



# Anti-Money Laundering and Combating Terrorist Financing Rules 2010

made under Law No. (4) of 2010 on Anti-Money Laundering and  
Combating the Financing of Terrorism.

## Contents

---

	Page
<b>Chapter 1</b>	<b>7</b>
<b>General provisions</b>	<b>7</b>
<b>Part 1.1</b>	<b>7</b>
<b>Introductory</b>	<b>7</b>
1.1.1 Name of rules	7
1.1.2 Commencement	7
1.1.3 General application of these rules	7
1.1.4 Annex	7
1.1.5 Notes and examples	7
<b>Part 1.2</b>	<b>7</b>
<b>Key AML/CFT principles</b>	<b>7</b>
1.2.1 Principle 1—senior management responsibility	7
1.2.2 Principle 2—risk-based approach	7
1.2.3 Principle 3—know your customer	8
1.2.4 Principle 4—effective reporting	8
1.2.5 Principle 5—high standard screening and appropriate training	8
1.2.6 Principle 6—evidence of compliance	8
<b>Part 1.3</b>	<b>8</b>
<b>Key terms</b>	<b>8</b>
1.3.1 What is a Regulator?	8
1.3.2 What is a licensed party?	8
1.3.3 What is a financial services institution?	8
1.3.4 Who is a customer?	8
1.3.5 Who is the <i>beneficial owner</i> ?	9
1.3.6 Who is a <i>politically exposed person</i> ?	9
1.3.7 What is a <i>correspondent securities relationship</i> ?	10
1.3.8 What is a <i>shell bank</i> ?	11
<b>Chapter 2</b>	<b>12</b>
<b>General AML and CFT responsibilities</b>	<b>12</b>
<b>Part 2.1</b>	<b>12</b>
<b>The licensed party</b>	<b>12</b>
2.1.1 Licensed parties to develop AML/CFT programme	12
2.1.2 Policies etc must be risk-sensitive, appropriate and adequate	12
2.1.3 Matters to be covered by policies etc	12
2.1.4 Assessment and review of policies etc	13
2.1.5 Compliance by officers, employees, agents etc	14
2.1.6 Application of AML/CFT Law requirements, policies etc to branches and associates	14
2.1.7 Application of AML/CFT Law requirements, policies etc to outsourced functions and activities	16

<b>Part 2.2</b>	<b>Senior management</b>	<b>17</b>
2.2.1	Overall senior management responsibility	17
2.2.2	Particular responsibilities of senior management	17
<b>Part 2.3</b>	<b>MLRO and deputy MLRO</b>	<b>18</b>
<b>Division 2.3.A</b>	<b>Appointment of MLRO and deputy MLRO</b>	<b>18</b>
2.3.1	Appointment—MLRO and deputy MLRO	18
2.3.2	Eligibility to be MLRO	18
<b>Division 2.3.B</b>	<b>Roles of MLRO and deputy MLRO</b>	<b>19</b>
2.3.3.	General responsibilities of MLRO	19
2.3.4	Particular responsibilities of MLRO	19
2.3.5	Role of deputy MLRO	20
2.3.6	How MLRO must carry out role	20
<b>Division 2.3.C</b>	<b>Reporting by MLRO to senior management</b>	<b>20</b>
2.3.7	MLRO reports	20
2.3.8	Minimum annual report by MLRO	21
2.3.9	Consideration of MLRO reports	21
<b>Chapter 3</b>	<b>The risk-based approach</b>	<b>23</b>
<b>Part 3.1</b>	<b>The risk-based approach generally</b>	<b>23</b>
3.1.1	Licensed parties must conduct risk assessment and decide risk mitigation	23
3.1.2	Approach to risk mitigation must be based on suitable methodology	23
3.1.3	Risk profiling a business relationship	24
<b>Part 3.2</b>	<b>Customer risk</b>	<b>24</b>
3.2.1	Risk assessment for customer risk	24
3.2.2	Policies etc for customer risk	25
3.2.3	Scoring business relationships sources of wealth and funds	25
3.2.4	Persons associated with terrorist acts etc—enhanced CDD and ongoing monitoring	25
3.2.5	Measures for politically exposed persons	25
3.2.6	Legal persons, legal arrangements and facilities—risk assessment process	26
<b>Part 3.3</b>	<b>Product risk</b>	<b>27</b>
3.3.1	Risk assessment for product risk	27
3.3.2	Policies etc for product risk	27
3.3.3	Scoring business relationships—types of products	27
3.3.4	Products with fictitious or false names or no names	27
3.3.5	Correspondent securities relationships generally	28
3.3.6	Shell banks	29
3.3.7	Payable through accounts	29
3.3.8	Power of attorney	30
3.3.9	Bearer shares and share warrants to bearer	30
3.3.10	Wire transfers	30

<b>Part 3.4</b>	<b>Interface risk</b>	<b>31</b>
<b>Division 3.4.A</b>	<b>Interface risks—general</b>	<b>32</b>
3.4.1	Risk assessment for interface risk	32
3.4.2	Policies etc for interface risk , etc.	32
3.4.3	Scoring business relationships—interface risk	32
3.4.4	Electronic verification of identification documentation	32
3.4.5	Payment processing using on-line services	33
<b>Division 3.4.B</b>	<b>Reliance on others generally</b>	<b>33</b>
3.4.6	Activities to which DIV 3.4B does not apply	33
3.4.7	Reliance on certain third parties generally	33
3.4.8	Introducers	33
3.4.9	Group introductions	34
3.4.10	Intermediaries	35
<b>Division 3.4.C</b>	<b>Third party certification—identification documents</b>	<b>36</b>
3.4.11	Third party certification of identification documents	36
<b>Part 3.5</b>	<b>Jurisdiction risk</b>	<b>36</b>
3.5.1	Risk assessment for jurisdiction risk	36
3.5.2	Policies etc for jurisdiction risk	37
3.5.3	Scoring business relationships—types of associated jurisdictions	37
3.5.4	Decisions about effectiveness of AML/CFT regimes in other jurisdictions	37
3.5.5	Jurisdictions with impaired international cooperation	37
3.5.6	Non-cooperative, high risk and sanctioned jurisdictions	37
3.5.7	Jurisdictions with high propensity for corruption	38
<b>Chapter 4</b>	<b>Know your customer</b>	<b>39</b>
<b>Part 4.1</b>	<b>Know your customer—</b>	<b>39</b>
4.1.1	Know your customer principle—	39
4.1.2	Overview of CDD requirements	39
4.1.3	Customer identification documents	39
<b>Part 4.2</b>	<b>Know your customer—key terms</b>	<b>40</b>
4.2.1	What are customer due diligence measures?	40
4.2.2	What is <i>ongoing monitoring</i> ?	41
4.2.3	Who is an <i>applicant for business</i> ?	42
4.2.4	What is a <i>business relationship</i> ?	42
<b>Part 4.3</b>	<b>Customer due diligence measures and ongoing monitoring</b>	<b>43</b>
4.3.1	When CDD required—basic requirement	43
4.3.2	Licensed party unable to complete CDD for customer	43
4.3.3	When CDD may not be required—acquired businesses	43
4.3.4	Timing of CDD—establishment of business relationship	44
4.3.5	When CDD required—additional requirement for existing customers	44

4.3.6	Extent of CDD—general requirement	45
4.3.7	Extent of CDD—legal persons and arrangements	45
4.3.8	Ongoing monitoring required	46
4.3.9	Procedures for ongoing monitoring	46
<b>Part 4.4</b>	<b>Customer identification documentation</b>	<b>47</b>
<b>Division 4.4. A</b>	<b>Customer identification documentation—general</b>	<b>47</b>
4.4.1	Elements of customer identification documentation	47
4.4.2	Records of customer identification documentation etc	47
<b>Division 4.4 B</b>	<b>Customer identification documentation—the economic activity</b>	<b>47</b>
4.4.3	Risks associated with the economic activity	47
4.4.4	Risks associated with the economic activity—source of wealth and funds	48
4.4.5	Risks associated with the economic activity—purpose and intended nature of business relationship	48
<b>Division 4.4 C</b>	<b>Customer identification documentation—particular applicants for business</b>	<b>49</b>
4.4.6	Customer identification documentation—individuals	49
4.4.7	Customer identification documentation—multiple individual applicants	49
4.4.8	Customer identification documentation—corporations	49
4.4.9	Customer identification documentation—unincorporated partnerships and associations	50
4.4.10	Customer identification documentation—charities	51
4.4.11	Customer identification documentation—trusts	51
4.4.12	Customer identification documentation—clubs and societies	51
4.4.13	Customer identification documentation—governmental bodies	52
<b>Part 4.5</b>	<b>Enhanced CDD and ongoing monitoring</b>	<b>53</b>
4.5.1	Enhanced CDD and ongoing monitoring	53
<b>Part 4.6</b>	<b>Reduced or simplified CDD</b>	<b>53</b>
4.6.1	Reduced or simplified CDD—general	53
4.6.2	Reduced or simplified CDD—financial institution customer	53
4.6.3	Reduced or simplified CDD—listed, regulated public companies	53
<b>Chapter 5</b>	<b>Reporting and tipping off</b>	<b>55</b>
<b>Part 5.1</b>	<b>Reporting requirements</b>	<b>55</b>
<b>Division 5.1.A</b>	<b>Reporting requirements</b>	<b>55</b>
5.1.1	Unusual and inconsistent transactions	55
<b>Division 5.1.B</b>	<b>Internal reporting</b>	<b>56</b>
5.1.2	Internal reporting policies	56
5.1.3	Access to MLRO	56
5.1.4	Obligation of officer or employee to report to MLRO	56
5.1.5	Obligations of MLRO on receipt of internal report	57

<b>Division 5.1.C</b>	<b>External reporting</b>	<b>58</b>
5.1.6	External reporting policies	58
5.1.7	Obligation of licensed party to report to FIU	58
5.1.8	Obligation not to destroy records relating to customer under investigation	59
5.1.9	Licensed party may restrict or terminate business relationship	60
<b>Division 5.1.D</b>	<b>Reporting records</b>	<b>60</b>
5.1.10	Reporting records to be made by MLRO	60
<b>Part 5.2</b>	<b>Tipping off</b>	<b>60</b>
5.2.1	What is tipping off?	60
5.2.2	Licensed party must ensure no tipping off occurs	61
5.2.3	Information relating to suspicious transaction reports to be safeguarded	61
<b>Chapter 6</b>	<b>Screening and training requirements</b>	<b>62</b>
<b>Part 6.1</b>	<b>Screening procedures</b>	<b>62</b>
6.1.1	Screening procedures—particular requirements	62
<b>Part 6.2</b>	<b>AML/CFT training programme</b>	<b>62</b>
6.2.1	Appropriate AML/CFT training programme to be delivered	62
6.2.2	Training must be maintained and reviewed	64
<b>Chapter 7</b>	<b>Providing documentary evidence of compliance</b>	<b>65</b>
<b>Part 7.1</b>	<b>General record-keeping obligations</b>	<b>65</b>
7.1.1	Records about compliance	65
7.1.2	How long records must be kept	65
7.1.3	Retrieval of records	66
<b>Part 7.2</b>	<b>Particular record-keeping obligations</b>	<b>66</b>
7.2.1	Records for customers and transactions	66
7.2.2	Training records	67
<b>Chapter 8</b>	<b>Miscellaneous</b>	<b>68</b>
8.1.1	Approved forms to be used	68
8.1.2	Completion of forms	68
<b>Annex</b>	<b>69</b>	

## Chapter 1 General provisions

### Part 1.1 Introductory

#### 1.1.1 Name of rules

These rules are the Anti-Money Laundering and Combating Terrorist Financing Rules 2010.

#### 1.1.2 Commencement

These rules come into effect on the date of their issuance. They are to be published in the official gazette.

#### 1.1.3 General application of these rules

- (1) These rules apply to licensed parties that conduct business or activities in the jurisdiction of the Regulator.
- (2) A reference in these rules to a *licensed party* is a reference to the party so far as it conducts business or activities in the jurisdiction of the Regulator, unless these rules otherwise provide.

#### 1.1.4 Annex

The annex at the end of these rules is part of these rules.

#### 1.1.5 Notes and examples

- (1) A note in or to these rules is explanatory and is not part of the rules.
- (2) An example in these rules—
  - (a) is not exhaustive; and
  - (b) may extend, but does not limit, the meaning of the rules or the particular part of the rules to which it relates.

### Part 1.2 Key AML/CFT principles

#### 1.2.1 Principle 1—senior management responsibility

The senior management of a licensed party must ensure that the party's policies, procedures, systems and controls appropriately and adequately address the requirements of the AML/CFT Law and these rules.

#### 1.2.2 Principle 2—risk-based approach

A licensed party must adopt a risk-based approach to these rules and their requirements.

### 1.2.3 Principle 3—know your customer

A licensed party must know each of its customers to the extent appropriate for the customer's risk profile.

### 1.2.4 Principle 4—effective reporting

A licensed party must have effective measures in place to ensure that there is internal and external reporting whenever money laundering or terrorist financing is known or suspected.

### 1.2.5 Principle 5—high standard screening and appropriate training

A licensed party must—

- (a) have adequate screening procedures to ensure high standards when appointing or employing officers and employees; and
- (b) have an appropriate ongoing AML/CFT training programme for its officers and employees.

### 1.2.6 Principle 6—evidence of compliance

A licensed party must be able to provide documentary evidence of its compliance with the requirements of the AML/CFT Law and these rules.

## Part 1.3 Key terms

### 1.3.1 What is a Regulator?

The Regulator is the Qatar Financial Markets Authority.

### 1.3.2 What is a licensed party?

A *licensed party* is a financial institution that has a licence granted by the Regulator.

