هيئة تنظيم مركز قطر للمال

QATAR FINANCIAL CENTRE
REGULATORY AUTHORITY

Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 (AML/CFTR)

Version No. 1

Effective: 1 February 2020

هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE REGULATORY AUTHORITY

Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019

QFCRA Rules 2019-8

made under

Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing

Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing

Financial Services Regulations

Contents

Page

Chapter 1 General provisions 1

Part 1.1 Introductory 1

1.1.1 Name of rules 1
1.1.2 Commencement 1
1.1.3 Repeal of 2010 AML/CFTR 1
1.1.4 Application of these rules 1
1.1.5 Effect of definitions, notes and examples 2
1.1.6 References to particular currencies 2

page

Part 1.2 Key AML/CFT principles 3
1.2.1 Principle 1—responsibilities 3
1.2.2 Principle 2—risk-based approach 3
1.2.3 Principle 3—know your customer 3
1.2.4 Principle 4—effective reporting 3
1.2.5 Principle 5—high standard screening and appropriate training 3
1.2.6 Principle 6—evidence of compliance 4

Part 1.3 Key terms 4
1.3.1 What is a *firm*? 4
1.3.2 What is a *financial institution*? 4
1.3.3 What is a *DNFBP*? 5
1.3.4 Who is a *customer*? 7
1.3.5 Who is the *beneficial owner*? 8
1.3.6 Politically exposed persons, their family members and associates 9
1.3.7 What is *correspondent banking*? 10
1.3.8 What is a *shell bank*? 10
1.3.9 What is a *correspondent securities relationship*? 11

Chapter 2 General AML and CFT responsibilities 12

Part 2.1 The firm 12
2.1.1 Firms to develop AML/CFT programme 12
2.1.2 Policies etc must be risk-sensitive, appropriate and adequate 13
2.1.3 Matters to be covered by policies etc 14
2.1.4 Assessment and review of policies etc 15
2.1.5 Compliance by officers, employees, agents etc 15
2.1.6 Application of AML/CFT Law requirements, policies etc to branches and associates 16
2.1.7 Application of AML/CFT Law requirements, policies etc to outsourced functions and activities 18

Part 2.2 Senior management 20
2.2.1 Overall senior management responsibility 20
2.2.2 Particular responsibilities of senior management 20

Part 2.3 MLRO and Deputy MLRO 23
Division 2.3.A Appointment of MLRO and Deputy MLRO 23
2.3.1 Appointment—MLRO and Deputy MLRO 23
2.3.2 Eligibility to be MLRO or Deputy MLRO 23

page

Division 2.3.B Roles of MLRO and Deputy MLRO 24
2.3.3 General responsibilities of MLRO 24
2.3.4 Particular responsibilities of MLRO 24
2.3.5 Role of Deputy MLRO 25
2.3.6 How MLRO must carry out role 26

Division 2.3.C Reporting by MLRO to senior management 26
2.3.7 MLRO reports 26
2.3.8 Minimum annual report by MLRO 27
2.3.9 Consideration of MLRO reports 28

Division 2.3.D Additional obligations etc of firm with non-resident MLRO 28
2.3.10 Annual reports 28
2.3.11 Visits by non-resident MLRO 28
2.3.12 Regulatory Authority may direct firm to appoint resident MLRO 29

Chapter 3 The risk-based approach 30

Part 3.1 The risk-based approach generally 30
3.1.1 Firms must conduct risk assessment and decide risk mitigation 30
3.1.2 Approach to risk mitigation must be based on suitable methodology 31
3.1.3 Risk profiling a business relationship 32

Part 3.2 Customer risk 34
3.2.1 Risk assessment for customer risk 34
3.2.2 Policies etc for customer risk 34
3.2.3 Scoring business relationships—types of customers 34
3.2.4 Persons associated with terrorist acts etc—enhanced CDD and ongoing monitoring 35
3.2.5 Measures for PEPs 35
3.2.6 Legal persons, legal arrangements and facilities—risk assessment process 36
3.2.7 Measures for persons in terrorist list 37

Part 3.3 Product risk 38
3.3.1 Risk assessment for product risk 38
3.3.2 Policies etc for product risk 38
3.3.3 Scoring business relationships—types of products 38
3.3.4 Products with fictitious or false names or no names 39
3.3.5 Correspondent banking relationships generally 39

page
3.3.6 Shell banks 41
3.3.7 Payable-through accounts 42
3.3.8 Powers of attorney 42
3.3.9 Bearer negotiable instruments 43
3.3.10 Wire transfers 44
3.3.11 Additional obligations of firms involved in wire transfers 47
3.3.12 Correspondent securities relationships generally 49

Part 3.4 Interface risk 51
Division 3.4.A Interface risks—general 51
3.4.1 Risk assessment for interface risk 51
3.4.2 Policies etc for interface risk 51
3.4.3 Scoring business relationships—interface risk 52
3.4.4 Electronic verification of identification documentation 52
3.4.5 Payment processing using on-line services 52
3.4.6 Concession for certain non-face-to-face transactions 53
Division 3.4.B Reliance on others generally 54
3.4.7 Activities to which Division 3.4.B does not apply 54
3.4.8 Reliance on certain third parties generally 54
3.4.9 Introducers 55
3.4.10 Group introductions 56
3.4.11 Intermediaries 57
Division 3.4.C Third party certification—identification documents 58
3.4.12 Third party certification of identification documents 58

Part 3.5 Jurisdiction risk 60
3.5.1 Risk assessment for jurisdiction risk 60
3.5.2 Policies etc for jurisdiction risk 60
3.5.3 Scoring business relationships—types of associated jurisdictions 61
3.5.4 Decisions about effectiveness of AML/CFT regimes in other jurisdictions 61
3.5.5 Jurisdictions with impaired international cooperation 61
3.5.6 Non-cooperative, high risk and sanctioned jurisdictions 61
3.5.7 Jurisdictions with high propensity for corruption 62

Chapter 4 Know your customer 63

Part 4.1 Know your customer—general 63
4.1.1 Know your customer principle—general 63

page
4.1.2 Overview of CDD requirements 63
4.1.3 Customer identification documents 64

Part 4.2 Know your customer—key terms 65
4.2.1 What is *customer due diligence*? 65
4.2.2 What is *ongoing monitoring*? 67
4.2.3 Who is an *applicant for business*? 67
4.2.4 What is a *business relationship*? 68
4.2.5 What is a *one-off transaction*? 68

Part 4.3 Customer due diligence and ongoing monitoring 69
4.3.1 Firm to assess applicants for business 69
4.3.2 When CDD required—basic requirement 69
4.3.3 Firm unable to complete CDD for customer 70
4.3.4 When CDD may not be required—acquired businesses 70
4.3.5 Timing of CDD—establishment of business relationship 71
4.3.6 Timing of CDD—one-off transactions 73
4.3.7 When CDD required—additional requirement for existing customers 73
4.3.8 Extent of CDD—general requirement 74
4.3.9 Extent of CDD—legal persons and arrangements 74
4.3.10 CDD for beneficiaries of life insurance policies—general 75
4.3.11 CDD for PEPs as beneficiaries of life insurance policies 76
4.3.12 CDD for purchaser and vendor of real estate 76
4.3.13 Ongoing monitoring required 76
4.3.14 Procedures for ongoing monitoring 77
4.3.15 Linked one-off transactions 78

Part 4.4 Enhanced CDD and ongoing monitoring 79
4.4.1 Enhanced CDD and ongoing monitoring—general 79
4.4.2 Measures required for enhanced CDD or ongoing monitoring 80
4.4.3 Measures in addition to enhanced CDD and ongoing monitoring 81

Part 4.5 Simplified CDD and ongoing monitoring 82
4.5.1 Simplified CDD—general 82
4.5.2 Customer with low level of risk 82
4.5.3 Listed, regulated public companies 82
4.5.4 Certain life insurance contracts 83
4.5.5 Simplified ongoing monitoring 83

page

Part 4.6 Customer identification documentation 84

Division 4.6.A Customer identification documentation—general 84

4.6.1 Elements of customer identification documentation 84

4.6.2 Records of customer identification documentation etc 84

Division 4.6.B Customer identification documentation—the economic activity 85

4.6.3 Risks associated with the economic activity—general 85

4.6.4 Risks associated with the economic activity—source of wealth and funds 85

4.6.5 Risks associated with the economic activity—purpose and intended nature of business relationship 86

Division 4.6.C Customer identification documentation—particular applicants for business 87

4.6.6 Customer identification documentation—individuals 87

4.6.7 Customer identification documentation—multiple individual applicants 87

4.6.8 Customer identification documentation—corporations 87

4.6.9 Customer identification documentation—unincorporated partnerships and associations 89

4.6.10 Customer identification documentation—charities 90

4.6.11 Customer identification documentation—legal arrangements 90

4.6.12 Customer identification documentation—clubs and societies 91

4.6.13 Customer identification documentation—governmental bodies 92

4.6.14 Other requirements for customer identification of legal persons 93

Chapter 5 Reporting and tipping-off 95

Part 5.1 Reporting requirements 95

Division 5.1.A Reporting requirements—general 95

5.1.1 Unusual and inconsistent transactions 95

Division 5.1.B Internal reporting 96

5.1.2 Internal reporting policies etc 96

5.1.3 Access to MLRO 96

5.1.4 Obligation of officer or employee to report to MLRO etc 96

5.1.5 Obligations of MLRO on receipt of internal report 98

Division 5.1.C External reporting 98

5.1.6 External reporting policies etc 98

5.1.7 Obligation of firm to report to FIU etc 99

5.1.8 Obligation not to destroy records relating to customer under investigation etc 101

page
5.1.9 Firm may restrict or terminate business relationship 101
Division 5.1.D Reporting records 101
5.1.10 Reporting records to be made by MLRO etc 101

Part 5.2 Tipping-off 102
5.2.1 What is *tipping-off*? 102
5.2.2 Firm must ensure no tipping-off occurs 102
5.2.3 Information relating to suspicious transaction reports to be safeguarded 103
5.2.4 When advice not considered to be tipping-off 103

Chapter 6 Screening and training requirements 104

Part 6.1 Screening procedures 104
6.1.1 Screening procedures—particular requirements 104

Part 6.2 AML/CFT training programme 106
6.2.1 Appropriate AML/CFT training programme to be delivered etc 106
6.2.2 Training must be maintained and reviewed 107

Chapter 7 Providing documentary evidence of compliance 109

Part 7.1 General record-keeping obligations 109
7.1.1 Records about compliance 109
7.1.2 How long records must be kept 110
7.1.3 Retrieval of records 110

Part 7.2 Particular record-keeping obligations 112
7.2.1 Records for customers and transactions 112
7.2.2 Training records 113

Glossary 114

Endnotes 123

Chapter 1 General provisions

Part 1.1 Introductory

1.1.1 Name of rules

These rules are the *Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019* (AML/CFTR).

