while the wire transfer is under its control, the information in (a) remains with the wire transfer and any related message throughout the payment chain; and~~
 - (c) ~~monitor wire transfers for the purpose of detecting those wire transfers that do not contain originator and beneficiary information and take appropriate measures to identify any money laundering risks.~~
- (2) ~~The requirement in (1) does not apply to an Authorised Person which transfers funds to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.~~
- (3) An Authorised Person must ensure that information accompanying all wire transfers contains at a minimum:
- (a) the name of the originator;
 - (b) the originator account number where such an account is used to process the transaction;
 - (c) the originator’s address, or national identity number, or customer identification number, or date and place of birth;
 - (d) the name of the beneficiary; and

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

Application

- 9.3.1** (1) This section applies to an Authorised Person when it sends or transmits funds by electronic means, or when it receives funds (including serial payments and cover payments) by electronic means, on the account of a payer or payee.
- (2) This section does not apply to a transfer and settlement between Financial Institutions if the Financial Institutions are acting on their own behalf as the payer and the payee.

Definitions

9.3.2 In this section:

- (a) “batch transfer” means a transfer that consists of a number of individual fund transfers that are bundled for transmission, whether the individual fund transfers are intended ultimately for one or more payees;
- (b) “beneficiary institution” means the Financial Institution that receives the fund transfer from the ordering institution, whether directly or through an intermediary institution, and makes the funds available to the payee;
- (c) “cover payment” means a fund transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction from the ordering institution to the beneficiary institution through one or more intermediary institutions;
- (d) “cross-border fund transfer” means a fund transfer where the ordering institution and the beneficiary institution are located in different countries and includes any chain of fund transfers in which at least one of the Financial Institutions involved is located in a different country;
- (e) “customer identification number” means a number that is different from the unique transaction reference number and:
- (i) uniquely identifies the payer to the ordering institution; and
- (ii) refers to a record held by the ordering institution that contains at least one of the following: the payer’s address, national identity number or date and place of birth;
- (f) “domestic fund transfer” means a fund transfer where the ordering institution and beneficiary institution are located in the same country and includes any chain of fund transfers that takes place entirely within a country, even if the system used to transfer the payment message is located in another country;
- (g) “fund transfer” means any transaction carried out on behalf of a payer through a Financial Institution by electronic means with a view to making an amount of funds available to a payee at a beneficiary institution, irrespective of whether the payer and the payee are the same person;
- (h) “intermediary institution” means the Financial Institution in a serial payment or cover payment chain that receives and transmits a fund transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (i) “ordering institution” means the Financial Institution that transfers the funds upon receiving the request for a fund transfer on behalf of the payer;
- (j) “payee” means the natural or legal person identified by the payer as the recipient of the requested fund transfer;
- (k) “payer” means the account holder who allows the fund transfer from that account or, if there is no account, the natural or legal person that places the fund transfer order with the ordering institution to perform the fund transfer;
- (l) “serial payment” means a direct sequential chain of payment where the fund transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution, directly or through one or more intermediary institutions;
- (m) “straight-through processing” means payment transactions that are conducted electronically without the need for manual intervention; and
- (n) “unique transaction reference number” means a combination of letters, numbers or symbols, determined by the Financial Institution in accordance with the protocols of the payment and settlement system or messaging system used for the fund transfer, and which permits the traceability of the fund transfer.

Requirements for ordering institution

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

- (a) identify the payer and verify the identity of the payer if the identity has not previously been identified; and
- (b) record adequate details of the fund transfer that are sufficient to permit its reconstruction, including but not limited to, the date of the transfer, the payer and payee, and the type and amount of currency transferred and the value date.

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

- (a) the name of the payer;
- (b) the payer’s account number (or unique transaction reference number if no account number exists);
- (c) the name of the payee; and
- (d) the payee’s account number (or unique transaction reference number if no account number exists).