### 1.3.3 What is a financial services institution?

A *financial services institution* is any entity that conducts, as a business, or more of the activities licensed by the Regulator,

### 1.3.4 Who is a customer?

A *customer* is a person who engages in a business transaction with the licensed party whether for himself or as agent for or on behalf of another person.

and, to remove any doubt, also includes a client or investor, or prospective client or investor.

### 1.3.5 Who is the *beneficial owner*?

- (1) The *beneficial owner* is—
  - (a) for an account—the individual who ultimately owns, or exercises effective control, over the account; or
  - (b) for a transaction—the individual for whom, or on whose behalf, the transaction is ultimately being, or is ultimately to be, conducted; or
  - (c) for a legal person the individual who ultimately owns, or exercises effective control over, the person
- (2) Without limiting subrule (1) (a), the *beneficial owner* for an account includes any individual in accordance with whose instructions any of the following are accustomed to act:
  - (a) the signatories of the account (or any of them);
  - (b) any individual who, directly or indirectly, instructs the signatories (or any of them).
- (3) Without limiting subrule (1) (c), the *beneficial owner* for a corporation includes—
  - (a) an individual who, directly or indirectly, owns or controls at least 25% of the shares or voting rights of the corporation; and
  - (b) an individual who, directly or indirectly, otherwise exercises control over the corporation’s management.
- (4) Without limiting subrule (1) (c), the *beneficial owner* for a legal arrangement that administers and distributes funds includes—
  - (a) if the beneficiaries and their distributions have already been decided—an individual who is to receive at least 25% of the funds of the arrangement; and
  - (b) if the beneficiaries or their distributions have not already been decided—the class of persons in whose main interest the arrangement is established or operated as beneficial owner; and
  - (c) an individual who, directly or indirectly, exercises control over at least 25% (by value) of the property of the arrangement.

### 1.3.6 Who is a *politically exposed person*?

- (1) A *politically exposed person (PEP)* is—
  - (a) an individual (A) who is, or has been, entrusted with prominent public functions in a foreign jurisdiction; or
  - (b) a family member of A; or
  - (c) a close associate of A.

- (2) In deciding whether a person is a close associate of A, a licensed party need only have regard to information that is in its possession or is publicly known.
- (3) Individuals *entrusted with prominent public functions* include the following:
  - (a) heads of state, heads of government, ministers and deputy or assistant ministers;
  - (b) members of parliament, other senior politicians and important political party officials;
  - (c) members of supreme courts, of constitutional courts, or of other high-level judicial bodies
  - (d) members of the boards of central banks;
  - (e) ambassadors and chargés d'affaires;
  - (f) high-ranking officers in the armed forces;
  - (g) members of administrative, management or supervisory bodies of state-owned enterprises (other than members who are middle ranking or more junior officials).
- (4) Without limiting subrule (1) (b), family members of A include the following:
  - (a) spouses;
  - (b) children and their spouses;
  - (c) parents.
- (5) Without limiting subrule (1) (c), close associates of A include the following:
  - (a) individuals who have joint beneficial ownership of a legal entity or legal arrangement, or any close business relations, with A;
  - (b) individuals with sole beneficial ownership of a legal entity or legal arrangement which has been set up for A's benefit.

### 1.3.7 What is a *correspondent securities relationship*?

*Correspondent securities relationship* is the provision of services in relation to securities provided by a licensed party to a financial institution in a foreign jurisdiction.

**Examples of services**

the buying, selling, lending or otherwise holding of securities

**Examples of financial institutions**

brokers, dealers or custodians (however described)

### 1.3.8 What is a *shell bank*?

- (5) A *shell bank* is a bank that—
- (a) has no physical presence in the jurisdiction in which it is incorporated and licensed (however described); and
  - (b) is not affiliated with a regulated financial services group that is subject to effective consolidated supervision.
- (6) For this rule, *physical presence* in a jurisdiction is a presence involving meaningful decision-making and management and not merely the presence of a local agent or low level staff.

*Note* *Jurisdiction* is defined in the glossary.

## Chapter 2

## General AML and CFT responsibilities

### Part 2.1

### The licensed party

#### 2.1.1 Licensed parties to develop AML/CFT programme

- (1) A licensed party must develop a programme against money laundering and terrorist financing.
- (2) The type and extent of the measures adopted by the licensed party as part of its programme must be appropriate having regard to the risk of money laundering and terrorist financing and the size, complexity and nature of its business.
- (3) However, the programme must, as a minimum, include the following:
  - (a) developing, establishing and maintaining internal policies, procedures, systems and controls to prevent money laundering and terrorist financing;
  - (b) adequate screening procedures to ensure high standards when appointing or employing officers or employees;
  - (c) an appropriate ongoing training programme for its officers and employees;
  - (d) an adequately resourced and independent audit function to test compliance with the licensed party's AML/CFT policies, procedures, systems and controls (including by sample testing);
  - (e) appropriate compliance management arrangements;
  - (f) the appropriate ongoing assessment and review of the policies, procedures, systems and controls.

#### 2.1.2 Policies etc must be risk-sensitive, appropriate and adequate

A licensed party's AML/CFT policies, procedures, systems and controls must be risk-sensitive, appropriate and adequate having regard to the risk of money laundering and terrorist financing and the size, complexity and nature of its business.

#### 2.1.3 Matters to be covered by policies etc

- (1) A licensed party's AML/CFT policies, procedures, systems and controls must, as a minimum, cover the following:
  - (a) customer due diligence measures and ongoing monitoring;

- (b) record making and retention;
  - (c) the detection of suspicious transactions;
  - (d) the internal and external reporting obligations;
  - (e) the communication of the policies, procedures, systems and controls to the party's officers and employees;
  - (f) anything else required under the AML/CFT Law and these rules.
- (2) Without limiting subrule (1), the licensed party's AML/CFT policies, procedures, systems and controls must—
- (a) provide for the identification and scrutiny of—
    - (i) complex or unusual large transactions, and unusual patterns of transactions, that have no apparent economic or visible lawful purpose; and
    - (ii) any other transactions that the licensed party considers particularly likely by their nature to be related to money laundering or terrorist financing; and
  - (b) require the taking of enhanced customer due diligence measures to prevent the use for money laundering or terrorist financing of products and transactions that might favour anonymity; and
  - (c) provide appropriate measures to reduce the risks associated with establishing business relationships with politically exposed persons; and
  - (d) before any function or activity is outsourced by the licensed party, require an assessment to be made and documented of the money laundering and terrorist financing risks associated with the outsourcing; and
  - (e) require the risks associated with the outsourcing of a function or activity by the licensed party to be monitored on an ongoing basis; and
  - (f) require everyone in the licensed party to comply with the requirements of the AML/CFT Law and these rules in relation to the making of suspicious transaction reports; and
  - (g) be designed to ensure that the licensed party can otherwise comply, and does comply, with the AML/CFT Law and these rules.

#### **2.1.4 Assessment and review of policies etc**

A licensed party must carry out regular assessments of the adequacy of, and at least annually review the effectiveness of, its AML/CFT policies, procedures, systems and controls in preventing money laundering and terrorist financing.

### **2.1.5 Compliance by officers, employees, agents etc**

- (1) A licensed party must ensure that its officers, employees, agents and contractors, wherever they are, comply with—
  - (a) the requirements of the AML/CFT Law and these rules; and
  - (b) its AML/CFT policies, procedures, systems and controls; except so far as the law of another jurisdiction prevents the application of this subrule.
- (2) Without limiting subrule (1), the licensed party's AML/CFT policies, procedures, systems and controls must—
  - (a) require officers, employees, agents and contractors, wherever they are, to provide suspicious transaction reports for transactions in, from or to the Regulator's jurisdiction to the licensed party's MLRO; and
  - (b) provide timely, unrestricted access by the licensed party's senior management and MLRO, and by the Regulator and FIU, to documents and information of the licensed party, wherever they are held, that relate directly or indirectly to transactions in, from or to the Regulator's jurisdiction; except so far as the law of another jurisdiction prevents the application of this subrule.
- (3) Subrule (2) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to the Regulator's jurisdiction.
- (4) This rule does not prevent the licensed party from applying higher, consistent standards in its AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend over a number of jurisdictions.
- (5) If the law of another jurisdiction prevents the application of a provision of this rule to an officer, employee, agent or contractor of the licensed party, the party must immediately tell the Regulator in writing about the matter.

### **2.1.6 Application of AML/CFT Law requirements, policies etc to branches and associates**

- (1) This rule applies to a licensed party if it has a branch in a foreign jurisdiction, or an associate in a foreign jurisdiction over which it can exercise control. The licensed party must ensure that the branch or associate, and the officers, employees, agents and contractors of the branch or associate, wherever they are, comply with—
  - (a) the requirements of the AML/CFT Law and these rules.; and

- (b) the licensed party's AML/CFT policies, procedures, systems and controls.;
- except so far as the law of another jurisdiction prevents the application of this subrule.
- (2) Without limiting subrule (2), the licensed party's AML/CFT policies, procedures, systems and controls must—
- (a) require the branch or associate approved by the Regulator, and the officers, employees, agents and contractors of the branch or associate approved by the Regulator, wherever they are, to provide suspicious transaction reports for transactions in, from or to the Regulator's jurisdiction or to the licensed party's MLRO; and
- (b) provide timely, unrestricted access by the licensed party's senior management and MLRO, and by the Regulator and FIU, to documents and information of the branch or associate approved by the Regulator, wherever they are held, that relate directly or indirectly to transactions in, from or to the Regulator's jurisdiction;
- except so far as the law of another jurisdiction prevents the application of this subrule.
- (3) Subrule (3) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to that jurisdiction.
- (4) Despite subrule (2), if the AML/CFT requirements of the Regulator's jurisdiction and another jurisdiction differ, the branch or associate approved by the Regulator must apply the requirements that impose the highest standard, except so far as the law of another jurisdiction prevents the application of this subrule.
- (5) Also, this rule does not prevent the licensed party and its branches or associates approved by the Regulator, or the other members of its group, from applying higher, and more consistent standards in their AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend across the licensed party and its branches or the licensed party and the other members of its group.
- (6) If the law of another jurisdiction prevents the application of a provision of this rule to the branch or associate or any of its officers, employees, agents or contractors, the licensed party must immediately tell the Regulator in writing about the matter.

### 2.1.7 Application of AML/CFT Law requirements, policies etc to outsourced functions and activities

- (1) This rule applies if a licensed party outsources any of its functions or activities to a third party.
- (2) The licensed party, and its senior management, remain responsible for ensuring that the AML/CFT Law and these rules are complied with.
- (3) The licensed party must, through a service level agreement ensure that the third party, and the officers, employees, agents and contractors of the third party, wherever they are, comply with the following in relation to the outsourcing:
  - (a) the requirements of the AML/CFT Law and these rules;
  - (b) the licensed party's AML/CFT policies, procedures, systems and controls;except so far as the law of another jurisdiction prevents the application of this subrule.
- (4) Without limiting subrule (3), the licensed party's AML/CFT policies, procedures, systems and controls must—
  - (a) require the third party, and the officers, employees, agents and contractors of the third party, wherever they are, to provide suspicious transaction reports for transactions in, from or to the Regulator's jurisdiction involving the licensed party (or the third party on its behalf) to the licensed party's MLRO; and
  - (b) provide timely, unrestricted access by the licensed party's senior management and MLRO, and by the Regulator and FIU, to documents and information of the third party, wherever they are held, that relate directly or indirectly to transactions in, from or to the Regulator's jurisdiction involving the licensed party (or the third party on its behalf);except so far as the law of another jurisdiction prevents the application of this subrule.
- (5) Subrule (4) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to the Regulator's jurisdiction.
- (6) If the law of another jurisdiction prevents the application of a provision of this rule to the third party or any of its officers, employees, agents or contractors—
  - (a) the third party must immediately tell the licensed party about the matter; and
  - (b) the licensed party must immediately tell the Regulator in writing about the matter.

## Part 2.2 Senior management

The senior management of a licensed party is required to ensure that the party's policies, procedures, systems and controls appropriately and adequately address the requirements of the AML/CFT Law and these rules.

### 2.2.1 Overall senior management responsibility

The senior management of a licensed party is responsible for the effectiveness of the party's policies, procedures, systems and controls in preventing money laundering and terrorist financing.

### 2.2.2 Particular responsibilities of senior management

- (1) The senior management of a licensed party must ensure the following:
  - (a) that the licensed party develops, establishes and maintains effective AML/CFT policies, procedures, systems and controls in accordance with these rules;
  - (b) that the licensed party has adequate screening procedures to ensure high standards when appointing or employing officers or employees;
  - (c) that the licensed party identifies, designs, delivers and maintains an appropriate ongoing AML/CFT training programme for its officers and employees;
  - (d) that the licensed party has an adequately resourced and independent audit function to test (including by sample testing) the effectiveness of, the party's AML/CFT policies, procedures, systems and controls;
  - (e) that regular and timely information is made available to senior management about the management of the licensed party's money laundering and terrorist financing risks;
  - (f) that the licensed party's money laundering and terrorist financing risk management policies and methodology are appropriately documented, including the party's application of them;
  - (g) that there is at all times an MLRO for the licensed party who—
    - (i) has sufficient seniority, experience and authority; and
    - (ii) is Resident in the State of Qatar.
    - (iii) has sufficient resources, including appropriate staff and technology to carry out the role in an effective, objective and independent way; and

- (iv) has timely, unrestricted access to all information of the licensed party relevant to AML and CFT, including, for example—
  - (A) all customer identification documents and all source documents, data and information; and
  - (B) all other documents, data and information obtained from, or used for, CDD and ongoing monitoring; and
  - (C) all transaction records; and
  - (D) has appropriate back-up arrangements to cover absences, including a deputy MLRO to act as MLRO;
  - (E) that a licensed party-wide AML/CFT compliance culture is promoted within the party;
  - (F) that appropriate measures are taken to ensure that money laundering and terrorist financing risks are taken into account in the day-to-day operation of the licensed party, including in relation to—
    - (i) The development of new products; and
    - (ii) The taking on of new customers; and
    - (iii) Changes in the licensed party's business profile.
- (2) This rule does not limit the particular responsibilities of the senior management of the licensed party.