1.1.2 Commencement

These rules commence on 1 February 2020.

1.1.3 Repeal of 2010 AML/CFTR

(1) The *Anti-Money Laundering and Combating Terrorist Financing Rules 2010* is repealed.

(2) A reference to the *Anti-Money Laundering and Combating Terrorist Financing Rules 2010* or to any of its provisions in other Rules or any instrument that has not been specifically changed is taken to be a reference to the *Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019* or to their equivalent provisions as necessary to give effect to those Rules, instrument or provisions.

1.1.4 Application of these rules

(1) These rules apply to firms that conduct business or activities in or from this jurisdiction.

(2) A reference in these rules to a ***firm*** is a reference to a firm that conducts, and so far as it conducts, business or activities in or from this jurisdiction, unless these rules otherwise provide.

(3) However, these rules do not apply to a firm to which the *Anti-Money Laundering and Combating the Financing of Terrorism (General*

Insurance) Rules 2019 (AMLG) apply. A reference in these rules to a ***firm*** does not include such a firm.

Note The AMLG apply to a firm that conducts only either or both of (a) general insurance business and (b) insurance mediation in relation to either or both of general insurance contracts and non-investment insurance contracts.

1.1.5 Effect of definitions, notes and examples

(1) A definition in the Glossary also applies to any instructions or document made under these rules.

(2) A note in or to these rules is explanatory and is not part of these rules. However, examples and guidance are part of these rules.

(3) An example is not exhaustive, and may extend, but does not limit, the meaning of these rules or the particular provision of these rules to which it relates.

Note Under FSR, art 17 (4), guidance is indicative of the view of the Regulatory Authority at the time and in the circumstances in which it was given.

1.1.6 References to particular currencies

In these rules, the specification of an amount of money in a particular currency is also taken to specify the equivalent sum in any other currency at the relevant time.

Part 1.2 Key AML/CFT principles

1.2.1 Principle 1—responsibilities

The Governing Body of a firm is responsible for approving the policies, procedures, systems and controls necessary to ensure the effective prevention of money laundering and terrorism financing. The senior management of the firm must ensure that the policies, procedures, systems and controls are implemented, and that they appropriately and adequately address the requirements of the AML/CFT Law and these rules.

1.2.2 Principle 2—risk-based approach

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

1.2.3 Principle 3—know your customer

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

1.2.4 Principle 4—effective reporting

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

1.2.5 Principle 5—high standard screening and appropriate training

A firm 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 firm 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 *firm*?

A ***firm*** is a financial institution or a DNFBP.

1.3.2 What is a *financial institution*?

(1) A ***financial institution*** is any entity that conducts, as a business, 1 or more of the following activities for or on behalf of a customer:

(a) accepting deposits or other repayable funds from the public, including, for example, private banking;

(b) lending (including consumer credit and mortgage credit), the purchase of debts and equity whether with or without the right to recourse, and financing commercial transactions;

(c) financial leasing, other than financial leasing arrangements in relation to consumer products;

(d) transferring money or value, whether in the formal sector or informal sector (such as an alternative remittance activity), but does not include the provision to a financial institution of services consisting solely of the provision of messaging or other support services for transmitting funds;

(e) issuing or managing means of payment, including, for example, credit and debit cards, cheques, travellers' cheques, money orders, bankers' drafts and electronic money;

(f) providing financial guarantees or commitments;

(g) trading in:

(i) money market instruments, including, for example, cheques, bills, certificates of deposit and derivatives;

(ii) foreign exchange;

(iii) exchange, interest rate and index instruments;

(iv) transferable securities; or

(v) commodity futures;

(h) participating in securities issues and providing financial services related to securities issues;

(i) undertaking individual or collective portfolio management;

(j) safekeeping or administering cash or liquid securities on behalf of other entities;

(k) otherwise investing, administering or managing funds on behalf of other entities;

(l) underwriting or placing life insurance and other investment-related insurance, whether as insurer or insurance intermediary;

(m) money or currency changing;

(n) any other activity or transaction prescribed by a decision of the Council of Ministers under Article 2 of the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing.

(2) Despite subrule (1), every authorised firm (other than an authorised firm that is a firm within the meaning given by the *Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012*, rule 1.3.1) is a ***financial institution***.

1.3.3 What is a *DNFBP*?

(1) A ***designated non-financial business or profession*** (or ***DNFBP***) is any of the following:

(a) a real estate agent, if the agent acts for clients in relation to the buying or selling of real estate (or both);

(b) a dealer in precious metals or stones, if the dealer engages in cash transactions with customers with a value (or, for transactions that are or appear to be linked, with a total value) of at least QR 50,000;

(c) a lawyer, notary, other independent legal professional, or accountant, whether a sole practitioner, partner or employed professional in a professional firm, if the person prepares, executes or conducts transactions for clients in relation to all or any of the following activities:

(i) buying or selling real estate;

(ii) managing client money, securities or other assets;

(iii) managing bank, savings or securities accounts;

(iv) organising contributions for the creation, operation or management of companies or other entities;

(v) creating, operating or managing legal persons or legal arrangements;

(vi) buying or selling business entities;

(d) a trust and company service provider, if the provider prepares or conducts transactions for clients on a commercial basis in relation to all or any of the following activities:

(i) acting as a formation agent of legal persons;

(ii) acting, or arranging for another person to act, as a director or secretary of a company or a partner of a partnership, or having a similar position in relation to other legal persons;

(iii) providing a registered office, business address or accommodation, or providing a correspondence or administration address, for a company, a partnership or any other legal person or legal arrangement;

(iv) acting as, or arranging for another person to act as, a trustee of an express trust;

(v) acting as, or arranging for another person to act as, a nominee shareholder for another entity;

(e) any other business or professional entity prescribed by a decision of the Council of Ministers under Chapter 1 of the AML/CFT Law, definition of DNFBP;

but does not include a financial institution.

(2) A ***DNFBP*** is also any auditor, tax consultant or insolvency practitioner, whether a sole practitioner, partner or employed professional in a professional firm, if the person prepares or conducts transactions for clients in relation to all or any of the activities mentioned in subrule (1) (c) (i) to (vi), but does not include a financial institution.

(3) Subrules (1) (c) and (2) do not apply to:

(a) a professional employed by a business that is not a legal professional, accounting, auditing, tax consultancy or insolvency business; or

(b) a professional employed by a government agency.

(4) If an entity that has been granted a licence by the Qatar Financial Centre Authority (other than a financial institution) proposes to conduct any activity mentioned in subrule (1) in or from this jurisdiction, the firm is taken to be a ***DNFBP***.

1.3.4 Who is a *customer*?

(1) A ***customer***, in relation to a firm, includes any person who engages in, or who has contact with the firm with a view to engaging in, any transaction with the firm or a member of the firm's group:

(a) on the person's own behalf; or

(b) as agent for or on behalf of another person.

(2) To remove any doubt, ***customer*** also includes:

(a) any person receiving a service offered by the firm (or by a member of the firm's group) in the normal course of its business; and

(b) a client or investor, or prospective client or investor, of the firm or a member of the firm's group.

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;

(b) for a transaction—the individual for whom, or on whose behalf, the transaction is ultimately being, or is ultimately to be, conducted (whether by proxy, trusteeship or mandate, or by any other form of representation); or

(c) for a legal person or legal arrangement—the individual who ultimately owns, or exercises effective control over, the person or arrangement.

(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 20% 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 20% of the funds of the arrangement;

(b) if the beneficiaries or their distributions have not already been decided—the class of individuals 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 20% (by value) of the property of the arrangement.

1.3.6 Politically exposed persons, their family members and associates

(1) A ***politically exposed person (PEP)*** means an individual who is, or has been, entrusted with prominent public functions.

Examples of persons who can be PEPs

1 Heads of State or of government
2 senior politicians
3 senior government, judicial or military officials
4 members of Parliament
5 important political party officials
6 senior executives of state owned companies
7 members of senior management (directors, deputy directors and members of the board or equivalent functions) in international organisations.

(3) A ***family member of a PEP*** means an individual related to the PEP by blood, or by marriage, up to the second degree.

Examples of individuals related to a PEP in the first or second degree

1 the PEP's father and mother
2 the PEP's husband or wife
3 the PEP's father-in-law or mother-in law
4 the PEP's son or daughter
5 the PEP's stepson or stepdaughter
6 the PEP's grandfather and grandmother
7 the PEP's brother or sister
8 the PEP's brother-in-law or sister-in-law
9 the PEP's grandson or granddaughter

(3) A person is a ***close associate of a PEP*** if the person:

(a) is in partnership with the PEP in a legal person or legal arrangement;

(b) is associated with the PEP through a business or social relationship; or

(c) is a beneficial owner of a legal person or legal arrangement owned, or effectively controlled, by the PEP.

1.3.7 What is *correspondent banking*?

Correspondent banking is the provision of banking services by a bank (the ***correspondent***) to another bank (the ***respondent***).

Examples of banking services that may be provided to respondent

1 cash management (including interest-bearing accounts in different currencies)
2 wire transfers
3 cheque clearing
4 payable-through accounts
5 foreign exchange

1.3.8 What is a *shell bank*?

(1) 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.

(2) For this rule, ***physical presence*** in a jurisdiction is a presence involving effective management that has the authority to make

decisions, and not merely the presence of a local agent or low-level staff.

1.3.9 What is a *correspondent securities relationship*?

A ***correspondent securities relationship*** is a relationship under which services in relation to securities are provided by a firm (the ***correspondent***) to another firm (the ***respondent***).