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

- (a) the payer’s address:

- (b) the payer's national identity number, such as an identity card number or passport number;
- (c) the payer's customer identification number; or
- (d) the date and place of birth of the payer.

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

- (a) the batch file contains the payer information required under Rule 9.3.4 and, if applicable, Rule 9.3.5;
- (b) it has verified the payer information referred to in (a); and
- (c) the batch file contains the payee information required under Rule 9.3.4 for each payee and that information is fully traceable in the payee's country.

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

- (a) include in the message or payment instruction that accompanies or relates to the fund transfer the following:
 - (i) the name of the payer;
 - (ii) the payer's account number (or unique transaction reference number if no account number exists); and
 - (iii) any one of the following:
 - (A) the payer's address;
 - (B) the payer's national identity number, such as an identity card number or passport number;
 - (C) the payer's customer identification number; or
 - (D) the date and place of birth of the payer; or
- (b) include only the payer's account number (or unique transaction reference number if no account number exists), provided that:
 - (i) those details will permit the transaction to be traced back to the payer and payee; and
 - (ii) the ordering institution must provide the payer information set out in paragraph (a) within 3 business days of a request for the information by the beneficiary institution or the DFSA or immediately upon request of a law enforcement agency.

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

Guidance

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

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

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

Requirements for beneficiary institution

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

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

Requirements for intermediary institution

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

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

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

Systems and controls concerning fund transfers

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

Guidance

1. ~~In the absence of an account number, a unique transaction reference number should be included which permits traceability of the transaction.~~
2. ~~The DFSA considers that concealing or removing in a wire fund transfer any of the information required by this section Rule 9.3.2(3) would be a breach of the requirement to ensure that the wire fund transfer contains accurate originator payer and beneficiary payee information.~~

9.4 Audit

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

Guidance

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

10 SANCTIONS AND OTHER INTERNATIONAL OBLIGATIONS

10.1 Application

[deleted]

10.2 Relevant United Nations resolutions and sanctions

- 10.2.1** (1) A Relevant Person must establish and maintain effective systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council.
- (2) A Relevant Person must immediately notify the DFSA when it becomes aware that it is:
- (a) carrying on or about to carry on an activity;
 - (b) holding or about to hold money or other assets; or
 - (c) undertaking or about to undertake any other business whether or not arising from or in connection with (a) or (b);
- for or on behalf of a person, where such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the United Nations Security Council.
- (3) A Relevant Person must ensure that the notification stipulated in (2) above includes the following information:
- (a) a description of the relevant activity in (2) (a), (b) or (c); and
 - (b) the action proposed to be taken or that has been taken by the Relevant Person with regard to the matters specified in the notification.

Guidance

1. In Rule 10.2.1(1), taking reasonable measures to comply with a United Nations Security Council resolution or sanction may include, for example, mean that a Relevant Person ~~cannot undertake~~ not undertaking a transaction for or on behalf of a person or ~~that it may need to undertake~~ ing further due diligence in respect of a person.
2. Relevant United Nations Security Council resolutions or sanctions mentioned in Rule 10.2.1 may, among other things, relate to money laundering, terrorist financing or the financing of weapons of mass destruction or otherwise be relevant to the activities carried on by the Relevant Person. For example:
 - a. a Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a person engaged in money laundering, terrorist financing or the financing of weapons of mass destruction; and

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- b. an Authorised Market Institution should exercise due care to ensure that it does not facilitate fund raising activities or listings by persons engaged in money laundering or terrorist financing or financing of weapons of mass destruction.
3. A Relevant Person should be proactive in checking for, and taking measures to comply with, relevant resolutions or sanctions issued by the United Nations Security Council. The DFSA expects Relevant Persons to perform checks on an ongoing basis against their customer databases and records for any names appearing in resolutions or sanctions issued by the United Nations Security Council as well as to monitor transactions accordingly.
4. A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with this module.