## **Part 2.3 MLRO and deputy MLRO**

### **Division 2.3.A Appointment of MLRO and deputy MLRO**

#### **2.3.1 Appointment—MLRO and deputy MLRO**

The licensed party must appoint an individual as its MLRO and another individual as its deputy MLRO.

The licensed party must ensure that there is at all times an MLRO and a deputy MLRO for the party.

#### **2.3.2 Eligibility to be MLRO**

The MLRO for a licensed party must—

- (1) be employed at the management level by the licensed party, have sufficient seniority, experience and authority for the role, and in particular—
  - (a) to act independently; and

- (b) to report FIU along with notifying the Regulator if necessary.
- (2) be resident in Qatar.

## **Division 2.3.B Roles of MLRO and deputy MLRO**

### **2.3.3. General responsibilities of MLRO**

The MLRO for a licensed party is responsible for the following:

- (1) Oversighting the implementation of the licensed party's AML/CFT policies, procedures, systems and controls in relation to the jurisdiction
- (2) Ensuring that appropriate policies, procedures, systems and controls are developed, established and maintained across the licensed party to monitor the party's day-to-day operations—
  - (a) for compliance with the AML/CFT Law, these rules, and the licensed party's AML/CFT policies, procedures, systems and controls; and
  - (b) to assess, and regularly review, the effectiveness of the policies, procedures, systems and controls in preventing money laundering and terrorist financing;
- (3) Being the licensed party's key person in implementing the party's AML/CFT strategies in relation to the jurisdiction;
- (4) Supporting and coordinating senior management work on managing the licensed party's money laundering and terrorist financing risks in its business areas;
- (5) Helping ensure that the licensed party's responsibility for preventing money laundering and terrorist financing.
- (6) Promoting a licensed party-wide view to be taken of the need for AML/CFT monitoring and accountability.

### **2.3.4 Particular responsibilities of MLRO**

The MLRO is responsible for the following:

- (1) receiving, investigating and assessing internal suspicious transaction reports
- (2) making suspicious transaction reports to the FIU and telling the Regulator about them;
- (3) acting as central point of contact between the licensed party, and the FIU, the Regulator and other State authorities, in relation to AML and CFT issues;
- (4) responding promptly to any request for information by the FIU, the Regulator and other State authorities in relation to AML and CFT information

- (5) receiving and acting on government, regulatory and relevant international authorities findings about AML and CFT issues;
- (6) monitoring the appropriateness and effectiveness of the licensed party's AML/CFT training programme;
- (7) reporting to the licensed party's senior management on AML and CFT issues;
- (8) keeping the deputy MLRO informed of any significant AML/CFT developments (whether internal or external);
- (9) exercising any other functions given to the MLRO, whether under the AML/CFT Law, these rules or otherwise.

### **2.3.5 Role of deputy MLRO**

- (1) The deputy MLRO acts as the party's MLRO during absences of the MLRO and whenever there is a vacancy in the MLRO's position.
- (2) When the deputy MLRO acts as MLRO, the deputy MLRO is subject to the same rules that apply to the MLRO.

### **2.3.6 How MLRO must carry out role**

The MLRO must act honestly, reasonably and independently, particularly in—

- (1) receiving, investigating and assessing internal suspicious transaction reports; and
- (2) deciding whether to make, and making, suspicious transaction reports to the FIU.

## **Division 2.3.C Reporting by MLRO to senior management**

### **2.3.7 MLRO reports**

- (1) The senior management of a licensed party must, on a regular basis, decide what reports should be given to it by the MLRO, and when the reports should be given to it, to enable it to discharge its responsibilities under the AML/CFT Law and these rules.
- (2) However, a report that complies with rule 2.3.8 (Minimum annual report by MLRO) must be given to the senior management by the MLRO for each financial year of the licensed party and with sufficient promptness to enable the senior management to comply with rule 2.3.9 (2).
- (3) To remove any doubt, subrule (2) does not limit the reports—
  - (a) that the senior management may require to be given to it; or

- (b) that the MLRO may give to the senior management on the MLRO's own initiative to discharge the MLRO's responsibilities under the AML/CFT Law and these rules.

### **2.3.8 Minimum annual report by MLRO**

- (1) This rule sets out the minimum requirements that must be complied with in relation to the report that must be given to the senior management by the MLRO for each financial year of the licensed party (see rule 2.3.7 (2)).
- (2) The report must assess the adequacy and effectiveness of the licensed party's AML/CFT policies, procedures, systems and controls in combating money laundering and terrorist financing.
- (3) The report must include the following for the period to which it relates:
  - (a) the numbers and types of internal suspicious transaction reports made to the MLRO;
  - (b) the number of these reports that have, and the number of these reports that have not, been passed on to the FIU;
  - (c) the reasons why reports have or have not been passed on to the FIU;
  - (d) the numbers and types of breaches by the licensed party of the AML/CFT Law, these rules, or the party's AML/CFT policies, procedures, systems and controls;
  - (e) areas where the licensed party's AML/CFT policies, procedures, systems and controls should be improved, and proposals for making appropriate improvements;
  - (f) a summary of the AML/CFT training delivered to the licensed party's officers and employees;
  - (g) areas where the licensed party's AML/CFT training programme should be improved, and proposals for making appropriate improvements;
  - (h) the number and types of customers of the licensed party that are categorised as high risk;
  - (i) progress in implementing any AML/CFT action plans;
  - (j) the outcome of any relevant quality assurance or audit reviews in relation to the licensed party's AML/CFT policies, procedures, systems and controls;
  - (k) the outcome of any review of the licensed party's risk assessment policies, procedures, systems and controls.

### **2.3.9 Consideration of MLRO reports**

- (1) The senior management of a licensed party must, in a timely way

- 
- (a) consider each report made to it by the MLRO;
  - (b) if the report identifies deficiencies in the licensed party's compliance with the AML/CFT Law or these rules—make, approve, or document an action plan to remedy the deficiencies in a timely way.
- (2) For the report that must be given to the senior management for a financial year of the licensed party (see rule 2.3.7 (2)), the senior management must deal with the report in accordance with subrule (1) not later than one month after the day the licensed party's financial year ends.

## Chapter 3 The risk-based approach

### Part 3.1 The risk-based approach generally

Principle 2 (see 1.2.2) requires a licensed party to adopt a risk-based approach to these rules and their requirements.

#### 3.1.1 Licensed parties must conduct risk assessment and decide risk mitigation

A licensed party must—

- (a) conduct an assessment of the money laundering and terrorist financing risks that it faces (a **business risk assessment**), including, for example, risks arising from—
  - (i) the types of customers that it has (and proposes to have); and
  - (ii) the products and services that it provides (and proposes to provide); and
  - (iii) the technologies that it uses (and proposes to use) to provide those products and services; and
- (b) decide what action is needed to mitigate those risks.

#### 3.1.2 Approach to risk mitigation must be based on suitable methodology

- (1) The intensity of a licensed party's approach to the mitigation of its money laundering and terrorist financing risks must be based on a suitable methodology that addresses the risks that it faces.
- (2) A licensed party must be able to demonstrate that its threat assessment methodology—
  - (a) includes assessing the risk profile of the business relationship with its customers and
  - (b) is suitable for the size, complexity and nature of the licensed party's business; and
  - (c) is designed to enable the licensed party—
    - (i) to identify and recognise any changes in its money laundering and terrorist financing risks; and
    - (ii) to change its threat assessment methodology as needed; and
  - (d) includes assessing risks posed by—
    - (i) new products and services; and
    - (ii) new or developing technologies.

- (3) A licensed party must also be able to demonstrate that its practice matches its threat assessment methodology.

### 3.1.3 Risk profiling a business relationship

- (1) In developing the risk profile of a business relationship with a customer, a licensed party must consider at least the following 4 risk elements in relation to the relationship:
- (a) customer risk;
  - (b) product risk;
  - (c) interface risk;
  - (d) jurisdiction risk.
- (2) The licensed party must identify any other risk elements that are relevant to the business relationship, especially because of the size, complexity and nature of its business and any business of its customer.
- (3) The licensed party must also consider the risk elements (if any) identified under subrule (2) in relation to the business relationship.
- (4) Together the 4 risk elements mentioned in subrule (1), and any other risk elements identified under subrule (2), combine to produce the risk profile of the business relationship.
- (5) This risk profile must be taken into account in deciding the intensity of the customer due diligence measures and ongoing monitoring to be conducted for the customer.

## Part 3.2 Customer risk

This part relates to the risks posed by the types of customers of a licensed party.

### 3.2.1 Risk assessment for customer risk

- (1) A licensed party must assess and document the risks of money laundering, terrorist financing and other illicit activities posed by different types of customers.

#### Examples of types of customers

- 1 salaried employees with no other significant sources of income or wealth
  - 2 publicly listed companies
  - 3 legal arrangements
  - 4 politically exposed persons
- (2) The intensity of the customer due diligence measures and ongoing monitoring conducted for a particular customer must be proportionate to the perceived or potential level of risk posed by the relationship with that customer.

### 3.2.2 Policies etc for customer risk

A licensed party must have policies, procedures, systems and controls to address the specific risks of money laundering, terrorist financing and other illicit activities posed by different types of customers.

### 3.2.3 Scoring business relationships sources of wealth and funds

A licensed party must include, in its methodology, a statement of the basis on which business relationships with customers will be scored, having regard to their sources of wealth and funds.

### 3.2.4 Persons associated with terrorist acts etc—enhanced CDD and ongoing monitoring

- (1) This rule applies to a customer of a licensed party if the party knows or suspects that the customer is—
  - (a) an individual, charity, non-profit organisation or other entity that is associated with, or involved in, terrorist acts, terrorist financing or a terrorist organisation; or
  - (b) an individual or other entity that is subject to sanctions or other international initiatives.
- (2) Irrespective of the risk score otherwise obtained for the customer, the licensed party must conduct enhanced customer due diligence measures and enhanced ongoing monitoring for the customer.
- (3) A decision to enter into a business relationship with the customer must only be taken with senior management approval after enhanced customer due diligence measures have been conducted.

### 3.2.5 Measures for politically exposed persons

A licensed party must, as a minimum, adopt the following measures to reduce the risks associated with establishing and maintaining business relationships with politically exposed persons (*PEPs*):

- (1) The licensed party must have clear policies, procedures, systems and controls for business relationships with PEPs.
- (2) The licensed party must establish and maintain an appropriate risk management system to decide whether a potential or existing customer, or the beneficial owner of a potential or existing customer, is a PEP;

#### Examples of measures forming part of a risk management system

- 1 seeking relevant information from customers
  - 2 referring to publicly available information
  - 3 having access to, and referring to, commercial electronic databases of PEPs.
- (3) Decisions to enter into business relationships with PEPs must only be taken with senior management approval after enhanced customer due diligence measures have been conducted for PEPs;

- (4) If an existing customer, or the beneficial owner of an existing customer, is subsequently found to be, or to have become, a PEP—the relationship may be continued with senior management approval;
- (5) The licensed party must take reasonable measures to establish the sources of wealth and funds of customers and beneficial owners identified as PEPs;
- (6) PEPs must be subject to enhanced ongoing monitoring.

### **3.2.6 Legal persons, legal arrangements and facilities—risk assessment process**

- (1) A licensed party's risk assessment process must include recognition of the risks posed by legal persons, legal arrangements and facilities.
- (2) In assessing the risks posed by a legal person or legal arrangement, a licensed party must ensure that the risks posed by any beneficial owners, officers, shareholders, trustees, settlors, beneficiaries, managers and other relevant entities are reflected in the risk profile of the person or arrangement.
- (3) In assessing the risks posed by a facility, a licensed party must ensure that the risks posed by any reduction in transparency, or any increased ability to conceal or obscure, are reflected in the facility's risk profile.
- (4) Subrules (2) and (3) do not limit the matters to be reflected in the risk profile of a legal person, legal arrangement or facility.

## Part 3.3 Product risk

- 1 This part relates to the risks posed by the types of products offered by companies.
- 2 Product includes the provision of a service

### 3.3.1 Risk assessment for product risk

- (1) A licensed party must assess and document the risks of money laundering, terrorist financing and other illicit activities posed by the types of products it offers (or proposes to offer).
- (2) The intensity of the customer due diligence measures and ongoing monitoring required in relation to a particular type of product must be proportionate to the perceived or potential level of risk posed by the type of product.

### 3.3.2 Policies etc for product risk

A licensed party must have policies, procedures, systems and controls to address the specific risks of money laundering, terrorist financing and other illicit activities posed by the types of products it offers (or proposes to offer).

### 3.3.3 Scoring business relationships—types of products

A licensed party must include, in its methodology, a statement of the basis on which business relationships with customers will be scored, having regard to the types of products it offers (or proposes to offer) to them.

### 3.3.4 Products with fictitious or false names or no names

- (1) A licensed party must not permit any of its products to be used if the product—
  - (a) Uses a fictitious or false name for a customer; or
  - (b) Does not identify the customer's name.
- (2) Subrule (1) does not prevent the licensed party from providing a level of privacy to the customer within the licensed party itself by not including the customer's name or details on the account name or customer file if—
  - (a) Records of the customer's details are kept in a more secure environment in the licensed party itself; and
  - (b) The records are available to the licensed party's senior management and MLRO, and to the Regulator and FIU.
- (3) Without limiting subrule (1), if the licensed party has numbered accounts, the party must maintain them in a way that enables it to fully comply with the AML/CFT Law and these rules.