Examples of services in relation to securities

buying, selling, lending or otherwise holding securities

Chapter 2 General AML and CFT responsibilities

Part 2.1 The firm

2.1.1 Firms to develop AML/CFT programme

(1) A firm must develop a programme against money laundering and terrorism financing.

(2) The type and extent of the measures adopted by the firm as part of its programme must be appropriate having regard to the risk of money laundering and terrorism financing and the size, complexity and nature of its business.

(3) However, the programme must, as a minimum, include:

(a) developing, establishing and maintaining internal policies, procedures, systems and controls to prevent money laundering and terrorism financing;

(b) adequate screening procedures to ensure high standards when appointing or employing officers or employees;

Note See also Part 6.1 (Screening procedures).

(c) an appropriate ongoing training programme for its officers and employees;

Note See also Part 6.2 (AML/CFT training programme).

(d) an independent review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls in accordance with subrule (4);

(e) appropriate compliance management arrangements; and

Note See also:

- rule 2.1.5 (Compliance by officers, employees, agents etc)

- rule 2.1.6 (Application of AML/CFT Law requirements, policies etc to branches and associates)
- rule 2.1.7 (Application of AML/CFT Law requirements, policies etc to outsourced functions and activities).

(f) the appropriate ongoing assessment and review of the policies, procedures, systems and controls.

Note See also rule 2.1.4 (Assessment and review of policies etc).

(4) The review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls must be adequately resourced and must be conducted at least once every 2 years. The person making the review must be professionally competent, qualified and skilled, and must be independent of:

(a) the function being reviewed; and

(b) the division, department, unit or other part of the firm where that function is performed.

Note The review and testing may be conducted by the firm's internal auditor, external auditor, risk specialist, consultant or an MLRO from another branch of the firm. Testing would include, for example, sample testing the firm's AML/CFT programme, screening of employees, record making and retention and ongoing monitoring for customers.

(5) The firm must make and keep a record of the results of its review and testing under subrule (4) and must give the Regulator a copy of the record by 31 July 2021 and every 2 years thereafter.

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

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

2.1.3 Matters to be covered by policies etc

(1) A firm's AML/CFT policies, procedures, systems and controls must, as a minimum, cover:

(a) CDD 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 firm's officers and employees; and

(f) anything else required under the AML/CFT Law or these rules.

(2) Without limiting subrule (1), the firm'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 firm considers particularly likely by their nature to be related to money laundering or terrorism financing;

(b) require the taking of enhanced CDD to prevent the use for money laundering or terrorism financing of products and transactions that might favour anonymity;

(c) provide appropriate measures to reduce the risks associated with establishing business relationships with PEPs;

(d) before any function or activity is outsourced by the firm, require an assessment to be made and documented of the money laundering and terrorism financing risks associated with the outsourcing;

(e) require the risks associated with the outsourcing of a function or activity by the firm to be monitored on an ongoing basis;

(f) require everyone in the firm to comply with the requirements of the AML/CFT Law and these rules in relation to the making of suspicious transaction reports;

(g) set out the conditions that must be satisfied to permit a customer to use the business relationship even before the customer's identity (or the identity of the beneficial owner of the customer) is verified;

Note For the situations when verification of identity may be delayed, see rules 4.3.5 and 4.5.1 (2).

(h) ensure that there are appropriate systems and measures to enable the firm to implement any targeted financial sanction that may be required under Law No. (27) of 2019 on Combating Terrorism, and for complying with any other requirements of that law; and

Note ***Targeted financial sanction*** is defined in the Glossary.

(i) be designed to ensure that the firm can otherwise comply, and does comply, with the AML/CFT Law and these rules.

2.1.4 Assessment and review of policies etc

A firm 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 terrorism financing.

Note For other annual assessments and reviews, see:

- rule 2.3.8 (Minimum annual report by MLRO)
- rule 2.3.9 (Consideration of MLRO reports)
- rule 3.3.5 (3) (Correspondent banking relationships generally)
- rule 3.3.12 (3) (Correspondent securities relationships generally).

2.1.5 Compliance by officers, employees, agents etc

(1) A firm 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 this subrule from applying.

(2) Without limiting subrule (1), the firm's AML/CFT policies, procedures, systems and controls:

(a) must require officers, employees, agents and contractors, wherever they are, to provide the firm's MLRO with suspicious transaction reports for transactions in, from or to this jurisdiction; and

(b) must provide timely, unrestricted access by the firm's senior management and MLRO, and by the Regulator and FIU, to documents and information of the firm, wherever they are held, that relate directly or indirectly to its customers or accounts or to transactions in, from or to this jurisdiction;

except so far as the law of another jurisdiction prevents this subrule from applying.

(3) Subrule (2) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to this jurisdiction.

(4) This rule does not prevent the firm from applying higher, consistent standards in its AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend over 2 or more jurisdictions.

(5) If the law of another jurisdiction prevents a provision of this rule from applying to an officer, employee, agent or contractor of the firm, the firm must immediately tell the Regulator about the matter.

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

(1) This rule applies to a firm if:

(a) it has a branch or associate in Qatar; or

(b) it has a branch in a foreign jurisdiction, or an associate in a foreign jurisdiction over which it can exercise control.

(2) The firm 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 firm's AML/CFT policies, procedures, systems and controls;

except so far as the law of another jurisdiction prevents this subrule from applying.

(3) Without limiting subrule (2), the firm's AML/CFT policies, procedures, systems and controls:

(a) must require the branch or associate, and the officers, employees, agents and contractors of the branch or associate, wherever they are, to provide to the firm's MLRO suspicious transaction reports for transactions in, from or to this jurisdiction; and

(b) must provide timely, unrestricted access by the firm's senior management and MLRO, and by the Regulator and FIU, to documents and information of the branch or associate, wherever they are held, that relate directly or indirectly to its customers or accounts or to transactions in, from or to this jurisdiction;

except so far as the law of another jurisdiction prevents this subrule from applying.

(4) Subrule (3) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to this jurisdiction.

(5) Despite subrule (2), if the AML/CFT requirements of this jurisdiction and another jurisdiction differ, the branch or associate must apply the requirements that impose the highest standard, except so far as the law of another jurisdiction prevents this subrule from applying.

(6) Also, this rule does not prevent the firm and its branches, or the firm and the other members of its group, from applying higher, consistent

standards in their AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend across the firm and its branches or the firm and the other members of its group.

(7) If the law of another jurisdiction prevents a provision of this rule from applying to the branch or associate or any of its officers, employees, agents or contractors, the firm:

(a) must immediately tell the Regulator about the matter; and

(b) must apply additional measures to manage the money laundering and terrorism financing risks (for example, by requiring the branch or associate to give to the firm additional information and reports).

(8) If the Regulator is not satisfied with the additional measures applied by the firm under subrule (7) (b), the Regulator may, on its own initiative, apply additional supervisory measures by, for example, directing the firm:

(a) in the case of a branch—to suspend the transactions through the branch in the foreign jurisdiction; or

(b) in the case of an associate—to suspend the transactions of the associate insofar as they relate to Qatar.

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

(1) This rule applies if a firm outsources any of its functions or activities to a third party.

Note See also rule 2.1.3 (2) (d) and (e) (Matters to be covered by policies etc) for other requirements relating to outsourcing.

(2) The firm, and its senior management, remain responsible for ensuring that the AML/CFT Law and these rules are complied with.

(3) The firm must, through a service level agreement or otherwise, 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 firm's AML/CFT policies, procedures, systems and controls;

except so far as the law of another jurisdiction prevents this subrule from applying.

(4) Without limiting subrule (3), the firm's AML/CFT policies, procedures, systems and controls:

(a) must 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 this jurisdiction involving the firm (or the third party on its behalf) to the firm's MLRO; and

(b) must provide timely, unrestricted access by the firm'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 the firm's customers or accounts or to transactions in, from or to this jurisdiction involving the firm (or the third party on its behalf);

except so far as the law of another jurisdiction prevents this subrule from applying.

(5) Subrule (4) (a) does not prevent a suspicious transaction report also being made in another jurisdiction for a transaction in, from or to this jurisdiction.

(6) If the law of another jurisdiction prevents a provision of this rule from applying to the third party or any of its officers, employees, agents or contractors:

(a) the third party must immediately tell the firm about the matter; and

(b) the firm must immediately tell the Regulator about the matter.

(7) If the firm is an authorised firm, this rule is in addition to any other provision of the Regulator's Rules about outsourcing.

Part 2.2 Senior management

Note for Part 2.2

Principle 1 (see rule 1.2.1) requires the senior management of a firm to ensure that the firm's policies, procedures, systems and controls are implemented, and that they 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 firm is responsible for the effectiveness of the firm's policies, procedures, systems and controls in preventing money laundering and terrorism financing.

2.2.2 Particular responsibilities of senior management

(1) The senior management of a firm must ensure:

(a) that the firm develops, establishes and maintains effective AML/CFT policies, procedures, systems and controls in accordance with these rules;

(b) that the firm has adequate screening procedures to ensure high standards when appointing or employing officers or employees;

(c) that the firm identifies, designs, delivers and maintains an appropriate ongoing AML/CFT training programme for its officers and employees;

Note See Part 6.2 (AML/CFT training programme) for details of the firm's training requirements.

(d) that independent review and testing of the firm's compliance with its AML/CFT policies, procedures, systems and controls are conducted in accordance with rule 2.1.1 (4);

(e) that regular and timely information is made available to senior management about the management of the firm's money laundering and terrorism financing risks;

(f) that the firm's money laundering and terrorism financing risk management policies and methodology are appropriately documented, including the firm's application of them;

(g) that there is at all times an MLRO for the firm who:

(i) has sufficient seniority, knowledge, experience and authority;

(ii) has an appropriate knowledge and understanding of the legal and regulatory responsibilities of the role, the AML/CFT Law and these rules;

(iii) has sufficient resources, including appropriate staff and technology, to carry out the role in an effective, objective and independent way;

(iv) has timely, unrestricted access to all information of the firm relevant to AML and CFT, including, for example:

(A) all customer identification documents and all source documents, data and information;

(B) all other documents, data and information obtained from, or used for, CDD and ongoing monitoring; and

(C) all transaction records; and

(v) has appropriate back-up arrangements to cover absences, including a Deputy MLRO to act as MLRO;

(h) that a firm-wide AML/CFT compliance culture is promoted within the firm;

Guidance

The Regulatory Authority expects a firm's senior management to ensure that there is an AML/CFT culture within the firm where:

- senior management consistently enforces a top-down approach to its AML/CFT responsibilities;
- there is a demonstrable and sustained firm-wide commitment to the AML/CFT principles and compliance with the AML/CFT Law, these rules and the firm's AML/CFT policies, procedures, systems and controls;
- AML/CFT risk management and regulatory requirements are embedded at all levels of the firm and in all elements of its business or activities.