10.3 Government, regulatory and international findings

- 10.3.1** (1) A Relevant Person must establish and maintain systems and controls to ensure that on an ongoing basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions (each of which is referred to in this Rule as a “finding”) issued by:
- (a) the government of the U.A.E. or any government departments in the U.A.E.;
 -
- (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.
- (3) For the purposes of (1), measures in a finding that a Relevant Person must comply with include, but are not limited to, measures:
- (a) requiring specific elements of enhanced due diligence;
 - (b) requiring enhanced reporting mechanisms or systematic reporting of financial transactions;
 - (c) limiting business relationships or financial transactions with specified persons or persons in a specified jurisdiction;
 - (d) prohibiting Relevant Persons from relying on third parties located in a specified jurisdiction to conduct customer due diligence;
 - (e) requiring correspondent relationships with banks in a specified jurisdiction to be reviewed, amended or, if necessary, terminated;

- (f) prohibiting the execution of specified electronic fund transfers; or
 - (g) requiring increased external audit requirements for financial groups with respect to branches and subsidiaries located in a specified jurisdiction.
- (34) A Relevant Person must immediately notify the DFSA in writing if it becomes aware of non-compliance by a person with a finding and provide the DFSA with sufficient details of the person concerned and the nature of the non-compliance.

Guidance

1. The purpose of this Rule is to ensure that a Relevant Person takes into consideration the broad range of tools used by competent authorities and international organisations to communicate AML/CTF risks to stakeholders.
2. The Rule also permits the DFSA to require enhanced due diligence or other specific countermeasures to address risks identified in a specific country or jurisdiction. The DFSA may impose such countermeasures either when called upon to do so by FATF or independently of any FATF request.
- ~~2. A Relevant Person should examine and pay special attention to any transactions or business relationship with persons located in countries or jurisdictions mentioned by the persons in Rule 10.3.1(1)(a) to (e).~~
3. Relevant Persons considering transactions or business relationships with persons located in countries or jurisdictions that have been identified as deficient, or against which the U.A.E. or the DFSA have outstanding advisories, should be aware of the background against which the assessments, or the specific recommendations have been made. These circumstances should be taken into account in respect of introduced business from such jurisdictions, and when receiving inward payments for existing customers or in respect of inter-bank transactions.

.....

...

14 GENERAL OBLIGATIONS

14.1 Groups, branches and subsidiaries

- 14.1.1** (1) A Relevant Person which is a DIFC entity must ensure that its policies, procedures, systems and controls required by Rule 5.2.1 apply to:
- (a) any of its branches or Subsidiaries; and
 - (b) any of its Group entities in the DIFC.
- (2) ~~The requirement in (1) does not apply if the Relevant Person can satisfy the DFSA that the relevant branch, Subsidiary or Group entity is subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance with such regulations.~~
- (2) Where the anti-money laundering requirements in another jurisdiction differ from those in the DIFC, the Relevant Person must require its branch or Subsidiary in that jurisdiction to apply the higher of the two standards, to the extent permitted by the law of that jurisdiction.
- (3) Where the law of another jurisdiction does not permit the implementation of policies, procedures, systems and controls that are equivalent to or higher than consistent with those that apply to the Relevant Person in the DIFC, the Relevant Person must:
- (a) inform the DFSA in writing; and
 - (b) apply appropriate additional measures to manage the money laundering risks posed by the relevant branch or Subsidiary.

Guidance

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

14.1.2 A Relevant Person must:

- (a) communicate the policies and procedures which it establishes and maintains in accordance with these Rules to its Group entities, branches and Subsidiaries; and
- (b) document the basis for its satisfaction that the requirement in Rule 14.1.1(2) is met.