#### Example for r (3)

The licensed party could properly identify the customer for an account in accordance with the AML/CFT Law and these rules and make the

customer identification records available to the MLRO of the licensed party the Regulator and the FIU.

### 3.3.5 Correspondent securities relationships generally

- (1) Before a licensed party establishes a correspondent securities relationship with a financial services corporation in a foreign jurisdiction, the licensed party must do all of the following:
  - (a) gather sufficient information about the foreign financial services corporation to understand fully the nature of its business;
  - (b) decide from publicly available information the foreign financial services corporation's reputation and the quality of its regulation and supervision;
  - (c) assess the respondent's AML/CFT policies, procedures, systems and controls, and decide that they are adequate and effective;
  - (d) obtain senior management approval to establish the relationship;
  - (e) document its responsibilities and those of the foreign financial services corporation, including in relation to AML and CFT matters;
  - (f) be satisfied that, in relation to the foreign financial services corporation's customers that will have direct access to accounts of the licensed party, the foreign financial services corporation—
    - (i) will have conducted customer due diligence measures for the customers and verified the customers' identities;
    - (ii) will conduct ongoing monitoring for the customers;
    - (iii) will be able to provide to the licensed party, on request, the documents, data or information obtained in conducting CDD and ongoing monitoring for the customers.
- (2) Without limiting subrule (1) (b), in making a decision for that provision, the licensed party must consider all of the following:
  - (a) Whether the foreign financial services corporation has been the subject of any investigation, or civil or criminal proceeding, relating to money laundering or terrorist financing;
  - (b) The foreign financial services corporation's financial position;
  - (c) Whether it is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalent to the Regulator in each foreign jurisdiction in which it operates;
  - (d) Whether each foreign jurisdiction has an effective AML/CFT regime;

if the foreign financial services corporation is a subsidiary of another legal person—the following additional matters:

- (i) the other person's domicile and location (if different);
  - (ii) its reputation;
  - (iii) whether it is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalent to the Regulator in each jurisdiction in which it operates;
  - (iv) whether each foreign jurisdiction in which it operates has an effective AML/CFT regime;
  - (v) its ownership, control and management structure (including whether it is owned, controlled or managed by a politically exposed person).
- (3) If the licensed party establishes a correspondent securities relationship with the foreign financial services corporation, the party must—
- (a) If the foreign financial services corporation is in a high risk jurisdiction—conduct enhanced ongoing monitoring of the volume and nature of the transactions conducted under the relationship; and
  - (b) In any case—at least annually review the relationship and the transactions conducted under it.

### **3.3.6 Shell banks**

- (1) A licensed party must not enter into, or continue, a correspondent securities relationship with a shell bank.
- (2) A licensed party must ensure that it does not enter into, or continue, a correspondent securities relationship with a financial services company in any jurisdiction if that financial services company is known to permit its accounts to be used by a shell bank.

### **3.3.7 Payable through accounts**

- (1) The rule applies if—
  - (a) A licensed party has a correspondent securities relationship with a broker or dealer foreign financial services corporation) in a foreign jurisdiction; and
  - (b) Under the relationship, a customer of the foreign financial services corporation who is not a customer of the licensed party may have direct access to an account of the party.
- (2) The licensed party must not allow the customer to have access to the account unless the party is satisfied that the foreign financial services corporation
  - (a) has conducted customer due diligence measures for the customer and verified the customer's identity; and

- (b) conducts ongoing monitoring for the customer; and
  - (c) can provide to the licensed party, on request, the documents, data or information obtained in conducting CDD and ongoing monitoring for the customer.
- (3) If—
- (a) the licensed party asks the respondent for documents, data or information mentioned in subrule (2) (c); and
  - (b) the foreign financial services corporation fails to satisfactorily comply with the request;
- the licensed party must immediately terminate the customer's access to accounts of the licensed party and consider making a suspicious transaction report to the FIU.

### 3.3.8 Power of attorney

- (1) This rule applies to a power of attorney if it authorises the holder to exercise control over assets of the grantor.
- (2) Before dealing in a transaction involving the power of attorney, a licensed party must conduct customer due diligence measures for both the holder and the grantor.
- (3) For subrule (2), the holder and the grantor are both taken to be customers of the licensed party.

### 3.3.9 Bearer shares and share warrants to bearer

- (1) In this rule:
  - bearer instrument* means—
    - (a) a bearer share; or
    - (b) a share warrant to bearer.
- (2) A licensed party must have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to the use of bearer instruments.
- (3) Before becoming involved in or associated with a transaction involving the conversion of a bearer instrument to registered form, or the surrender of coupons for a bearer instrument for payment of dividend, bonus or a capital event, a licensed party must conduct enhanced customer due diligence measures for the holder of the instrument and any beneficial owner.
- (4) For subrule (3), the holder and any beneficial owner are taken to be customers of the licensed party.

### 3.3.10 Wire transfers

- (1) This rule applies to a transaction conducted by a financial institution (X) by electronic means on behalf of a person (the *originator*) with a view to making an amount of money available

to a person (the *recipient*) at another financial institution (*Y*). The transaction conducted from or to an account maintained by a licensed party for the originator or the recipient in his capacity of customer.

- (2) This rule applies to the transaction whether or not—
  - (a) the originator and recipient are the same person; or
  - (b) the transaction is conducted through intermediary financial institutions; or
  - (c) X, Y or any intermediary financial institution is outside Qatar.
- (3) However, this rule does not apply if the originator and recipient are both financial institutions acting on their own behalf.
- (4) The licensed party must—
  - (a) obtain and keep full originator and recipient information; and
  - (b) conduct customer due diligence measures for the originator;
  - (c) where receiving a wire transfer that is not accompanied by complete originator information, and using a risk-sensitive approach, decide whether a suspicious transaction report should be made to the FIU.

*Note* See div 5.1C (External reporting).

- (5) In this rule:  
*full originator and recipient information* means the following information:
  - (a) account number
  - (b) full name;
  - (c) residency address;
  - (d) valid identity number;
  - (e) nationality;
  - (f) date and place of birth.

## Part 3.4 Interface risk

This part relates to the risks posed by the mechanisms through which business relationships with a licensed party are started or conducted.

## Division 3.4.A Interface risks—general

### 3.4.1 Risk assessment for interface risk

- (1) A licensed party must assess and document the risks of money laundering, terrorist financing and other illicit activities posed by the mechanisms through which its business relationships are started and conducted.
- (2) The intensity of the customer due diligence measures and ongoing monitoring conducted in relation to a particular mechanism must be proportionate to the perceived or potential level of risk posed by the mechanism.

### 3.4.2 Policies etc for interface risk , etc.

- (1) A licensed party must have customer due diligence policies, procedures, systems and controls to address the specific risks of money laundering, terrorist financing and other illicit activities posed by the types of mechanisms through which its business relationships are started and conducted.
- (2) Without limiting subrule (1), the policies, procedures, systems and controls must include measures—
  - (a) to prevent the misuse of technological developments in money laundering and terrorist financing schemes; and
  - (b) to manage any specific risks associated with non-face to face business relationships or transactions.

#### Examples of non-face to face business relationships or transactions

- 1 business relationships concluded over the Internet or through the post
- 2 services and transactions provided or conducted over the Internet, or by telephone or fax.

#### Examples of policies, procedures, systems and controls for par (b)

- 1 requiring third party certification of identification documents presented by or for non-face to face customers
- 2 requiring additional identification documents for non-face to face customers
- 3 developing independent contact with non-face to face customers

- (3) The policies, procedures, systems and controls must apply in relation to establishing business relationships and conducting ongoing monitoring.

### 3.4.3 Scoring business relationships—interface risk

A licensed party must include, in its methodology, a statement of the basis on which business relationships with customers will be scored, having regard to the mechanisms through which its business relationships are started or conducted.

### 3.4.4 Electronic verification of identification documentation

- (1) A licensed party may rely on electronic verification of identification documentation if it complies with the risk-based approach and other requirements of these rules.

- (2) However, the licensed party must make and keep a record that clearly demonstrates the basis on which it relied on the electronic verification of identification documentation.

### **3.4.5 Payment processing using on-line services**

A licensed party may permit payment processing to take place using on-line services if it ensures that the processing is subject to—

- (1) the same monitoring as its other services; and
- (2) the same risk-based methodology.

## **Division 3.4.B Reliance on others generally**

### **3.4.6 Activities to which DIV 3.4B does not apply**

This division does not apply to a licensed party in relation to customer due diligence measures conducted for the party—

- (1) By a third-party service provider under an outsourcing; or
- (2) By an agent under a contractual arrangement between the licensed party and the agent
- (3) If the licensed party is a bank under a correspondent banking relationship to which the licensed party is a party.

### **3.4.7 Reliance on certain third parties generally**

- (1) A licensed party may rely on introducers, intermediaries or other third parties to conduct some elements of customer due diligence measures for a customer, or to introduce business to the licensed party, if it does so under, and in accordance with, this division.
- (2) However, the licensed party (and, in particular, its senior management) remains responsible for the proper conduct of CDD and ongoing monitoring for its customers.

### **3.4.8 Introducers**

- (1) This rule applies in relation to a customer introduced to a licensed party by a third party (the *introducer*) if—
  - (a) the introducer's function in relation to the customer is merely to introduce the customer to the licensed party; and
  - (b) the licensed party is satisfied that the introducer—
    - (i) is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction; and
    - (ii) is subject to the AML/CFT Law and these rules or to equivalent legislation of another jurisdiction; and

- (iii) is based, or incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime; and
  - (iv) is not subject to a secrecy law or anything else that would prevent the licensed party from obtaining any information or original documentation about the customer that the party may need for AML and CFT purposes.
- (2) The licensed party may rely on the customer due diligence measures conducted by the introducer for the customer and need not—
  - (a) conduct CDD itself for the customer; or
  - (b) obtain any of the original documents obtained by the introducer in conducting CDD for the customer.
- (2) However, the licensed party must not start a business relationship with the customer relying on subrule (2) unless—
  - (a) it has received from the introducer an introducer's certificate for the customer; and
  - (b) it has received from the introducer all information about the customer obtained from the CDD conducted by the introducer for the customer that it would need if it had conducted the CDD itself; and
  - (c) it has, or can immediately obtain from the introducer on request, a copy of every document relating to the customer that it would need if it were conducting CDD itself for the customer.

#### 3.4.9 Group introductions

- (1) This rule applies in relation to a customer introduced to a licensed party by a financial institution (**B**) in the same group, whether in or outside Qatar, if—
  - (a) B or another financial institution in the group has conducted customer due diligence measures for the customer; and
  - (b) The licensed party is satisfied that all of the following conditions have been met:
    - (i) the relevant financial institution is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction; and
    - (ii) it is subject to the AML/CFT Law and these rules or to equivalent legislation of another jurisdiction; and
    - (iii) it is based, or incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime; and

- (iv) the licensed party has all information about the customer obtained from the CDD conducted by the relevant financial institution for the customer that the party would need if it had conducted the CDD itself; and
  - (v) the licensed party has, or can immediately obtain from the relevant financial institution on request, a copy of every document relating to the customer that it would need if it were conducting CDD itself for the customer.
- (2) The licensed party may rely on the customer due diligence measures conducted by the relevant financial institution and need not—
- (a) Conduct CDD itself for the customer; or
  - (b) Obtain any of the original documents obtained by the relevant financial institution in conducting CDD for the customer.

#### 3.4.10 Intermediaries

- (1) This rule applies to a licensed party in relation to a customer of an intermediary, wherever located, if the customer is introduced to the party by the intermediary.
- Example of intermediary**
- a fund manager who has an active, ongoing business relationship with a customer in relation to the customer's financial affairs in the securities field and holds assets on the customer's behalf
- (2) The licensed party may treat the intermediary as its customer, and need not conduct customer due diligence measures itself for the intermediary's customer, if the party is satisfied that all of the following conditions have been met:
- (a) the intermediary is a financial institution
  - (b) it is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction;
  - (c) it is subject to the AML/CFT Law and these rules or to equivalent legislation of another jurisdiction; and
  - (d) it is based, or incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime;
  - (e) the licensed party has all information about the customer obtained from the CDD conducted by the intermediary for the customer that the party would need if it had conducted the CDD itself;
  - (f) the licensed party has, or can immediately obtain from the intermediary on request, a copy of every document relating to

the customer that it would need if it were conducting CDD itself for the customer.

- (3) If the licensed party is not satisfied that all of the conditions in subrule (2) have been met, the party must conduct customer due diligence measures itself for the customer.

## **Division 3.4.C Third party certification— identification documents**

### **3.4.11 Third party certification of identification documents**

- (1) A licensed party must not rely, for customer due diligence measures, on the certification of an identification document by a third party rather than sighting the document itself unless it is reasonable for it to rely on that certification.
- (2) Without limiting subrule (1), the licensed party must not rely on the certification of an identification document by a third party unless the third party is an individual approved under subrule (3).
- (3) The senior management of the licensed party may approve an individual under this subrule if the party's MLRO has certified that the MLRO is satisfied, on the basis of satisfactory documentary evidence, that the individual—
- (a) adheres to appropriate ethical or professional standards; and
  - (b) is readily contactable; and
  - (c) conducts his or her occupation or profession in Qatar or a foreign jurisdiction with an effective AML/CFT regime.

## **Part 3.5 Jurisdiction risk**

This part relates to the risks posed by the types of jurisdiction with which customers are (or may become) associated.

### **3.5.1 Risk assessment for jurisdiction risk**

- (1) A licensed party must assess and document the risks of involvement in money laundering, terrorist financing and other illicit activities posed by the different types of jurisdictions with which its customers are (or may become) associated.