(i) that appropriate measures are taken to ensure that money laundering and terrorism financing risks are taken into account in the day-to-day operation of the firm, including in relation to:

(i) the development of new products;

(ii) the taking on of new customers; and

(iii) changes in the firm's business profile; and

(j) that all reasonable steps have been taken so that a report required to be given to the Regulator for AML or CFT purposes is accurate, complete and given promptly.

(2) This rule does not limit the particular responsibilities of the senior management of the firm.

Note See, for example, Division 2.3.C (Reporting by MLRO to senior management).

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

(1) A firm must ensure that there is at all times an MLRO and a Deputy MLRO for the firm.

(2) Accordingly, the firm must, from time to time, appoint an individual as its MLRO and another individual as its Deputy MLRO.

2.3.2 Eligibility to be MLRO or Deputy MLRO

(1) The MLRO and Deputy MLRO for a firm:

(a) must be employed at the management level by the firm, or by a legal person in the same group, whether as part of its governing body, management or staff; and

(b) must have sufficient seniority, knowledge, experience and authority for the role, and in particular:

(i) to act independently; and

(ii) to report directly to the firm's senior management.

(2) The MLRO for a QFC insurer (other than a QFC captive insurer) that is a company incorporated under the Companies Regulations 2005, or a QFC bank, must be ordinarily resident in Qatar.

(3) In the case of any other firm:

(a) if the firm proposes to appoint as MLRO an individual who is not ordinarily resident in Qatar, the firm must satisfy the Regulator that the MLRO function can be adequately exercised by an MLRO who is not resident in Qatar; and

(b) if the Regulator considers that the MLRO function for the firm cannot be adequately exercised by an MLRO who is not resident in Qatar, the Regulator may direct the firm to appoint as MLRO an individual who is ordinarily resident in Qatar.

Division 2.3.B Roles of MLRO and Deputy MLRO

2.3.3 General responsibilities of MLRO

The MLRO for a firm is responsible for:

(a) overseeing the implementation of the firm's AML/CFT policies, procedures, systems and controls in relation to this jurisdiction, including the operation of the firm's risk-based approach;

(b) ensuring that appropriate policies, procedures, systems and controls are developed, established and maintained across the firm to monitor the firm's day-to-day operations:

(i) for compliance with the AML/CFT Law, these rules, and the firm's AML/CFT policies, procedures, systems and controls; and

(ii) to assess, and regularly review, the effectiveness of the policies, procedures, systems and controls in preventing money laundering and terrorism financing;

(c) being the firm's key person in implementing the firm's AML/CFT strategies in relation to this jurisdiction;

(d) supporting and coordinating senior management focus on managing the firm's money laundering and terrorism financing risks in individual business areas;

(e) helping to ensure that the firm's wider responsibility for preventing money laundering and terrorism financing is addressed centrally; and

(f) promoting a firm-wide view to be taken of the need for AML/CFT monitoring and accountability.

2.3.4 Particular responsibilities of MLRO

(1) The MLRO for a firm is responsible for:

(a) receiving, investigating and assessing internal suspicious transaction reports for the firm;

(b) making suspicious transaction reports to the FIU and telling the Regulator about them;

(c) acting as central point of contact between the firm, and the FIU, the Regulator and other State authorities, in relation to AML and CFT issues;

(d) responding promptly to any request for information by the FIU, the Regulator and other State authorities in relation to AML and CFT issues;

(e) receiving and acting on government, regulatory and international findings about AML and CFT issues;

(f) monitoring the appropriateness and effectiveness of the firm's AML/CFT training programme;

(g) reporting to the firm's senior management on AML and CFT issues;

(h) keeping the Deputy MLRO informed of significant AML/CFT developments (whether internal or external); and

(i) exercising any other functions given to the MLRO, whether under the AML/CFT Law, these rules or otherwise.

(2) If the Regulator issues guidance, the MLRO must bring it to the attention of the firm's senior management. The firm must make and keep a record of:

(a) whether the senior management took the guidance into account;

(b) any action that the senior management took as a result; and

(c) the reasons for taking or not taking action.

2.3.5 Role of Deputy MLRO

(1) The Deputy MLRO for a firm acts as the firm'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, these rules apply in relation to the Deputy MLRO as if the Deputy MLRO were the MLRO.

(3) However, to remove any doubt, rule 2.3.2 (2) (Eligibility to be MLRO or Deputy MLRO) does not apply in relation to the Deputy MLRO of a QFC insurer (other than a QFC captive insurer) that is a company incorporated under the Companies Regulations 2005 or a QFC bank when the Deputy MLRO acts as MLRO.

2.3.6 How MLRO must carry out role

The MLRO for a firm must act honestly, reasonably and independently, particularly in:

(a) receiving, investigating and assessing internal suspicious transaction reports; and

(b) 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 firm 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, the MLRO must give the senior management a report that complies with rule 2.3.8 (Minimum annual report by MLRO) for each calendar year. The report must be given in time to enable compliance 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 calendar year (see rule 2.3.7 (2)).

(2) The report must assess the adequacy and effectiveness of the firm's AML/CFT policies, procedures, systems and controls in preventing money laundering and terrorism 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 firm of the AML/CFT Law, these rules, or the firm's AML/CFT policies, procedures, systems and controls;

(e) areas where the firm'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 firm's officers and employees;

(g) areas where the firm's AML/CFT training programme should be improved, and proposals for making appropriate improvements;

(h) the number and types of customers of the firm that are categorised as high risk;

(i) progress in implementing any AML/CFT action plans;

Note These provisions require action plans:

- rule 2.3.9 (b) (Consideration of MLRO reports)

- rule 4.3.4 (3) and (4) (When CDD may not be required—acquired businesses)
- rule 6.2.2 (3) (b) (Training must be maintained and reviewed).

(j) the outcome of any relevant quality assurance or audit reviews in relation to the firm's AML/CFT policies, procedures, systems and controls;

(k) the outcome of any review of the firm's risk assessment policies, procedures, systems and controls.

2.3.9 Consideration of MLRO reports

(1) The senior management of a firm must promptly:

(a) consider each report made to it by the MLRO; and

(b) if the report identifies deficiencies in the firm's compliance with the AML/CFT Law or these rules—approve an action plan to remedy the deficiencies.

(2) For the report that must be given for each calendar year under rule 2.3.7 (2), the senior management must confirm in writing that it has considered the report and, if an action plan is required, has approved such a plan. The firm's MLRO must give the Regulator a copy of the report and confirmation before 1 June of the next year.

Division 2.3.D Additional obligations etc of firm with non-resident MLRO

2.3.10 Annual reports

A firm whose MLRO is not ordinarily resident in Qatar must report to the Regulator, in a form approved for this rule under the *General Rules 2005*, before 1 June in each year.

2.3.11 Visits by non-resident MLRO

A firm whose MLRO is not ordinarily resident in Qatar must ensure that the MLRO inspects the firm's operations in Qatar frequently

enough to allow him or her to assess the accuracy and reliability of the information supplied to the Regulator in the reports required by rule 2.3.10.

2.3.12 Regulatory Authority may direct firm to appoint resident MLRO

(1) This rule applies if, for any reason, the Regulator considers that the MLRO function for a firm is not being adequately exercised by an individual who is not ordinarily resident in Qatar.

(2) The Regulator may direct the firm:

(a) to require the individual to be ordinarily resident in Qatar; or

(b) to appoint another individual who is ordinarily resident in Qatar.

Chapter 3 The risk-based approach

Part 3.1 The risk-based approach generally

Note for Part 3.1

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

3.1.1 Firms must conduct risk assessment and decide risk mitigation

(1) A firm:

(a) must conduct, at regular and appropriate intervals, an assessment (a ***business risk assessment***) of the money laundering and terrorism financing risks that it faces, including risks identified in the National Risk Assessment and those that may arise from:

(i) the types of customers that it has (and proposes to have) (***customer risk***);

(ii) the products and services that it provides (and proposes to provide) (***product risk***);

(iii) the technologies that it uses (and proposes to use) to provide those products and services (***interface risk***); and

(iv) the jurisdictions with which its customers are (or may become) associated (***jurisdiction risk***); and

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.

(b) must decide what action is needed to mitigate those risks.

(2) The firm must be able to demonstrate:

(a) how it determined the risks that it faces;

(b) how it took into consideration the National Risk Assessment and other sources in determining those risks;

(c) when and how it conducted the business risk assessment; and

(d) how the actions it has taken after the assessment have mitigated, or have failed to mitigate, the risks it faces.

(3) If the firm fails to take into account the National Risk Assessment and other sources or fails to assess any of the risks it faces, it must give the reasons for its failure to do so, if required by the Regulator.

3.1.2 Approach to risk mitigation must be based on suitable methodology

(1) The intensity of a firm's approach to the mitigation of its money laundering and terrorism financing risks must be based on a suitable methodology (a ***threat assessment methodology***) that addresses the risks that it faces.

(2) A firm must be able to demonstrate that its threat assessment methodology:

(a) includes:

(i) identifying the purpose and intended nature of the business relationship with each customer; and

(ii) assessing the risk profile of the business relationship by scoring the relationship;

Note 1 ***Business relationship*** is defined in rule 4.2.4.

Note 2 For scoring the business relationship in relation to customer risk, product risk, interface risk and jurisdiction risk, see rule 3.2.3, rule 3.3.3, rule 3.4.3 and rule 3.5.3, respectively.

(b) is suitable for the size, complexity and nature of the firm's business;

(c) is designed to enable the firm:

(i) to identify and recognise any changes in its money laundering and terrorism 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 firm 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 firm 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 firm 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 firm 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 CDD and ongoing monitoring to be conducted for the customer.