Guidance

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

14.2 Group policies

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

- ~~(a) understands the policies and procedures covering the sharing of information between Group entities, particularly when sharing Customer Due Diligence information;~~
- (a) has developed and implemented policies and procedures for the sharing of information between Group entities, including the sharing of information relating to Customer Due Diligence and money laundering risks;
- (b) has in place adequate safeguards on the confidentiality and use of information exchanged between Group entities, including consideration of relevant data protection legislation;
- (c) remains aware of the money laundering risks of the Group as a whole and of its exposure to the Group and takes active steps to mitigate such risks;
- (d) contributes to a Group-wide risk assessment to identify and assess money laundering risks for the Group; and
- (e) provides its Group-wide compliance, audit and AML functions with customer account and transaction information from branches and subsidiaries when necessary for AML purposes.

14.3 Notifications

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

- (a) receives a request for information from a regulator or agency responsible for AML, counter-terrorism financing, or sanctions regarding enquiries into potential money laundering or terrorist financing or sanctions breaches;
- (b) becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;
- (c) becomes aware of any money laundering or sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or
- (d) becomes aware of a significant breach of a Rule in this module or a breach of Federal AML legislation by the Relevant Person or any of its Employees.

14.4 Record keeping

14.4.1 A Relevant Person must maintain the following records:

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

- (a) a copy of all documents and information obtained in undertaking initial and ongoing Customer Due Diligence;
- (b) ~~the supporting~~ records (consisting of the original documents or certified copies) in respect of the customer business relationship, including ~~transactions~~;
 - (i) business correspondence and other information relating to a customer's account;
 - (ii) sufficient records of transactions to enable individual transactions to be reconstructed; and
 - (iii) internal findings and analysis relating to a transaction or any business, such as if the transaction or business is unusual or suspicious, whether or not it results in a Suspicious Activity Report;
- (c) notifications made under Rule 13.2.2;
- (d) Suspicious Activity Reports and any relevant supporting documents and information, including internal findings and analysis;
- (e) any relevant communications with the FID; ~~and~~
- (f) the documents in Rule 14.4.2; ~~and~~
- (g) any other matter that the Relevant Person is expressly required to record under these Rules.

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

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

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

- (a) the risk assessment of its business undertaken under Rule 5.1.1;
- (b) how the assessment in (a) was used for the purposes of complying with Rule 6.1.1(1);
- (c) the risk assessment of the customer undertaken under Rule 6.1.1(1)(a); and
- (d) the determination made under Rule 6.1.1(1)(b).

Guidance

1. The records required to be kept under Rule 14.4.1 may be kept in electronic format, provided that such records are readily accessible and available to respond promptly to any DFSA requests for information. Authorised Persons are reminded of their obligations in GEN Rule 5.3.24.
2. If the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML)

3. The records maintained by a Relevant Person should be kept in such a manner that:
 - a. the DFSA or another competent authority is able to assess the Relevant Person's compliance with legislation applicable in the DIFC;
 - b. any transaction which was processed by or through the Relevant Person on behalf of a customer or other third party can be reconstructed;
 - c. any customer or third party can be identified; and
 - d. the Relevant Person can satisfy, ~~within an appropriate time,~~ without delay any regulatory enquiry or court order to disclose information.

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

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

- (a) take reasonable steps to ensure that the records are held in a manner consistent with these Rules;
- (b) ensure that the records are easily accessible to the Relevant Person; and
- (c) upon request by the DFSA, ensure that the records are immediately available for inspection ~~within a reasonable period of time.~~

14.4.4 A Relevant Person must:

- (a) verify if there is secrecy or data protection legislation that would restrict access without delay to the records referred to in Rule 14.4.1 by the Relevant Person, the DFSA or the law enforcement agencies of the U.A.E.; and
- (b) where such legislation exists, obtain without delay certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons in (a).

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

Guidance

1. In complying with Rule 14.4.3, Authorised Persons are reminded of their obligations in GEN Rule 5.3.24.
2. The DFSA considers that "appropriate measures" in Rule 14.4.5 may include the maintenance of a training log setting out details of:
 - a. the dates when the training was given;
 - b. the nature of the training; and
 - c. the names of Employees who received the training.

...