#### **Examples of 'associated' jurisdictions for a customer**

- 1 the jurisdiction where the customer lives or is incorporated or otherwise established
  - 2 each jurisdiction where the customer conducts business or has assets
- (2) The intensity of the customer due diligence measures and ongoing monitoring conducted for customers associated with a particular

jurisdiction must be proportionate to the perceived or potential level of risk posed by the jurisdiction.

**Examples of jurisdictions requiring enhanced CDD**

- 1 jurisdictions with ineffective AML/CFT regimes
- 2 jurisdictions with impaired international cooperation
- 3 jurisdictions subject to international sanctions
- 4 jurisdictions with high propensity for corruption

### **3.5.2 Policies etc for jurisdiction risk**

A licensed party must have policies, procedures, systems and controls to address the specific risks of money laundering, terrorist financing and other illicit activities posed by the types of jurisdictions with which its customers are (or may become) associated.

### **3.5.3 Scoring business relationships—types of associated jurisdictions**

A licensed party must include, in its methodology, a statement of the basis on which business relationships with customers will be scored, having regard to the types of jurisdictions with which customers are (or may become) associated.

### **3.5.4 Decisions about effectiveness of AML/CFT regimes in other jurisdictions**

- (1) This rule applies to a licensed party in making a decision about whether a jurisdiction has an effective AML/CFT regime.
- (2) The licensed party must consider the following 3 factors in relation to the jurisdiction:
  - (a) legal framework;
  - (b) enforcement and supervision;
  - (c) international cooperation.
- (3) In considering these 3 factors, the licensed party must have regard to the relevant findings about jurisdictions published by international organisations, governments and other bodies.

### **3.5.5 Jurisdictions with impaired international cooperation**

A licensed party must guard against customers or introductions from jurisdictions where the ability to cooperate internationally is impaired and must, therefore, subject business relationships from these jurisdictions to enhanced customer due diligence measures and enhanced ongoing monitoring.

### **3.5.6 Non-cooperative, high risk and sanctioned jurisdictions**

A licensed party must conduct enhanced customer due diligence measures and enhanced ongoing monitoring in relation to transactions

conducted under a business relationship if a source of wealth or funds of the relationship derives from a jurisdiction—

- (1) that is identified by FATF as a non-cooperative country or territory, or
- (2) that is subject to international sanctions.

### **3.5.7 Jurisdictions with high propensity for corruption**

- (1) A licensed party must—
  - (a) assess and document the jurisdictions that are more vulnerable to corruption; and
  - (b) conduct enhanced customer due diligence measures and enhanced ongoing monitoring for customers from high risk jurisdictions whose line of business is more vulnerable to corruption.
- (2) If a licensed party's policy permits the acceptance of politically exposed persons as customers, the party must take additional measures to mitigate the additional risk posed by PEPs from jurisdictions with a high propensity for corruption.

## Chapter 4 Know your customer

### Part 4.1 Know your customer—

The licensed party is required to know each of its customers to the extent appropriate for the customer's risk profile.

#### 4.1.1 Know your customer principle—

The know your customer principle requires every licensed party to know who its customers are, and have the necessary customer identification documentation, data and information to evidence this.

Principle 6 (see r 1.2.6) requires a licensed party to be able to provide documentary evidence of its compliance with the requirements of the AML/CFT Law and these rules.

#### 4.1.2 Overview of CDD requirements

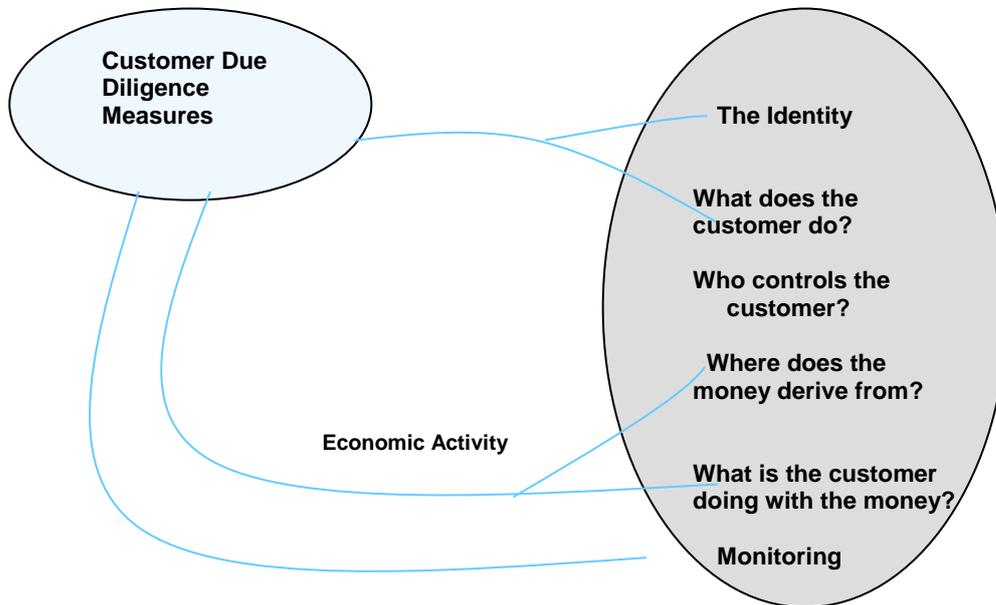
- (1) As a general rule, a licensed party must not establish a business relationship with a customer unless—
  - (a) all the relevant parties (including any beneficial owner) have been identified and verified; and
  - (b) the purpose and intended nature of the business expected to be conducted with the customer has been clarified.
- (2) Once an ongoing relationship has been established, any regular business undertaken with the customer must be assessed at regular intervals against the expected pattern of activity of the customer. Any unexpected activity can then be examined to decide whether there is a suspicion of money laundering or terrorist financing.
- (3) If the licensed party does not obtain satisfactory evidence of identity for all the relevant parties, the party must not establish the business relationship or carry out a transaction for or with them and must consider making a suspicious transaction report to the FIU.
- (4) This rule provides a simplified explanation of some of the customer due diligence requirements in this chapter and is subject to the more detailed provisions of this chapter.

#### 4.1.3 Customer identification documents

The application of customer due diligence measures to a customer should result in the licensed party obtaining a set of documents which are collectively known as the 'customer identification documents'. These documents, which are summarised in figure 4.1.3, form the basis of the licensed party's knowledge of the customer and should drive the risk-profiling and therefore the intensity of the customer due diligence

measures and ongoing monitoring the party must conduct for the customer.

**Figure 4.1.3 Customer identification documents**



## Part 4.2 Know your customer—key terms

### 4.2.1 What are customer due diligence measures?

- (1) *Customer due diligence measures* (or *CDD*), in relation to a customer of a licensed party, are all of the following measures:
- (a) identifying the customer;
  - (b) verifying the customer's identity using reliable, independent source documents, data or information;
  - (c) establishing whether the customer is acting on behalf of another person;
  - (d) if the customer is acting on behalf of another person (*A*)—the following additional measures:
    - (i) verifying that the customer is authorised to act on behalf of *A*;
    - (ii) identifying *A*;
    - (iii) verifying *A*'s identity using reliable, independent source documents, data or information;
  - (e) if the customer is a legal person or legal arrangement—the following additional measures:

- (i) verifying that any person (**B**) purporting to act on behalf of the customer is authorised to act on behalf of the customer;
  - (ii) identifying B;
  - (iii) verifying B's identity using reliable, independent source documents, data or information;
  - (iv) verifying the legal status of the customer;
  - (v) taking reasonable measures, on a risk-sensitive basis—
    - (A) to understand the customer's ownership and control structure; and
    - (B) to establish the individuals who ultimately own or control the customer, including the individuals who exercise ultimate effective control over the customer;
  - (f) establishing whether B is the beneficial owner;
  - (g) if B is not the beneficial owner (**C**)—the following additional measures:
    - (i) identifying C;
    - (ii) verifying C's identity using reliable, independent source documents, data or information;
    - (iii) if C is a legal person or legal arrangement—taking the additional measures mentioned in paragraph (e) (iv) and (v) as if it were the customer;
  - (h) obtaining information about the sources of the customer's wealth and funds;
  - (i) obtaining information on the purpose and intended nature of the business relationship.
- (2) For subrule (1) (e) (5) (B), examples of the type of measures required are—
- (a) if the customer is a company—identifying the individuals with a controlling interest and the individuals who comprise the mind and management of the customer; and
  - (b) if the customer is a trust—identifying the settlor, the protector, the trustee and any person exercising effective control over the trust, and the beneficiaries.

#### 4.2.2 What is *ongoing monitoring*?

*Ongoing monitoring*, in relation to a customer of a licensed party, consists of the following:

- (1) scrutinising transactions conducted under the business relationship with the customer to ensure that the transactions are consistent with the licensed party's knowledge of the customer, the customer's business and risk profile, and, where necessary, the source of the customer's wealth and funds;
- (2) reviewing the licensed party's records of the customer to ensure that documents, data and information collected using customer due diligence measures and ongoing monitoring for the customer are kept up-to-date and relevant.

#### 4.2.3 Who is an *applicant for business*?

An *applicant for business*, in relation to a licensed party, is a person seeking to form a business relationship with the party.

##### Examples of applicants for business

- 1 A person dealing with a licensed party on his or her own behalf is an applicant for business for the party.
- 2 If a person (**B**) provides funds to a licensed party and wants an investment purchased with the funds to be registered in the name of another person (eg a grandchild), B (and not the other person) is an applicant for business for the party.
- 3 If an intermediary introduces a client to a licensed party as a potential investor and gives the client's name as the investor, the client (and not the intermediary) is an applicant for business for the party.
- 4 If a person seeks advice from a licensed party in his or her own name and on his or her own behalf, the person is an applicant for business for the party.
- 5 If a professional agent introduces a third party to a licensed party so the third party can be given advice or make an investment in his or her own name, the third party (and not the professional agent) is an applicant for business for the party.
- 6 If an individual claiming to represent a company, partnership or other legal person applies to a licensed party to conduct business on behalf of the legal person, the legal person (and not the individual claiming to represent it) is an applicant for business for the party.
- 7 If a company manager or company formation agent (**C**) introduces a client company to a licensed party, the client company (and not C) is an applicant for business for the party.
- 8 If a trust is introduced to a licensed party, the settlor of the trust is an applicant for business for the party.

#### 4.2.4 What is a *business relationship*?

A *business relationship*, in relation to a licensed party, is a business, professional or commercial relationship between the licensed party and a customer, other than a relationship that is reasonably expected by the party, when contact is established, to be merely transitory.

## Part 4.3 Customer due diligence measures and ongoing monitoring

### 4.3.1 When CDD required—basic requirement

A licensed party must conduct customer due diligence measures for a customer when —

- (a) it establishes a business relationship with the customer; or
- (b) it suspects the customer of money laundering or terrorist financing; or
- (c) it has doubts about the veracity or adequacy of documents, data or information previously obtained in relation to the customer for the purposes of identification or verification.

### 4.3.2 Licensed party unable to complete CDD for customer

- (1) This rule applies if a licensed party cannot complete customer due diligence measures for a customer.

#### Examples

- 1 the licensed party is unable to verify the customer's identity using reliable, independent source, data or information
- 2 the customer exercises cancellation or cooling-off rights

- (2) The licensed party must—

- (a) immediately terminate any relationship with the customer and consider whether it should make a suspicious transaction report to the FIU

### 4.3.3 When CDD may not be required—acquired businesses

- (1) This rule applies if a licensed party acquires the business of another licensed party, either in whole or as a product portfolio
  - (2) The licensed party is not required to conduct customer due diligence measures for all customers acquired with the business if—
    - (a) all customer account records are acquired with the business; and
    - (b) due diligence inquiries before the acquisition did not give rise to doubt that the AML/CFT procedures followed for the business were being conducted in accordance the AML/CFT Law and these rules or the law of another jurisdiction that has an effective AML/CFT regime.
- (1) However, if the AML/CFT procedures followed by the acquired business were not conducted (or it is not possible to establish whether they were conducted) in accordance with the AML/CFT Law and these rules or the law of another jurisdiction that has an effective AML/CFT regime, the

licensed party's senior management must prepare or approve, and document, an action plan that ensures that the party conducts customer due diligence measures for all of the customers acquired with the business as soon as possible.

- (2) Also, if subrule (3) does not apply, but full customer records are not available to the licensed party for all of the customers acquired with the business, the party's senior management must prepare or approve, and document, an action plan that ensures that the party conducts customer due diligence measures for all of the customers for whom full customer records are not available to the party as soon as possible.

#### 4.3.4 Timing of CDD—establishment of business relationship

- (1) A licensed party must conduct customer due diligence measures for a customer before it establishes a business relationship with the customer.
- (2) However, the customer due diligence measures may be conducted during the establishment of the relationship if—
- (a) this is necessary in order not to interrupt the normal conduct of business; and

**Examples of where it may be necessary in order not to interrupt the normal conduct of business**

- 1 non-face to face business
- 2 securities transactions

- (b) there is little risk of money laundering or terrorist financing and these risks are effectively managed; and

**Examples of measures to effectively manage risks**

- 1 limiting the number, types and amount of transactions that may be conducted during the establishment of the relationship
- 2 monitoring large or complex transactions being carried out outside the expected norms for the relationship

- (c) they are completed as soon as practicable after contact is first established with the customer.

- (3) If the licensed party establishes a business relationship with the customer under subrule (2), but cannot complete customer due diligence measures for the customer, the licensed party must—

- (a) immediately terminate any relationship with the customer; and
- (b) consider whether it should make a suspicious transaction report to the FIU.

#### 4.3.5 When CDD required—additional requirement for existing customers

- (1) A licensed party must conduct customer due diligence measures for existing customers at other appropriate times on a risk-sensitive basis.