Note Each of the 4 risk elements mentioned in subrule (1) is dealt with in the following Parts of this Chapter.

Part 3.2 Customer risk

Note for Part 3.2

This Part relates to the risks posed by the types of customers of a firm.

3.2.1 Risk assessment for customer risk

(1) A firm must assess and document the risks of money laundering, terrorism 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 PEPs

(2) The intensity of the CDD 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.

Example

The duration of the relationship with the customer and the frequency of transactions may affect the intensity of CDD and ongoing monitoring.

3.2.2 Policies etc for customer risk

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

3.2.3 Scoring business relationships—types of customers

A firm must include, in its methodology, a statement of the basis on which business relationships with customers will be scored, having regard to the different types of customers it has (and proposes to have).

Example

The risk to the firm from a salaried employee whose only transactions are derived from electronic payments made by the employee's employer are likely to be much

lower than the risk to the firm from an individual whose transactions are cash-based with no discernible source for those funds.

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

(1) This rule applies to a customer of a firm if the firm knows or suspects that the customer is an individual, charity, non-profit organisation or other entity:

(a) that is associated with, or involved in, terrorist acts, terrorism financing or a terrorist organisation; or

(b) that is subject to sanctions or other international initiatives.

(2) Irrespective of the risk score otherwise obtained for the customer, the firm must conduct enhanced CDD and enhanced ongoing monitoring for the customer.

Note See rule 4.2.2 (What is *ongoing monitoring*?) and rule 4.3.13 (Ongoing monitoring required).

(3) A decision to enter into a business relationship with the customer must only be taken with senior management approval after enhanced CDD has been conducted.

3.2.5 Measures for PEPs

(1) A firm must, as a minimum, adopt the following measures to reduce the risks associated with establishing and maintaining business relationships with PEPs:

(a) the firm must have clear policies, procedures, systems and controls for business relationships with PEPs;

(b) the firm 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

(c) decisions to enter into business relationships with PEPs must only be taken with senior management approval after enhanced CDD has been conducted;

(d) 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 only with senior management approval;

(e) the firm must take reasonable measures to establish the sources of wealth and funds of customers and beneficial owners identified as PEPs;

(f) PEPs must be subject to enhanced ongoing monitoring.

(2) The firm must take the measures required by subrule (1) in relation to a family member or close associate of a PEP if, on a risk-sensitive basis, the firm considers that the family member or close associate should be treated as a PEP.

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

(1) A firm's risk assessment process must include a recognition of the risks posed by legal persons, legal arrangements and facilities.

Examples of legal persons

1 companies

2 partnerships

Example of legal arrangement

express trust

Examples of facilities

1 nominee shareholdings

2 powers of attorney

(2) In assessing the risks posed by a legal person or legal arrangement, a firm must ensure that the risk profile of the person or arrangement

takes into account the risks posed by any beneficial owners, officers, shareholders, trustees, settlors, beneficiaries, managers and other relevant entities.

(3) In assessing the risks posed by a facility, a firm must ensure that the facility's risk profile takes into account the risks posed by any reduction in transparency, or any increased ability to conceal or obscure.

(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.

3.2.7 Measures for persons in terrorist list

(3) A firm must, from the outset of its dealings with an applicant for business and on an ongoing basis during the business relationship, check whether the person is listed:

(a) under a relevant resolution of the UN Security Council; or

(b) in a Terrorist Designation Order published by the National Counter Terrorism Committee of the State.

(4) If the person is listed, the firm:

(a) must not establish, or continue, a relationship with, or carry out a transaction with or for the person;

(b) must make a suspicious transaction report to the FIU; and

(c) must immediately tell the Regulator.

Part 3.3 Product risk

Notes for Part 3.3

1 This Part relates to the risks posed by the types of products offered by a firm.

2 ***Product*** includes the provision of a service (see Glossary).

3.3.1 Risk assessment for product risk

(1) A firm must assess and document the risks of money laundering, terrorism financing and other illicit activities posed by the types of products it offers (and proposes to offer).

Examples of types of products

1 savings accounts

2 e-money products

3 payable-through accounts

4 wire transfers

5 life insurance contracts

(2) The intensity of the CDD and ongoing monitoring conducted 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.

Example

The level of deposits and the volume of transactions and operations that a customer has may affect the intensity of CDD and ongoing monitoring.

3.3.2 Policies etc for product risk

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

3.3.3 Scoring business relationships—types of products

A firm 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 (and proposes to offer) to them.

3.3.4 Products with fictitious or false names or no names

(1) A financial institution 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 financial institution from providing a level of privacy to the customer within the financial institution 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 firm itself; and

(b) the records are available to the financial institution's senior management and MLRO, and to the Regulator and FIU.

(3) Without limiting subrule (1), if the financial institution has numbered accounts, the financial institution must maintain them in a way that enables it to fully comply with the AML/CFT Law and these rules.

Example for subrule (3)

The financial institution 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, other appropriate officers and employees, the Regulator and the FIU.

3.3.5 Correspondent banking relationships generally

(1) Before a bank (the ***correspondent***) establishes a correspondent banking relationship with a bank (the ***respondent***) in a foreign jurisdiction, the correspondent must do all of the following:

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) decide from publicly available information the respondent'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 the respective responsibilities of the respondent and correspondent, including in relation to AML and CFT matters;

(f) be satisfied that, in relation to the respondent's customers that will have direct access to accounts of the correspondent, the respondent:

(i) will have conducted CDD for the customers and verified the customers' identities;

(ii) will conduct ongoing monitoring for the customers; and

(iii) will be able to provide to the correspondent, 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 correspondent must consider all of the following:

(a) whether the respondent has been the subject of any investigation, or civil or criminal proceeding, relating to money laundering or terrorism financing;

(b) the respondent'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 in which it operates has an effective AML/CFT regime;

(e) if the respondent 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 PEP).

(3) If the correspondent establishes a correspondent banking relationship with the respondent, the correspondent must:

(a) if the respondent 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 shell bank must not be established in, or operate in or from, this jurisdiction.

Note ***Shell bank*** is defined in rule 1.3.8.

(2) A financial institution must not enter into, or continue, a correspondent banking relationship or correspondent securities relationship with a shell bank.

(3) A financial institution must not enter into, or continue:

(a) a correspondent banking relationship with a bank in any jurisdiction if the bank is known to permit its accounts to be used by a shell bank; or

(b) a correspondent securities relationship with a firm in any jurisdiction if the firm 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 bank (the ***correspondent***) has a correspondent banking relationship with a bank (the ***respondent***) in a foreign jurisdiction; and

(b) under the relationship, a customer of the respondent who is not a customer of the correspondent may have direct access to an account of the correspondent.

(2) The correspondent must not allow the customer to have access to the account unless the correspondent is satisfied that the respondent:

(a) has conducted CDD for the customer and verified the customer's identity;

(b) conducts ongoing monitoring for the customer; and

(c) can provide to the correspondent, on request, the documents, data and information obtained in conducting CDD and ongoing monitoring for the customer.

(3) If:

(a) the correspondent asks the respondent for documents, data or information mentioned in subrule (2) (c); and

(b) the respondent fails to satisfactorily comply with the request;

the correspondent must immediately terminate the customer's access to accounts of the correspondent and consider making a suspicious transaction report to the FIU.

(4) ***Payable-through accounts*** are correspondent accounts that are used directly by third parties to transact business on their own behalf.

3.3.8 Powers 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 becoming involved in or associated with a transaction involving the power of attorney, a firm must conduct CDD for both the holder and the grantor.

(3) For subrule (2), the holder and the grantor are both taken to be customers of the firm.

3.3.9 Bearer negotiable instruments

(1) In this rule:

bearer negotiable instrument means:

(a) a monetary instrument in bearer form such as a traveller's cheque;

(b) a negotiable instrument, including cheque, promissory note, and money order that is either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery;

(c) an incomplete instrument including a cheque, promissory note and money order signed, but with the payee's name omitted;

(d) a bearer share; or

(e) a share warrant to bearer.

(2) A firm must have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to the use of bearer negotiable instruments.

(3) Before becoming involved in or associated with a transaction involving the conversion of a bearer negotiable instrument, or the surrender of coupons for a bearer negotiable instrument for payment of dividend, bonus or a capital event, a firm must conduct enhanced CDD 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 firm.

3.3.10 Wire transfers

(1) This rule applies to a transaction conducted by a financial institution (the ***ordering financial institution***) 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 (the ***beneficiary financial institution***).

(2) This rule applies to the transaction whether or not:

(a) the originator and recipient are the same person;

(b) the transaction is conducted through intermediary financial institutions; or

(c) the ordering financial institution, the beneficiary financial institution or any intermediary financial institution is outside Qatar.

(3) However, this rule does not apply to a transaction conducted using a credit or debit card if:

(a) the card number accompanies all transfers flowing from the transaction; and

Examples of transfers that may flow from the transaction

1 withdrawals from a bank account through an ATM

2 cash advances from a credit card

3 payments for goods and services

(b) the card is not used as a payment system to effect a money transfer.

(4) Also, this rule does not apply:

(a) to transfers from 1 financial institution to another; or

(b) if the originator and recipient are both financial institutions acting on their own behalf.

(5) If the ordering financial institution is in Qatar, it:

(a) must obtain and keep full originator information; and

(b) must conduct CDD for the originator;

unless the beneficiary financial institution and all intermediary financial institutions (if any) are in Qatar and the transaction involves the transfer of less than QR 3,500.

Note ***Full originator information*** is defined in the Glossary.

(6) To remove any doubt, the ordering financial institution needs only to comply with subrule (5) once for the originator.

(7) If the ordering financial institution is in Qatar and the beneficiary financial institution or any intermediary financial institution is outside Qatar, the ordering financial institution must include full originator information and full recipient information in a message or payment form accompanying the transfer.

Note ***Full recipient information*** is defined in the Glossary.

(8) However, if several separate transfers from the same originator are bundled in a batch file for transmission to several recipients in a foreign jurisdiction, the ordering financial institution needs only to include the originator's account number or unique reference number in relation to each individual transfer if the batch file (in which the individual transfers are batched) contains full originator information, and full recipient information for each recipient, that is fully traceable in the foreign jurisdiction.