- (2) Without limiting subrule (1), a licensed party must conduct customer due diligence measures for an existing customer if there is a material change in the nature or ownership of the customer.
- (3) Without limiting subrule (2), a licensed party must decide whether to conduct customer due diligence measures for a customer if—
  - (a) the licensed party's customer documentation standards change substantially; or
  - (b) there is a material change in the way an account is operated or in any other aspect of the business relationship with the customer; or
  - (c) a significant transaction with or for the customer is about to take place; or
  - (d) the licensed party becomes aware that it lacks sufficient information about the customer.

#### **4.3.6 Extent of CDD—general requirement**

- (1) A licensed party must—
  - (a) decide, the extent of customer due diligence measures for a customer on a risk-sensitive basis depending on, among other factors, the customer risk, the product risk, and the jurisdiction risk; and
  - (b) be able to demonstrate to the Regulator that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.
- (2) Without limiting subrule (1), a licensed party must conduct enhanced customer due diligence measures for a customer if, for example, the business relationship of the customer is assessed as carrying a higher money laundering or terrorist financing risk.

#### **4.3.7 Extent of CDD—legal persons and arrangements**

- (1) This rule applies if a licensed party is required to conduct customer due diligence measures for a legal person (other than a corporation) or a legal arrangement.
- (2) If the licensed party identifies the class of persons in whose main interest the legal person or legal arrangement is established or operated as a beneficial owner, the party is not required to identify all the members of the class.
- (3) However, if the customer due diligence measures are required to be conducted for a trust and the beneficiaries and their contributions have already been decided, the licensed party must identify each beneficiary who is to receive at least 25% of the funds of the trust (by value).

#### 4.3.8 Ongoing monitoring required

- (1) A licensed party must conduct ongoing monitoring for each customer.
- (2) Without limiting subrule (1), the licensed party must pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.
- (3) The licensed party must examine as far as possible the background and purpose of a transaction mentioned in subrule (2) and make a record of its findings.
- (4) A record made for subrule (2) must be kept for at least 6 years after the day it is made or, if any other provision of these rules requires the record to be kept for a longer period, this provision shall be put in effect.

This rule is subject to rule 5.2.2 (2) (Licensed party must ensure no tipping off occurs).

#### 4.3.9 Procedures for ongoing monitoring

- (1) A licensed party must have policies, procedures, systems and controls for ongoing monitoring for its customers.
- (2) The systems and controls must—
  - (a) flag transactions for further examination; and
  - (b) provide—
    - (i) for the prompt further examination of these transactions by a senior independent person; and
    - (ii) for appropriate action to be taken on the findings of the further examination; and
    - (iii) if there is knowledge or suspicion of money laundering or terrorist financing raised by the findings—for a report to be made promptly to the licensed party's MLRO.
- (3) The monitoring provided by the systems and controls may be—
  - (a) in real time, that is, transactions are reviewed as they take place or are about to take place; or
  - (b) after the event, that is, transactions are reviewed after they have taken place.
- (4) The monitoring may be, for example—
  - (a) by reference to particular types of transactions or the customer's risk profile; or
  - (b) by comparing the transactions of the customer, or the customer's risk profile, with those of customers in a similar peer group; or
  - (c) through a combination of those approaches.

## **Part 4.4 Customer identification documentation**

### **Division 4.4. A Customer identification documentation—general**

#### **4.4.1 Elements of customer identification documentation**

Customer identification documentation relates to 2 distinct elements, namely—

- (a) the customer as a physical person; and
- (b) the nature of the customer’s economic activity.

#### **4.4.2 Records of customer identification documentation etc**

- (1) A licensed party must make and keep a record of all the customer identification documentation that it obtains in conducting customer due diligence measures and ongoing monitoring for a customer.
- (2) Without limiting subrule (1), a licensed party must make and keep a record of how and when each of the steps of the customer due diligence measures for a customer were satisfactorily completed by the party.
- (3) This rule applies in relation to a customer irrespective of the nature and risk profile of the customer.

### **Division 4.4 B Customer identification documentation—the economic activity**

#### **4.4.3 Risks associated with the economic activity**

- (1) A licensed party must take into account that the risks associated with money laundering and the financing of terrorism arise from the fact that either—
  - (a) the funds that are going to be put through a business relationship derive from criminal activity or the business relationship will be used to channel these funds; or
  - (b) proceeds of criminal activity will be mixed with legitimate economic activity to disguise their origin.
- (2) A licensed party must properly address these risks using the following approach:
  - (a) identify the sources of the customer’s wealth and funds;  
*Note* By establishing that the sources are not from criminal activity, the licensed party substantially mitigates the customer risk.
  - (b) identify the purpose and intended nature of the business relationship.

*Note* By establishing this, the licensed party can adequately monitor transactions conducted under the business relationship and assess how these correspond to transactions intended to be conducted under the relationship. In the assessment of where these differ, the licensed party can better work out whether money laundering or terrorist financing is taking place.

#### **4.4.4 Risks associated with the economic activity—source of wealth and funds**

- (1) In conducting customer due diligence measures for an applicant for business, a licensed party must obtain, and document, information on the source of the applicant's wealth and funds.

*Note* Information obtained can assist the licensed party in establishing the money laundering and terrorist financing risks posed by both the customer risk as well as the jurisdiction risk. In certain cases the product risk will also be affected by establishing the source of the wealth and funds.

- (2) The licensed party must obtain, and document, the information to an appropriate level having regard to the applicant's risk profile
- (3) If the applicant's risk profile is not low risk, the licensed party must verify the source of the applicant's wealth and funds using reliable, independent source documents, data or information, and document this verification.
- (4) Information documented under this rule forms part of the licensed party's customer identification documentation.

#### **4.4.5 Risks associated with the economic activity—purpose and intended nature of business relationship**

- (1) In conducting customer due diligence measures for an applicant for business a licensed party must obtain, and document, information about the purpose and intended nature of the business relationship.
- (2) The extent and detail of this information must be sufficient to allow the licensed party—

- (a) to readily identify variances between the actual transactions conducted under the relationship and the stated purpose and intended nature of the relationship and
- (b) to increase information requirements to satisfy itself that money laundering or financing of terrorism has not taken place; and
- (c) if it is not satisfied about the information received—to consider making a suspicious transaction report to the FIU.

- (3) Information documented under this rule forms part of the licensed party's customer identification documentation.

## **Division 4.4 C Customer identification documentation—particular applicants for business**

### **4.4.6 Customer identification documentation—individuals**

- (1) This rule applies if an applicant for business is an individual.
- (2) If the individual's risk profile is low risk, the licensed party may satisfy the customer identification documentation requirements by confirming the individual's name and likeness by sighting—
  - (a) an official government issued document that has the individual's name and a photograph of the individual; or

#### **Examples**

- 1 a valid Qatari ID card
- 2 a valid passport
- (b) a document from a reliable, independent source that bears the individual's name and a photograph of the individual; or
- (c) other documents from reliable, independent data sources.

### **4.4.7 Customer identification documentation—multiple individual applicants**

- (1) This rule applies if 2 or more individuals are joint applicants for business for a licensed party.
- (2) The identities of all of them must be verified in accordance with these rules.

### **4.4.8 Customer identification documentation—corporations**

- (1) This rule applies if an applicant for business is a corporation.
- (2) If the corporation's risk profile is low risk, the licensed party may, subject to subrule (3), satisfy the customer documentation identification requirements by—
  - (a) either—
    - (i) obtaining a copy of the certificate of incorporation or trade (or any equivalent document), which includes—
      - (A) the corporation's full name; and
      - (B) the corporation's registered number; or
    - (ii) performing a search in the jurisdiction of incorporation and confirming all the matters that would be confirmed by a certificate (or equivalent document) mentioned in subparagraph (i); and
  - (b) confirming the corporation's registered office business address; and

- (c) obtaining a copy of the corporation's latest financial report;  
and
  - (d) obtaining a copy of the board resolution authorising—
    - (i) the establishing of the relationship with the licensed party;  
and
    - (ii) persons to act on behalf of the corporation in relation to the relationship, including by operating any accounts.
  - (3) If the corporation has a multi-layered ownership or control structure, the licensed party must—
    - (a) obtain an understanding of the corporation's ownership and control at each level of the structure using reliable, independent source documents, data or information; and
    - (b) document its understanding of the corporation's ownership and control at each level of the structure.
  - (4) Without limiting subrule (3), if the corporation has a multi-layered ownership or control structure, the customer identification requirements for each intermediate legal person must include reliable, independent source documents, data or information verifying—
    - (a) the legal person's existence; and
    - (b) its registered shareholdings and management.
- Example**
- If corporation applicant for business (*A*) is a subsidiary of another corporation (*B*) that is in turn a subsidiary of a third corporation (*C*), the licensed party must comply with subrule (3) and (4) in relation to B as well as C.
- (5) The licensed party must conduct additional customer due diligence if the corporation—
    - (a) is incorporated in a foreign jurisdiction; or
    - (b) has no direct business links to Qatar.

#### 4.4.9 Customer identification documentation—unincorporated partnerships and associations

- (1) This rule applies if an applicant for business for a licensed party is an unincorporated partnership, or an association that conducts business, (the *applicant*).
- (2) If applicant's partners or directors are not known to the company, the identity of all of the partners or directors must be verified using reliable, independent source documents, data or information.
- (3) If the applicant is a partnership with a formal partnership agreement, the licensed party must obtain a mandate from the partnership authorising—

- (a) the establishing of the relationship with the licensed party;  
and
- (b) persons to act on behalf of the partnership in relation to the relationship, including by operating any accounts.

#### **4.4.10 Customer identification documentation—charities**

- (1) This rule applies if an applicant for business for a licensed party is a charity.
- (2) The licensed party must conduct customer due diligence measures for the charity according to its legal form.

#### **4.4.11 Customer identification documentation—trusts**

- (1) This rule applies if an applicant for business is a trust.
- (2) In conducting a risk assessment for the trust, the licensed party must take into account the different money laundering and terrorist financing risks that are posed by trusts of different sizes and areas of activity.
- (3) Subrule (2) does not limit the matters the licensed party may take into account.
- (4) If the trust's risk profile is low risk, the licensed party must, as a minimum, obtain the following information about the trust:
  - (a) the trust's full name;
  - (b) the nature and purpose of the trust;
  - (c) the jurisdiction where the trust was established;
  - (d) the identity of the settlor;
  - (e) the identity of the trustee;
  - (f) the identity of the protector;
  - (g) if the beneficiaries and their distributions have already been decided—the identity of each beneficiary who is to receive at least 25% of the funds of the trust (by value);
  - (h) if the beneficiaries or their distributions have not already been decided—the class of persons in whose main interest the trust is established or operated as beneficial owner.
- (5) If the trust's risk profile is higher risk, the licensed party must conduct enhanced customer due diligence measures for the trust.

#### **4.4.12 Customer identification documentation—clubs and societies**

- (1) This rule applies if an applicant for business for a licensed party is a club or society (the *applicant*).
- (2) In conducting a risk assessment for the applicant, the licensed party must take into account the different money laundering and terrorist

financing risks that are posed by clubs and societies of different types and areas of activity.

- (3) Subrule (2) does not limit the matters the licensed party may take into account.
- (4) If the applicant's risk profile is low risk, the licensed party must, as a minimum, obtain the following information about the applicant:
  - (a) the applicant's full name;
  - (b) the applicant's legal status;
  - (c) the applicant's purpose, including any constitution;
  - (d) the names of all of the applicant's officers.
- (5) The licensed party must also verify the identities of the applicant's officers who have authority—
  - (a) to establish a relationship with the licensed party on the applicant's behalf; or
  - (b) to act on behalf of the applicant for the relationship, including by operating any account or by giving instructions about the use, transfer or disposal of any of the applicant's assets.

#### **4.4.13 Customer identification documentation—governmental bodies**

- (1) This rule applies if an applicant for business for a licensed party is a multi-jurisdictional entity, a government department or local authority (the *applicant*).
- (2) The licensed party must, as a minimum, obtain the following information about the applicant:
  - (a) the applicant's legal status;
  - (b) the applicant's ownership and control;
  - (c) the applicant's main address.
- (3) The licensed party must also verify the identities of the persons who have authority—
  - (a) to establish a relationship with the licensed party on the applicant's behalf; or
  - (b) to act on behalf of the applicant for the relationship, including by operating any account or by giving instructions about the use, transfer or disposal of any of the applicant's assets.

## Part 4.5 Enhanced CDD and ongoing monitoring

### 4.5.1 Enhanced CDD and ongoing monitoring

A licensed party must, on a risk-sensitive basis, conduct enhanced customer due diligence measures and enhanced ongoing monitoring—

- (a) in cases where it is required to do so under the AML/CFT Law or other provisions of these rules; or
- (b) in any other situation that by its nature can present a higher risk of money laundering or terrorist financing.

## Part 4.6 Reduced or simplified CDD

### 4.6.1 Reduced or simplified CDD—general

- (1) A licensed party may conduct reduced or simplified customer due diligence measures for a customer in cases where it is permitted to do so under a provision of this part when it establishes a business relationship with the customer; or

*Note* Reduced or simplified customer due diligence measures are permitted only under the following provisions of this part.

- (2) However, reduced or simplified customer due diligence measures must not be conducted under this part if there is a suspicion of money laundering or terrorist financing.

Source: FAFT R5. FATF methodologies 5.9 and 5.11

### 4.6.2 Reduced or simplified CDD—financial institution customer

A licensed party may conduct reduced or simplified customer due diligence measures for a customer if the customer is—

- (i) a financial institution that is based, or incorporated or otherwise established, in Qatar; or
- (ii) a financial institution that
  - (a) is based, or incorporated or otherwise established, in a foreign jurisdiction that imposes requirements similar to those of the AML/CFT Law and these rules; and
  - (b) is supervised for compliance with those requirements.

Source: FATF R5. FATF Meth. 5.9 Example (A)

### 4.6.3 Reduced or simplified CDD—listed, regulated public companies

A licensed party may conduct reduced or simplified customer due diligence measures for a customer if the customer is a public company

whose securities are listed on a regulated financial market that subjects public companies to disclosure obligations consistent with international standards of disclosure.

## Chapter 5 Reporting and tipping off

### Part 5.1 Reporting requirements

*Note for pt 5.1*

Principle 4 requires a licensed party to have effective measures in place to ensure there is internal and external reporting whenever money laundering or terrorist financing is known or suspected.

#### Division 5.1.A Reporting requirements

##### 5.1.1 Unusual and inconsistent transactions

- (1) A transaction that is unusual or inconsistent with a customer's known legitimate business and risk profile does not of itself make it suspicious.

*Note 1* The key to recognising unusual or inconsistent transactions is for a licensed party to know its customers well enough under ch 4 (Know your customer).

*Note 2* A licensed party's AML/CFT policies, procedures, systems and controls must provide for the identification and scrutiny of certain transactions;

- (2) A licensed party must consider the following matters in deciding whether an unusual or inconsistent transaction is a suspicious transaction:
- (a) whether the transaction has no apparent or visible economic or lawful purpose;
  - (b) whether the transaction has no reasonable explanation;
  - (c) whether the size or pattern of the transaction is out of line with any earlier pattern or the size or pattern of transactions of similar customers;
  - (d) whether the customer has failed to give an adequate explanation for the transaction or to fully provide information about it;
  - (e) whether the transaction involves the use of a newly established business relationship
  - (f) whether the transaction involves the use of offshore accounts, companies or structures that are not supported by the customer's economic needs;
  - (g) whether the transaction involves the unnecessary routing of funds through third parties.

- (3) Subrule (2) does not limit the matters that the licensed party may consider.

**Source:** FATF R 11. FATF Meth 11

## Division 5.1.B Internal reporting

### 5.1.2 Internal reporting policies

- (1) A licensed party must have clear and effective policies, procedures, systems and controls for the internal reporting of all known or suspected instances of money laundering or terrorist financing.
- (2) The policies, procedures, systems and controls must enable the licensed party to comply with the AML/CFT Law and these rules in relation to the prompt making of internal suspicious transaction reports to the party's MLRO.

### 5.1.3 Access to MLRO

A licensed party must ensure that all its officers and employees have direct access to the party's MLRO and that the reporting lines between them and the MLRO are as short as possible.

*Note* The MLRO is responsible for receiving, investigating and assessing internal suspicious transaction reports for the licensed party

### 5.1.4 Obligation of officer or employee to report to MLRO

- (1) This rule applies to an officer or employee of a licensed party if, in the course of his or her office or employment, the officer or employee knows, suspects, or has reasonable grounds to know or suspect, that funds are—
  - (a) the proceeds of criminal conduct; or
  - (b) related to terrorist financing; or
  - (c) linked or related to, or are to be used for, terrorism, terrorist acts or by terrorist organisations.
- (2) The officer or employee must promptly make a suspicious transaction report to the licensed party's MLRO.

*Note* See r 5.1.2 (2) for relevant matters to be included in the licensed party's AML/CFT policies, procedures, systems and controls.

- (3) The officer or employee must make the report—
  - (a) irrespective of the amount of any transaction relating to the funds; and
  - (b) whether or not any transaction relating to the funds involves tax matters; and
  - (c) even though—
    - (i) no transaction has been, or will be, conducted by the licensed party in relation to the funds; and
    - (ii) for an applicant for business—no business relationship has been, or will be, entered into by the licensed party with the applicant; and

- (iii) for a customer—the licensed party has terminated any relationship with the customer; and
  - (iv) any attempted money laundering or terrorist financing activity in relation to the funds has failed for any other reason.
- (4) If the officer or employee makes a suspicious transaction report to the MLRO (the *internal report*) in relation to the applicant for business or customer, the officer or employee must promptly give the MLRO details of every subsequent transaction of the applicant or customer (whether or not of the same nature as the transaction that gave rise to the internal report) until the MLRO tells the officer or employee not to do so.

*Note* An officer or employee who fails to make a report under this rule may commit an offence against the AML/CFT Law.

#### 5.1.5 Obligations of MLRO on receipt of internal report

- (1) If the MLRO of a licensed party receives a suspicious transaction report the MLRO must promptly—
- (a) if the licensed party’s policies, procedures, systems and controls allow an initial report to be made orally and the initial report is made orally—properly document the report; and
  - (b) give the individual making the report a written acknowledgment for the report, together with a reminder about the provisions of part 5.2 (Tipping off); and
  - (c) consider the report in light of all other relevant information held by the licensed party about the applicant for business, customer or transaction to which the report relates; and
  - (d) decide whether the transaction is suspicious; and
- Note* See r 5.1.7 (Obligation of licensed party to report to FIU etc).
- (e) give written notice of the decision to the individual who made the report.
- (2) A reference in this rule to the *MLRO* includes a reference to a person acting under rule 5.1.7 (3) (b) (Obligation of licensed party to report to FIU etc) in relation to the making of a report on the party’s behalf.

*Note* Under r 2.3.5 the deputy MLRO acts as the MLRO during absences of the MLRO and whenever there is a vacancy in the MLRO’s position.

Source: FATF R13, and SR IV, FATF Meth. 13 and IV.

## Division 5.1.C External reporting

### 5.1.6 External reporting policies

- (1) A licensed party must have clear and effective policies, procedures, systems and controls for reporting to the FIU all known or suspected instances of money laundering or terrorist financing.
- (2) The policies, procedures, systems and controls must enable the licensed party—
  - (a) to comply with the AML/CFT Law and these rules in relation to the prompt making of suspicious transaction reports to the FIU; and
  - (b) to cooperate effectively with the FIU and law enforcement agencies in relation to suspicious transaction reports made to the FIU.

**Source:** FATF R13 and SR IV. FATF Meth 13 and IV.

### 5.1.7 Obligation of licensed party to report to FIU

- (1) This rule applies to a licensed party if the licensed party knows, suspects, or has reasonable grounds to know or suspect, that funds are—
  - (a) the proceeds of criminal conduct; or
  - (b) related to terrorist financing; or
  - (c) linked or related to, or are to be used for, terrorism, terrorist acts or by terrorist organisations.
- (2) The licensed party must promptly make a suspicious transaction report to the FIU and ensure that any proposed transaction relating to the report does not proceed without consulting with the FIU.

*Note* See r 5.1.6 (2) for relevant matters to be included in the licensed party's AML/CFT policies, procedures, systems and controls.

- (3) The report must be made on the licensed party's behalf by—
  - (a) the MLRO; or
  - (b) if the report cannot be made by the MLRO (or deputy MLRO) for any reason—by a person who is employed (as described in rule 2.3.2 (a)) at the management level by the licensed party, or by a person in the same group, and who has sufficient seniority, experience and authority to investigate and assess internal suspicious transaction reports.

*Note* Under r 2.3.5 the deputy MLRO acts as the MLRO during absences of the MLRO and whenever there is a vacancy in the MLRO's position.

- (4) The licensed party must make the report—

- (a) whether or not an internal suspicious transaction report has been made under division 5.1B (Internal reporting) in relation to the funds; and
  - (b) irrespective of the amount of any transaction; and
  - (c) even though—
    - (i) no transaction has been, or will be, conducted by the licensed party in relation to the funds; and
    - (ii) for an applicant for business—no business relationship has been, or will be, entered into by the licensed party with the applicant; and
    - (iii) for a customer—the licensed party has terminated any relationship with the customer; and
    - (iv) any attempted money laundering or terrorist financing activity in relation to the funds has failed for any other reason.
- (5) The report must include a statement about—
- (a) the facts or circumstances on which the licensed party's knowledge or suspicion is based or the grounds for the licensed party's knowledge or suspicion; and
  - (b) if the licensed party knows or suspects that the funds belong to a third person—the facts or circumstances on which that knowledge or suspicion is based or the grounds for the licensed party's knowledge or suspicion.
- Note* An officer or employee who fails to make a report under this rule may commit an offence against the AML/CFT Law.
- Source: FATF R 13 and SR IV, FATF Methodology 13 and IV
- (6) If a licensed party makes a report to the FIU under this rule about a proposed transaction, it must immediately communicate the same to the Regulator in writing.

### **5.1.8 Obligation not to destroy records relating to customer under investigation**

- (1) This rule applies if—
- (a) a licensed party makes a suspicious transaction report to the FIU in relation to an applicant for business or a customer; or
  - (b) the licensed party knows that an applicant for business or customer is under investigation by a law enforcement

agency in relation to money laundering or terrorist financing.

- (2) The licensed party must not destroy any records relating to the applicant for business or customer without consulting with the FIU.

Source: FATF R 10

### 5.1.9 Licensed party may restrict or terminate business relationship

- (1) This division does not prevent a licensed party from restricting or terminating, for normal commercial reasons, its business relationship with a customer after the party makes a suspicious transaction report about the customer to the FIU.
- (2) However—
  - (a) before restricting or terminating the business relationship, the licensed party must consult with the FIU; and
  - (b) the licensed party must ensure that restricting or terminating the business relationship does not inadvertently result in tipping off the customer.

*Note* **Tipping off** is defined in r 5.2.1.

Source: FATF R 14. FATF Methodology 14.2

## Division 5.1.D Reporting records

### 5.1.10 Reporting records to be made by MLRO

The MLRO of a licensed party must make and keep records—

- (1) showing the details of each internal suspicious transaction report the MLRO receives; and
- (2) necessary to demonstrate how rule 5.1.5 (Obligations of MLRO on receipt of internal report) was complied with in relation to each internal suspicious transaction report; and
- (3) showing the details of each suspicious transaction report made to the FIU by the licensed party.

Source: FATF R 10 and 28

## Part 5.2 Tipping off

### 5.2.1 What is tipping off?

**Tipping off**, in relation to an applicant for business or a customer of a licensed party, is the unauthorised act of disclosing information that—

- (1) may result in the applicant or customer, or a third party (other than the FIU or the Regulator), knowing or suspecting that the applicant or customer is or may be the subject of—
  - (a) a suspicious transaction report; or

- (b) an investigation relating to money laundering or terrorist financing; and
- (2) may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorist financing.

### **5.2.2 Licensed party must ensure no tipping off occurs**

- (1) A licensed party must ensure that—
  - (a) its officers and employees are aware of, and sensitive to—
    - (i) the issues surrounding tipping off; and
    - (ii) the consequences of tipping off; and
  - (b) it has policies, procedures, systems and controls to prevent tipping off.
- (2) If a licensed party believes, on reasonable grounds, that an applicant for business or a customer may be tipped off by conducting customer due diligence measures or ongoing monitoring, the party may make a suspicious transaction report to the FIU instead of conducting the measures or monitoring.
- (3) If the licensed party acts under subrule (2), the MLRO must make and keep records to demonstrate the grounds for the belief that conducting customer due diligence measures or ongoing monitoring would have tipped off an applicant for business or a customer.

Source: FATF R 14b, FATF Methodology 14.2.

### **5.2.3 Information relating to suspicious transaction reports to be safeguarded**

- (1) A licensed party must take all reasonable measures to ensure that information relating to suspicious transaction reports is safeguarded and, in particular, that information relating to a suspicious transaction report is not disclosed to any person (other than a member of the party's senior management) without the consent of the party's MLRO.
- (2) The MLRO must not consent to information relating to a suspicious transaction report being disclosed to a person unless the MLRO is satisfied that disclosing the information to the person would not constitute tipping off.
- (3) If the MLRO gives consent, the MLRO must make and keep records to demonstrate how the MLRO was satisfied that disclosing the information to the person would not constitute tipping off.

Source: Recommendation 14b , Methodology 14.2

## Chapter 6 Screening and training requirements

### Part 6.1 Screening procedures

Principle 5 requires a licensed party to have adequate screening procedures to ensure high standards when appointing or employing officers and employees.

#### 6.1.1 Screening procedures—particular requirements

A licensed party's screening procedures for the appointment or employment of officers and employees must ensure that an individual is not appointed or employed unless—

- (1) The individual has the appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently;
- (2) The procedures must, as a minimum, provide that, before appointing or employing an individual, the licensed party must—
  - (a) obtain references about the individual; and
  - (b) obtain information about the individual's employment history and qualifications; and
  - (c) obtain details of any criminal convictions of the individual; and
  - (d) for licensed individuals, obtain details of any regulatory action taken in relation to the individual.

Source: FATF R15, FATF Meth 15.4

### Part 6.2 AML/CFT training programme

*Note for pt 6.2*

Principle 5 also requires a licensed party to have an appropriate ongoing AML/CFT training programme for its officers and employees.