(9) If the ordering financial institution, the beneficiary financial institution and all intermediary financial institutions (if any) are in Qatar, the ordering financial institution must include full originator information and full recipient information in a message or payment form accompanying the transfer unless:

(a) the transaction involves the transfer of less than QR 3,500; or

(b) both of the following conditions are satisfied:

(i) full originator information and full recipient information can be made available to the beneficiary financial institution, the Regulator, the FIU and law enforcement authorities within 3 business days after the day the information is requested;

(ii) law enforcement authorities can compel immediate production of the information.

(10) Each intermediary financial institution (if any) must ensure that all information relating to the originator and recipient that the financial institution receives in a message or payment form accompanying the transfer is transmitted to the next financial institution.

(11) If the beneficiary financial institution is in Qatar and is aware that full originator information or full recipient information has not been provided in a message or payment form accompanying the transfer (and is not fully traceable using a batch file as mentioned in subrule (8)), it must:

(a) either:

(i) reject the transfer; or

(ii) obtain the missing or incomplete information from the ordering financial institution; and

(b) using a risk-sensitive approach, decide whether a suspicious transaction report should be made to the FIU.

(12) If the ordering financial institution has regularly failed to provide the required information about the originators or recipients of transactions and the beneficiary financial institution is in Qatar, the beneficiary financial institution:

(a) must take appropriate steps to ensure that the ordering financial institution does not contravene this rule; and

(b) must report the matter to the FIU.

Examples of steps

1 issuing warnings and setting deadlines for the provision of information

2 rejecting future transfers from the ordering financial institution

3 restricting or terminating any business relationship with the ordering financial institution

(13) Despite anything in these rules, no money or value may be transferred by electronic means to a person listed:

(a) under a relevant resolution of the UN Security Council; or

(b) in a Terrorist Designation Order published by the National Counter Terrorism Committee of the State.

3.3.11 Additional obligations of firms involved in wire transfers

(1) A firm that acts as an intermediary financial institution in a cross-border wire transfer and a firm (the ***beneficiary financial institution***) that makes money available to the recipient after the cross-border wire transfer must take reasonable measures, on a risk-sensitive basis, to identify transfers to this jurisdiction that lack full originator information or full recipient information. The measures may include following-up (whether during, or after, the transfer) on information that is lacking about the originator or recipient.

(2) A firm that acts as intermediary financial institution or beneficiary financial institution must develop, establish and maintain policies, procedures, systems and controls to determine:

(a) when to execute, reject or suspend a wire transfer that lacks the full originator information or full recipient information; and

(b) when to take appropriate follow-up action.

(3) A firm that acts as intermediary financial institution in a cross-border wire transfer must ensure that all originator and recipient information accompanying the transfer is retained with it.

(4) A firm that acts as ordering financial institution, intermediary financial institution or beneficiary financial institution must keep full originator information and full recipient information for at least 10 years after:

(a) if the firm acted as ordering financial institution—the day the originator asked the firm to make the wire transfer;

(b) if the firm acted as intermediary financial institution—the day the firm transmitted the information to another intermediary or to the beneficiary financial institution; or

(c) if the firm acted as beneficiary financial institution—the day the money received via wire transfer is made available to the recipient.

(5) If a wire transfer between 2 financial institutions in Qatar (***domestic wire transfer***) is necessary to effect a cross-border wire transfer and, because of technical limitations, the full originator information and full recipient information cannot remain with the domestic wire transfer, the intermediary financial institution to which the domestic wire transfer is made must, if the intermediary financial institution is a firm, make and keep a record of the information received by it from the ordering financial institution or other intermediary financial institution in relation to the transaction. The record must be kept for 10 years after the day it is made.

(6) If a cross-border wire transfer is effected by the same firm as both ordering and beneficiary financial institutions, or if a firm controls both the originator and recipient of the wire transfer, the firm must take into account the information obtained from both sides of the transfer in considering whether to make a suspicious transaction report. If the firm suspects that the transfer may involve money laundering or terrorism financing, it must:

(a) make a report in each jurisdiction affected by the transfer; and

(b) make available, to the FIU (or its equivalent) in the jurisdiction, information relevant to the transfer.

(7) For wire transfers of more than QR 3,500, the beneficiary financial institution must verify the identity of the recipient before making money available, except if the recipient's identity has previously been verified.

3.3.12 Correspondent securities relationships generally

(1) Before a firm (the ***correspondent***) establishes a correspondent securities relationship with another firm (the ***respondent***) in a foreign jurisdiction, the correspondent must do all of the following:

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) decide from publicly available information the respondent'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 respondent, including in relation to AML and CFT matters;

(f) be satisfied that, in relation to the respondent's customers that will have direct access to accounts of the correspondent, the respondent:

(i) will have conducted CDD for the customers and verified the customers' identities; and

(ii) will conduct ongoing monitoring for the customers; and

(iii) will be able to provide to the correspondent, 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 correspondent must consider all of the following:

(a) whether the respondent has been the subject of any investigation, or civil or criminal proceeding, relating to money laundering or terrorism financing;

(b) the respondent'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 in which it operates has an effective AML/CFT regime;

(e) if the respondent 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 PEP).

(3) If the correspondent establishes a correspondent securities relationship with the respondent, the correspondent must:

(a) if the respondent 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.

Part 3.4 Interface risk

Note for Part 3.4

This Part relates to the risks posed by the mechanisms through which business relationships with a firm are started or conducted.

Division 3.4.A Interface risks—general

3.4.1 Risk assessment for interface risk

(1) A firm must assess and document the risks of money laundering, terrorism financing and other illicit activities posed by the mechanisms through which its business relationships are started and conducted.

(2) The intensity of the CDD 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

(1) A firm must have policies, procedures, systems and controls to address the specific risks of money laundering, terrorism 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 terrorism 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, using ATMs or by telephone or fax

3 electronic point of sale transactions using prepaid, reloadable or account-linked value cards

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

4 requiring first payments by or for non-face-to-face customers to be made through accounts in the customers' names with financial institutions subject to similar customer due diligence standards

(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 firm 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 firm 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 firm 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 financial institution may permit payment processing to take place using on-line services if it ensures that the processing is subject to:

(a) the same monitoring as its other services; and

(b) the same risk-based methodology.

3.4.6 Concession for certain non-face-to-face transactions

(1) This rule applies if:

(a) a customer of a firm would normally be required to produce evidence of identity before transacting business with the firm involving the making of a payment;

(b) it is reasonable in all the circumstances for payment to be made by post or electronically, or for details of the payment to be given by telephone; and

(c) payment is to be made from an account held in the customer's name at a financial institution.

(2) However, this rule does not apply if:

(a) initial or future payments can be received from third parties;

(b) cash withdrawals can be made, unless the withdrawals can only be made by the customer on a face-to-face basis where identity can be confirmed; or

Example of exception

a passbook account where evidence of identity is required to make withdrawals

(c) redemption or withdrawal proceeds can be paid to a third party or to an account that cannot be confirmed as belonging to the customer, unless the proceeds can only be paid to an executor or personal representative on the death of the customer.

(3) If this rule applies, the firm may waive identification requirements for the customer.

(4) However, a repayment may be made to another firm only if the other firm has confirmed that the amount of the repayment is either to be paid to the customer or reinvested elsewhere in the name of the customer.

(5) This rule applies to a joint account as if a reference to the ***customer*** included a reference to any of the customers.

Division 3.4.B Reliance on others generally

3.4.7 Activities to which Division 3.4.B does not apply

This Division does not apply to a firm in relation to CDD conducted for the firm:

(a) by a third-party service provider under an outsourcing;

(b) by an agent under a contractual arrangement between the firm and the agent;

(c) if the firm is a bank—under a correspondent banking relationship to which the firm is a party; or

(d) under a correspondent securities relationship to which the firm is a party.

Note See:

- rule 2.1.5 (Compliance by officers, employees, agents etc)
- rule 2.1.7 (Application of AML/CFT Law requirements, policies etc to outsourced functions and activities)
- rule 3.3.5 (Correspondent banking relationships generally)
- rule 3.3.12 (Correspondent securities relationships generally).

3.4.8 Reliance on certain third parties generally

(1) A firm may rely on introducers, intermediaries or other third parties to conduct some elements of CDD for a customer, or to introduce business to the firm, if it does so under, and in accordance with, this Division.

(2) However, the firm (and, in particular, its senior management) remains responsible for the proper conduct of CDD and ongoing monitoring for its customers.

(3) In determining whether to rely on a third party for purposes of this rule, the firm must have regard to any relevant findings published by international organisations, governments and other bodies about the jurisdiction where the third party is located.

3.4.9 Introducers

(1) This rule applies in relation to a customer introduced to a firm 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 firm; and

(b) the firm 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;

(ii) is subject to the AML/CFT Law and these rules or to equivalent legislation of another jurisdiction;

(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 firm from obtaining any information or original documentation about the customer that the firm may need for AML and CFT purposes.

(2) The firm may rely on the CDD 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.

(3) However, the firm 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;

(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.

3.4.10 Group introductions

(1) This rule applies in relation to a customer introduced to a financial institution in Qatar (the ***local firm***) by another financial institution (***B***) in the same group, whether in or outside Qatar, if:

(a) B or another financial institution in the group (the ***relevant financial institution***) has conducted CDD for the customer; and

(b) subject to subrule (2), the local firm 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;

(ii) it is subject to the AML/CFT Law and these rules or to equivalent legislation of another jurisdiction;

(iii) it is based, or incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime;

(iv) the local firm has all information about the customer obtained from the CDD conducted by the relevant financial institution for the customer that the firm would need if it had conducted the CDD itself;

(v) the local firm 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 local firm need not satisfy itself that all of the conditions in subrule (1) (b) have been met if the Regulator (or the equivalent regulatory or governmental authority, body or agency in another jurisdiction where the relevant financial institution is established) has determined that:

(a) the group's AML/CFT programme, CDD and record-keeping requirements comply with AML/CFT Law and these rules;

(b) the group's implementation of the programme and compliance with the requirements are subject to effective consolidated supervision by the Regulator or its equivalent; and

(c) the group's AML/CFT policies, procedures, systems and controls adequately mitigate risks related to operations in high risk jurisdictions.

(3) The local firm may rely on the CDD 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.