#### 6.2.1 Appropriate AML/CFT training programme to be delivered

- (1) A licensed party must identify, design, deliver and maintain an appropriate ongoing AML/CFT training programme for its officers and employees.
- (2) The programme must ensure that the licensed party's officers and employees are aware, and have an appropriate understanding, of the following:
  - (a) their legal and regulatory responsibilities and obligations, particularly those under the AML/CFT Law and these rules;

- (b) their role in preventing money laundering and terrorist financing, and the liability that they, and the licensed party, may incur for—
    - (i) involvement in money laundering or terrorist financing; and
    - (ii) failure to comply with the AML/CFT Law and these rules;
  - (c) how the licensed party is managing money laundering and terrorist financing risks, how risk management techniques are being applied by the party, the roles of the MLRO and deputy MLRO, and the importance of customer due diligence measures and ongoing monitoring;
  - (d) money laundering and terrorist financing threats, techniques, methods and trends, the vulnerabilities of the products offered by the licensed party, and how to recognise suspicious transactions;
  - (e) the licensed party's processes for making internal suspicious transaction reports, including how to make effective and efficient reports to the MLRO whenever money laundering or terrorist financing is known or suspected.
- (3) The training must enable the licensed party's officers and employees to seek and assess the information that is necessary for them to decide whether a transaction is suspicious.
- (4) In making a decision about what is appropriate training for its officers and employees, the licensed party must consider the following:
- (a) their differing needs, experience, skills and abilities;
  - (b) their differing functions, roles and levels in the licensed party;
  - (c) the degree of supervision over, or independence exercised by, them;
  - (d) the availability of information that is needed for them to decide whether a transaction is suspicious;
  - (e) the size of the licensed party's business and the risk of money laundering and terrorist financing;
  - (f) the outcome of reviews of their training needs;
  - (g) any analysis of suspicious transaction reports showing areas where training needs to be enhanced.

**Examples**

- 1 training for new employees needs to be different to the training for employees who have been with the licensed party for some time and are already aware of the party's policies, processes, systems and controls

- 2 the training for employees who deal with customers face to face needs to be different to the training for employees who deal with customers non-face to face
- (5) Subrule (4) does not limit the matters that the licensed party may consider.

Source: FATF R15 b, FATF Meth 15.3

### 6.2.2 Training must be maintained and reviewed

- (1) A licensed party's AML/CFT training must include ongoing training to ensure that its officers and employees—
- (a) maintain their AML/CFT knowledge, skills and abilities; and
  - (b) are kept up to date with new AML/CFT developments, including the latest money laundering and terrorist financing techniques, methods and trends; and
  - (c) are trained on changes to the licensed party's AML/CFT policies, procedures, systems and controls.
- (2) A licensed party must, at regular and appropriate intervals, carry out reviews of the AML/CFT training needs of its officers and employees and ensure that the needs are met.
- (3) The licensed party's senior management must in a timely way—
- (a) consider the outcomes of each review; and
  - (b) if a review identifies deficiencies in the licensed party's AML/CFT training—prepare or approve and document an action plan to remedy the deficiencies.

*Note* It is the MLRO's responsibility to monitor the licensed party's AML/CFT training programme

Source: FATF R 15b, FATF Meth 15.3

## Chapter 7 Providing documentary evidence of compliance

*Note for ch 7*

Principle 6 requires a licensed party to be able to provide documentary evidence of its compliance with the requirements of the AML/CFT Law and these rules.

### Part 7.1 General record-keeping obligations

#### 7.1.1 Records about compliance

- (1) A licensed party must make the records necessary—
  - (a) to enable it to comply with the AML/CFT Law and these rules; and
  - (b) to demonstrate at any time whether compliance with the AML/CFT Law and these rules has been achieved.
- (2) Without limiting rule (1) (b), the licensed party must make the records necessary to demonstrate how—
  - (a) the key AML/CFT principles in part 1.2 have been complied with; and
  - (b) the licensed party's senior management has complied with responsibilities under the AML/CFT Law and these rules; and
  - (c) the licensed party's risk-based approach has been designed and implemented; and
  - (d) each of the licensed party's risks have been mitigated; and
  - (e) customer due diligence measures and ongoing reviews were conducted for each customer; and
  - (f) customer due diligence measures and ongoing monitoring were enhanced where required by the AML/CFT Law or these rules.

*Note* See also r 5.1.10 (Reporting records to be made by MLRO etc).

Source: FATF R10

#### 7.1.2 How long records must be kept

- (1) All records made by a licensed party for the AML/CFT Law or these rules must be kept for at least 6 years after the day they are made.
- (2) All records made by a licensed party in relation to a customer for the purposes of AML/CFT Law or these rules must be kept for at least the longer of the following:

- (a) if the licensed party has (or has had) a business relationship with the customer—6 years after the day the business relationship with the customer ends;
  - (b) if the licensed party has not had a business relationship with the customer—6 years after the day the licensed party last completed a transaction with or for the customer.
- (3) If the day the business relationship with the customer ended is unclear, it is taken to have ended on the day the licensed party last completed a transaction for or with the customer.
- (4) This rule is subject to rule 5.1.8 (Obligation not to destroy records relating to customer under investigation etc).

Source: FATF R10

### 7.1.3 Retrieval of records

- (1) A licensed party must ensure that all types of records kept for the AML/CFT Law and these rules can be retrieved without undue delay.
- (2) Without limiting subrule (1), a licensed party must establish and maintain systems that enable it to respond fully and quickly to inquiries from the FIU and law enforcement authorities about—
- (a) whether it maintains, or has maintained during the previous 6 years, a business relationship with any person; and
  - (b) the nature of the relationship.

Source: FATF R10 and R28, FATF Meth 10.

## Part 7.2 Particular record-keeping obligations

### 7.2.1 Records for customers and transactions

- (1) A licensed party must make and keep records in relation to—
- (a) its business relationship with each customer; and
  - (b) each transaction that it conducts with or for a customer.
- (2) The records must—
- (a) comply with the requirements of the AML/CFT Law and these rules; and
  - (b) enable an assessment to be made of the licensed party's compliance with—

- (i) the AML/CFT Law and these rules; and
  - (ii) its AML/CFT policies, procedures, systems and controls; and
  - (c) enable any transaction effected by or through the licensed party to be reconstructed; and
  - (d) enable the licensed party to comply with any request, direction or order by a competent authority, judicial officer or court for the production of documents, or the provision of information, within a reasonable time; and
  - (e) indicate the nature of any evidence that it obtained in relation to an applicant for business, customer or transaction; and
  - (f) for any such evidence—include a copy of the evidence itself or, if this is not practicable, information that would enable a copy of the evidence to be obtained.
- (3) This rule is additional to any provision of the AML/CFT Law or any other provision of these rules.

**Source: FATF R10, FATF Meth 10**

### **7.2.2 Training records**

A licensed party must make and keep records of the AML/CFT training provided for the party's officers and employees, including, as a minimum—

- (1) the dates the training was provided; and
- (2) the nature of the training; and
- (3) the names of the individuals to whom the training was provided.

## Chapter 8 Miscellaneous

### 8.1.1 Approved forms to be used

- (1) The Regulator may, by written notice, approve forms for the purposes of the AML/CFT Law or these rules.
- (2) If a form is approved under subrule (1) for a particular purpose, the form must—
  - (a) be used for that purpose; and
  - (b) must be completed in accordance with rule 8.1.2.

### 8.1.2 Completion of forms

- (1) Substantial compliance with a form approved by the Regulator for the purposes of the AML/CFT Law or these rules is sufficient.
- (2) However, if a form requires—
  - (a) the form to be signed; or
  - (b) the form to be prepared in a particular way (for example, on paper of a particular size or quality or in a particular electronic form); or
  - (c) the form to be completed in a particular way; or
  - (d) particular information to be included in the form, or a particular document to be attached to or given to a person with the form; or
  - (e) the form, information in the form, or a document attached to or given with the form, to be verified in a particular way;the form is properly completed only if the requirement is complied with.

## Annex

(see r 1.1.4)

**account**, in relation to a financial institution, means an account of any kind with the financial institution, and includes anything else that involves a similar relationship between the financial institution and a customer.

*Source* Glossary of FATF Methodology

**activity** includes operation.

**AML/CFT Law** means Law No. (4) of 2010 on Anti-Money Laundering and Combating the Financing of Terrorism.

**another jurisdiction** means a jurisdiction other than Qatar Financial Markets Authority's jurisdiction

*Note* **Jurisdiction** defined in this glossary.

**applicant for business** has the meaning given by rule 4.2.3.

**asset** means any kind of asset, and includes, for example, property of any kind.

*Note* **Property** is defined in this glossary.

**associate**, in relation to a legal person (A), means any of the following:

- (a) a legal person in the same group as A;
- (b) a subsidiary of A.

*Note* **Legal person** and **group** are defined in this glossary.

**beneficial owner** has the meaning given by rule 1.3.5.

**beneficiary**, of a trust, means a person, or a person included in a class of persons, for whose benefit the trust property is held by the trustee.

*Source* FATF methodology glossary

**business day** means any day that is not a Friday, Saturday or a public holiday in Qatar.

**business relationship** has the meaning given by rule 4.2.4.

**correspondent Securities relationship** has the meaning given by rule 1.3. 7.

**customer** has the meaning given by rule 1.3.4.

**customer due diligence measures** (or **CDD**) has the meaning given by rule 4.2.1.

**director**, of a company, means a person appointed to direct the party's affairs, and includes—

- (a) a person named as director; and
- (b) any other person in accordance with whose instructions the licensed party is accustomed to act.

**Entity** means any entity, and includes for example any person.

**FATF** means the Financial Action Task Force, the inter-governmental body that sets standards, and develops and promotes policies, to combat money laundering and terrorist financing, and includes any successor entity.

**licensed party** has the meaning given by rule 1.3.1.

**financial institution** has the meaning given by rule 1.3.2.

**FIU** means the Financial Information Unit defined by Law No (4) of 2010.

**funds** includes assets of any kind.

**group**, in relation to a legal person (A), means the following:

- (a) A;
- (b) any parent entity of A;
- (c) any subsidiary (direct or indirect) of any parent entity.

**jurisdiction** means any kind of legal jurisdiction, and includes, for example—

- (a) the State; and
- (b) a foreign country (whether or not an independent sovereign jurisdiction), or a state, province or other territory of such a foreign country; and
- (c) the Qatar Financial Markets Authority or a similar jurisdiction.

**legal arrangement** means an express trust or similar legal arrangement.

**legal person** means an entity (other than an individual) on which the legal system of a jurisdiction confers rights and imposes duties, and includes, for example—

- (a) any entity that can establish a permanent customer relationship with a financial institution; and
- (b) any entity that can own, deal with, or dispose of, property.

Source FATF methodology glossary

**money laundering** means committing an act that is considered as a crime against the AML/CFT Law.

**outsourcing**, in relation to a licensed party, is any form of arrangement that involves the party relying on a third-party service provider (including a member of its group) for the exercise of a function, or the conduct of an activity, that would otherwise be exercised or conducted by the party, but does not include—

- (a) discrete advisory services, including, for example, the provision of legal advice, procurement of specialised training, billing, and physical security; or

- (b) supply arrangements and functions, including, for example, the supply of electricity or water and the provision of catering and cleaning services; or
- (c) the purchase of standardised services, including, for example, market information services and the provision of prices.

**parent entity**, in relation to a legal person (A), means any of the following:

- (a) a legal person that holds a majority of the voting power in A;
- (b) a legal person that is a member of A (whether direct or indirect, or through legal or beneficial entitlement) and alone, or together with 1 or more associates, holds a majority of the voting power in A;
- (c) a parent entity of any legal person that is a parent entity of A.

**person** means—

- (a) an individual (including an individual occupying an office from time to time); or
- (b) a legal person.

**politically exposed person** has the meaning given by rule 1.3. 6.

**property** means any estate or interest (whether present or future, vested or contingent, or tangible or intangible) in land or property of any other kind, and includes, for example—

- (a) money of any jurisdiction; and
- (b) bonds, commercial notes, drafts, letters of credit, money orders, securities, shares, travellers' cheques, and other negotiable or non-negotiable instruments of any kind; and
- (c) bank credits; and
- (d) any right to interest, dividends or other income on or accruing from or generated by property of any kind; and
- (e) any other things in action; and
- (f) any other charge, claim, demand, easement, encumbrance, lien, power, privilege, right, or title, recognised or protected by the law of any jurisdiction over, or in relation to, land or property of any other kind;
- (g) any other documents evidencing title to, or to any interest in, land or property of any kind.

**proceeds of criminal conduct**, in relation to any person who has benefited from criminal conduct, includes that benefit.

**product** includes the provision of a service.

**senior management**, of a licensed party, means the party's senior managers, jointly and separately.

**shell bank** has the meaning given by rule 1.3.8.

**suspicious transaction report**, in relation to a licensed party, means a suspicious transaction report to the party's MLRO or by the party to the FIU.

**terrorist means an individual who—**

- (a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and wilfully; or
- (b) participates as an accomplice in a terrorist act; or
- (c) organises or directs others to commit a terrorist act; or
- (d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose if the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

**terrorist act** includes—

- (a) an act that constitutes an offence within the scope of, and as defined in, any of the following treaties:
  - (i) the Convention for the Suppression of Unlawful Seizure of Aircraft (1970);
  - (ii) the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971);
  - (iii) the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973);
  - (iv) the International Convention against the Taking of Hostages (1979);
  - (v) the Convention on the Physical Protection of Nuclear Material (1980);
  - (vi) the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988);
  - (vii) the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988);

- (viii) the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988);
- (ix) the International Convention for the Suppression of Terrorist Bombings (1997); and
- (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of the act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.

***terrorist financing means the act of willingly, directly or indirectly, providing or collecting (or attempting to provide or collect) funds in order to use them to commit a terrorist act, or knowing that the funds will be used in whole or part—***

- (a) for the execution of a terrorist act; or
- (b) by a terrorist or terrorist organisation.

***terrorist organisation*** means any group of terrorists that—

- (a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and wilfully; or
- (b) participates as an accomplice in a terrorist act; or
- (c) organises or directs others to commit a terrorist act; or
- (d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose if the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

***the Regulator*** means the Qatar Financial Markets Authority.

***the State*** means the State of Qatar.

***tipping off*** has the meaning given by rule 5.2.1.

***transaction*** means a transaction or attempted transaction of any kind, and includes, for example—

- (a) the giving of advice; and
- (b) the provision of any service; and
- (c) the conducting of any other business or activity.