3.4.11 Intermediaries

(1) This rule applies to a firm in relation to a customer of an intermediary, wherever located, if the customer is introduced to the firm 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 and holds funds on the customer's behalf

(2) The firm may treat the intermediary as its customer, and need not conduct CDD itself for the intermediary's customer, if the firm is satisfied that all of the following conditions have been met:

(a) the intermediary is a firm;

(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;

(d) it is based, or incorporated or otherwise established, in Qatar or a foreign jurisdiction that has an effective AML/CFT regime;

(e) the firm has all information about the customer obtained from the CDD conducted by the intermediary for the customer that the firm would need if it had conducted the CDD itself;

(f) the firm 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 firm is not satisfied that all of the conditions in subrule (2) have been met, the firm must conduct CDD itself for the customer.

Division 3.4.C Third party certification—identification documents

3.4.12 Third party certification of identification documents

(1) A firm must not rely, for CDD, 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 firm 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 firm may approve an individual under this subrule if the firm'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;

(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

Note for Part 3.5

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 firm must assess and document the risks of involvement in money laundering, terrorism 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 CDD 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 firm must have policies, procedures, systems and controls to address the specific risks of money laundering, terrorism financing and other illicit activities posed by the types of jurisdictions with which its customers are (or may become) associated.

Examples of 'associated' jurisdiction for a customer

See examples to rule 3.5.1 (1).

3.5.3 Scoring business relationships—types of associated jurisdictions

A firm 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 firm in making a decision about whether a jurisdiction has an effective AML/CFT regime.

(2) The firm 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 firm must have regard to the relevant findings about jurisdictions published by international organisations, governments and other bodies.

Example of international organisation

FATF

3.5.5 Jurisdictions with impaired international cooperation

A firm 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 CDD and enhanced ongoing monitoring.

Examples of impairment

failings in the jurisdiction's judicial or administrative arrangements

3.5.6 Non-cooperative, high risk and sanctioned jurisdictions

A firm must conduct enhanced CDD 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:

(a) that is identified by FATF as a non-cooperative or high risk country or territory (however described); or

(b) that is subject to international sanctions.

3.5.7 Jurisdictions with high propensity for corruption

(1) A firm:

(a) must assess and document the jurisdictions that are more vulnerable to corruption; and

(b) must conduct enhanced CDD and enhanced ongoing monitoring for customers from high risk jurisdictions whose line of business is more vulnerable to corruption.

Example of line of business more vulnerable to corruption

arms sales

(2) If a firm's policy permits the acceptance of PEPs as customers, the firm 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—general

Note for Part 4.1

Principle 3 (see rule 1.2.3) requires a firm to know each of its customers to the extent appropriate for the customer's risk profile.

4.1.1 Know your customer principle—general

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

Note Principle 6 (see rule 1.2.6) requires a firm 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 firm 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 terrorism financing.

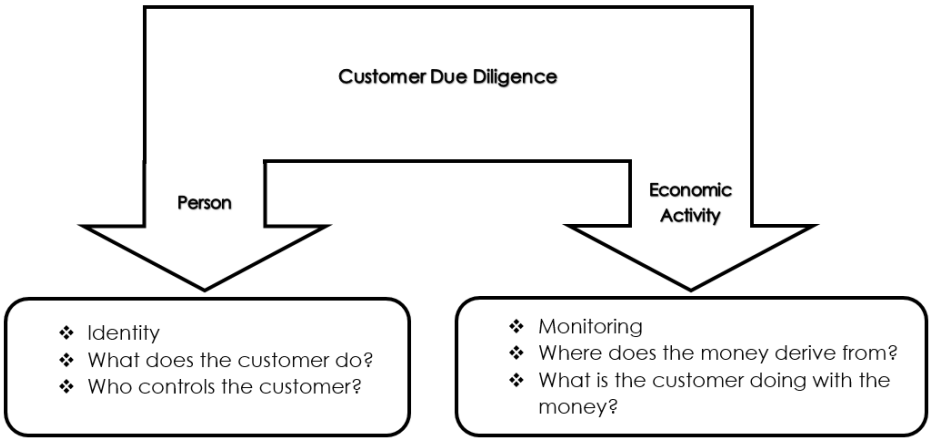
(3) If the firm does not obtain satisfactory evidence of identity for all the relevant parties, the firm must not establish the business relationship or carry out a transaction with or for them and must consider making a suspicious transaction report to the FIU.

(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 CDD to a customer should result in the firm 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 firm's knowledge of the customer and should drive the risk-profiling and therefore the intensity of the CDD and ongoing monitoring the firm must conduct for the customer.

Figure 4.1.3 Customer identification documents



Part 4.2 Know your customer—key terms

4.2.1 What is *customer due diligence*?

(1) ***Customer due diligence*** (or ***CDD***), in relation to a customer of a firm, is 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 (in particular whether the customer is acting as a trustee);

(d) obtaining information about the sources of the customer's wealth and funds;

(e) obtaining information about the purpose and intended nature of the business relationship.

Note For paragraphs (d) and (e), see generally Part 4.6 (Customer identification documentation). For the extent and detail of the information to be obtained, see rule 4.6.3 (Risks associated with the economic activity—general), rule 4.6.4 (2) (Risks associated with the economic activity—source of wealth and funds) and rule 4.6.5 (2) (Risks associated with the economic activity—purpose and intended nature of business relationship).

(2) If the customer is acting on behalf of another person (***A***), CDD also includes:

(a) verifying that the customer is authorised to act on behalf of A;

(b) identifying A; and

(c) verifying A's identity using reliable, independent source documents, data or information.

(3) If the customer is a legal person or legal arrangement, CDD also includes:

(a) verifying that any person (***B***) purporting to act on behalf of the customer is authorised to act on behalf of the customer;

(b) identifying B;

(c) verifying B's identity using reliable, independent source documents, data or information;

(d) verifying the legal status of the customer;

(e) taking reasonable measures, on a risk-sensitive basis:

(i) to understand the customer's ownership and control structure; and

(ii) to establish the individuals who ultimately own or control the customer, including the individuals who exercise ultimate effective control over the customer; and

(f) establishing whether B is a beneficial owner.

(4) If the customer is a legal person or legal arrangement, and a person purporting to act on behalf of the customer is not a beneficial owner of the customer, CDD also includes:

(a) identifying the beneficial owner; and

(b) verifying the beneficial owner's identity using reliable, independent source documents, data or information.

(5) For subrule (3) (e) (ii), examples of the measures required include:

(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

Note See rule 4.6.8 (Customer identification documentation—corporations).

(b) if the customer is a legal arrangement—identifying the parties to the arrangement, including the person exercising effective control over the arrangement.

Note See rule 4.3.9 (Extent of CDD—legal persons and arrangements) and rule 4.6.11 (Customer identification documentation—legal arrangements).

4.2.2 What is *ongoing monitoring*?

Ongoing monitoring, in relation to a customer of a firm, consists of:

(a) scrutinising transactions conducted under the business relationship with the customer to ensure that the transactions are consistent with the firm's knowledge of the customer, the customer's business and risk profile, and, where necessary, the source of the customer's wealth and funds; and

(b) reviewing the firm's records of the customer to ensure that documents, data and information collected during CDD 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 firm, is a person seeking to form a business relationship, or carry out a one-off transaction, with the firm.

Examples of applicants for business

1 A person dealing with a firm on his or her own behalf is an applicant for business for the firm.

2 If a person (***A***) is acting as agent for a principal (for example, as an authorised manager of a discretionary investment service for clients) in dealing with a firm and A deals with the firm in his or her own name on behalf of a client of the principal, A (and not the client) is an applicant for business for the firm.

3 If a person (***B***) provides funds to a firm and wants an investment purchased with the funds to be registered in the name of another person (for example, a grandchild), B (and not the other person) is an applicant for business for the firm.

4 If an intermediary introduces a client to a firm 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 firm.

5 If a person seeks advice from, or access to an execution-only dealing service with, a firm in his or her own name and on his or her own behalf, the person is an applicant for business for the firm.

6 If a professional agent introduces a third party to a firm 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 firm.

7 If an individual claiming to represent a company, partnership or other legal person applies to a firm 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 firm.

8 If a company manager or company formation agent (***C***) introduces a client company to a firm, the client company (and not C) is an applicant for business for the firm.

9 If a trust is introduced to a firm, the settlor of the trust is an applicant for business for the firm.

4.2.4 What is a *business relationship*?

A ***business relationship*** means a regular relationship between a customer and a firm in connection with a service that the customer receives from the firm.

Note A relationship that, when contact is established, is reasonably expected by a firm to be merely transitory does not constitute a business relationship.

4.2.5 What is a *one-off transaction*?

A ***one-off transaction***, in relation to a firm, is a transaction carried out by the firm for a customer otherwise than in the course of a business relationship with the customer.

Examples

1 a one-off foreign currency transaction

2 an isolated instruction to purchase shares

3 a one-off wire transfer

Part 4.3 Customer due diligence and ongoing monitoring

4.3.1 Firm to assess applicants for business

A firm must decide, from the outset of its dealings with an applicant for business, whether the person is seeking to establish a business relationship with the firm or is an occasional customer seeking to carry out a one-off transaction.

4.3.2 When CDD required—basic requirement

(1) A firm must conduct CDD for a customer when:

(a) it establishes a business relationship with the customer;

(b) it conducts a one-off transaction for the customer with a value (or, for transactions that are or appear (whether at the time or later) to be linked, with a total value) of at least QR 50,000;

Note A firm must have systems and controls to identify one-off transactions that are linked to the same person (see rule 4.3.15 (1)).

(c) it suspects the customer of money laundering or terrorism financing; or

(d) 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.

Note CDD must also be conducted under rule 3.3.8 (Powers of attorney) and rule 3.3.10 (Wire transfers).

(2) This rule is subject to:

- rule 3.4.9 (Introducers)
- rule 3.4.10 (Group introductions)
- rule 3.4.11 (Intermediaries)
- rule 4.3.4 (When CDD may not be required—acquired businesses)
- rule 5.2.2 (2) (Firm must ensure no tipping-off occurs).

4.3.3 Firm unable to complete CDD for customer

(1) This rule applies if a firm cannot complete CDD for a customer.

Examples

1 the firm 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 firm:

(a) must immediately terminate any relationship with the customer;

(b) must not establish a relationship with, or carry out a transaction with or for, the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

4.3.4 When CDD may not be required—acquired businesses

(1) This rule applies if a firm acquires the business of another firm, either in whole or as a product portfolio (for example, the mortgage book).

(2) The firm is not required to conduct CDD 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 with the AML/CFT Law and these rules or the law of another jurisdiction that has an effective AML/CFT regime.

(3) 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 firm's senior management must prepare or approve, and document, an action plan that ensures that the firm

conducts CDD for all of the customers acquired with the business as soon as possible.

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

4.3.5 Timing of CDD—establishment of business relationship

(1) A firm must conduct CDD for a customer before it establishes a business relationship with the customer.

(2) However, the CDD 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 terrorism financing and these risks are effectively managed;

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) the CDD is completed as soon as practicable after contact is first established with the customer; and

(d) the CDD is conducted in accordance with the policies, procedures, systems and controls on the use of the business relationship even before the customer's identity is verified.

Note Under rule 2.1.3 (2) (g), a firm must have policies, procedures, systems and controls that set out the conditions that must be satisfied to permit a

customer to use the business relationship even before the customer's identity (or the identity of the beneficial owner of the customer) is verified.

(3) Also, CDD may be conducted for the beneficiary under a life insurance contract after the business relationship has been established if they are conducted at or before:

(a) the time of payout; or

(b) the time the beneficiary exercises a right vested under the contract.

(4) In addition, CDD for a bank account holder may be conducted after the account has been opened if there are adequate safeguards in place to ensure that:

(a) the account is not closed before they are completed; and

(b) no payments are made from the account, and no other transactions are carried out by or on behalf of the account holder, before they are completed.

(5) If the firm establishes a business relationship with the customer under subrule (2), (3) or (4) but cannot complete CDD for the customer, the firm:

(a) must immediately terminate any relationship with the customer;

(b) must not carry out a transaction with or for the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

(6) Subrule (5) (c) does not apply if the firm:

(a) is a lawyer, notary, other legal professional, accountant, auditor, tax consultant or insolvency practitioner; and

(b) is:

(i) providing legal advice to the client; or

(ii) defending or representing the client in, or concerning, legal proceedings, including providing advice on instituting or avoiding legal proceedings.

Note For lawyers, notaries, other legal professionals and accountants, see rule 5.2.4 on giving advice and tipping-off.

4.3.6 Timing of CDD—one-off transactions

(1) A firm must conduct CDD for a customer before it conducts a one-off transaction for the customer.

(2) If the firm cannot complete CDD for the customer, the firm:

(a) must immediately terminate any relationship with the customer;

(b) must not carry out the transaction with or for the customer; and

(c) must consider whether it should make a suspicious transaction report to the FIU.

(3) Subrule (2) (c) does not apply if the firm:

(a) is a lawyer, notary, other legal professional, accountant, auditor, tax consultant or insolvency practitioner; and

(b) is:

(i) providing legal advice to the client; or

(ii) defending or representing the client in, or concerning, legal proceedings, including providing advice on instituting or avoiding legal proceedings.

Note For lawyers, notaries, other legal professionals and accountants, see rule 5.2.4 on giving advice and tipping-off.

4.3.7 When CDD required—additional requirement for existing customers

(1) A firm must also conduct CDD for existing customers at other appropriate times on a risk-sensitive basis.

(2) Without limiting subrule (1), a firm must conduct CDD for an existing customer if there is a material change in the nature or ownership of the customer.

(3) Without limiting subrule (2), a firm must decide whether to conduct CDD for a customer if:

(a) the firm's customer documentation standards change substantially;

(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;

(c) a significant transaction with or for the customer is about to take place; or

(d) the firm becomes aware that it lacks sufficient information about the customer.

Note See rule 3.3.4 (Products with fictitious or false names or no names).

4.3.8 Extent of CDD—general requirement

(1) A firm must:

(a) decide, consistently with these rules, the extent of CDD for a customer on a risk-sensitive basis depending on, among other factors, the customer risk, the product risk, the interface risk and the jurisdiction risk; and

(b) be able to demonstrate to the Regulator that the extent of the is appropriate in view of the risks of money laundering and terrorism financing.

(2) Without limiting subrule (1), a firm must conduct enhanced CDD for a customer if, for example, the business relationship of the customer is assessed as carrying a higher money laundering or terrorism financing risk.

4.3.9 Extent of CDD—legal persons and arrangements

(1) This rule applies if a firm is required to conduct CDD for a legal person (other than a corporation) or a legal arrangement.

(2) If the firm identifies the class of persons in whose main interest the legal person or legal arrangement is established or operated as a

beneficial owner, the firm is not required to identify all the members of the class.

(3) However, if the CDD is required to be conducted for a legal arrangement and the beneficiaries and their contributions have already been decided, the firm must identify each beneficiary who is to receive at least 20% of the funds of the arrangement (by value).

Note See also rule 4.6.11 (Customer identification documentation—legal arrangements).

4.3.10 CDD for beneficiaries of life insurance policies—general

(1) A financial institution must conduct the either of the following measures on each beneficiary of a life insurance policy or other investment-related insurance policy as soon as the beneficiary is identified or designated:

(a) for an identified beneficiary (whether a natural or legal person or a legal arrangement)—recording the beneficiary's name;

(b) for a beneficiary designated by characteristics or class (for example, spouse or children at the time that the insured event occurs) or by some other means (for example, under a will))—obtaining enough information about the beneficiary to satisfy the financial institution that it will be able to establish the identity of the beneficiary at the time of the payout.

(2) The institution must verify the identity of each beneficiary at the time of the payout.

(3) In deciding whether enhanced CDD is applicable, a financial institution must consider the beneficiary of a life insurance policy as a risk factor. If the financial institution decides that a beneficiary who is a legal person or a legal arrangement presents a higher risk, the enhanced CDD should include reasonable measures to identify, and verify the identity of, the beneficiary's beneficial owner at the time of payout.

(4) If a financial institution is unable to comply with this rule, it must consider making a suspicious transaction report to the FIU.

4.3.11 CDD for PEPs as beneficiaries of life insurance policies

(1) Before making a payout from a life insurance policy, a financial institution must take reasonable measures to determine whether the beneficiary, or the beneficial owner of the beneficiary, of the policy is a PEP.

(2) If the beneficiary or its beneficial owner is a PEP and the PEP presents a higher risk, the firm:

(a) must inform its senior management;

(b) must conduct enhanced CDD of its business relationship with the policyholder; and

(c) must make a suspicious transaction report to the FIU.

4.3.12 CDD for purchaser and vendor of real estate

A DNFBP acting as real estate agent in relation to a transaction for the sale of real property must conduct CDD on both the buyer and seller of the property (even if the DNFBP acts for only 1 of the parties to the transaction).

4.3.13 Ongoing monitoring required

(1) A firm must conduct ongoing monitoring for each customer.

Note See rule 4.2.2 (What is *ongoing monitoring*?).

(2) Without limiting subrule (1), the firm 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.

Examples

1 significant transactions relative to the business relationship with the customer

2 transactions that exceed set limits

3 very high turnover inconsistent with the size of the balance

4 transactions that fall outside the regular pattern of an account's activity

(3) The firm must examine as far as possible the background and purpose of a transaction mentioned in subrule (2) and must make a record of its findings.

(4) A record made for subrule (2) must be kept for at least 10 years after the day it is made.

(5) This rule is subject to rule 5.2.2 (2) (Firm must ensure no tipping-off occurs).

(6) In this rule:

transaction, in relation to insurance business, means the insurance product itself, the premium payment and the benefits.

4.3.14 Procedures for ongoing monitoring

(1) A firm must have policies, procedures, systems and controls for ongoing monitoring for its customers.

(2) The systems and controls:

(a) must flag transactions for further examination; and

(b) must provide for:

(i) the prompt further examination of these transactions by a senior independent person;

(ii) appropriate action to be taken on the findings of the further examination; and

(iii) if there is knowledge or suspicion of money laundering or terrorism financing raised by the findings—a report to be made promptly to the firm'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;

(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.

4.3.15 Linked one-off transactions

(1) A firm must have systems and controls to identify one-off transactions that are linked to the same person.

Note See rule 4.2.5 (What is a *one-off transaction*?).

(2) If a firm knows or suspects, or has reasonable grounds to know or suspect, that a series of linked one-off transactions involves money laundering or terrorism financing, the firm must make a suspicious transaction report to the FIU.

Part 4.4 Enhanced CDD and ongoing monitoring

4.4.1 Enhanced CDD and ongoing monitoring—general

A firm must, on a risk-sensitive basis, conduct enhanced CDD and enhanced ongoing monitoring:

(a) in cases where it is required to do so under the AML/CFT Law or these rules;

(b) if required by the Regulator or the NAMLTF Committee;

(c) in cases where FATF calls upon its members to require enhanced CDD and enhanced ongoing monitoring; and

(d) in any other case that by its nature can present a higher risk of money laundering or terrorism financing.

Note Enhanced CDD or enhanced ongoing monitoring is required under:

- rule 2.1.3 (2) (b) (Matters to be covered by policies etc)
- rule 3.2.4 (Persons associated with terrorist acts etc—enhanced CDD and ongoing monitoring)
- rule 3.2.5 (c) and (f) (Measures for PEPs)
- rule 3.3.5 (3) (a) (Correspondent banking relationships generally)
- rule 3.3.9 (3) (Bearer shares and share warrants to bearer)
- rule 3.3.12 (3) (a) (Correspondent securities relationships generally)
- rule 3.5.1 (2) examples (Risk assessment for jurisdiction risk)
- rule 3.5.5 (Jurisdictions with impaired international cooperation)
- rule 3.5.6 (Non-cooperative, high risk and sanctioned jurisdictions)
- rule 3.5.7 (1) (b) (Jurisdictions with high propensity for corruption)
- rule 4.3.8 (2) (Extent of CDD—general requirement)

4.4.2 Measures required for enhanced CDD or ongoing monitoring

A firm that is required to conduct enhanced CDD or enhanced ongoing monitoring must include the following measures, as appropriate to either or both requirements:

(a) obtain additional information about the customer (for example, profession, volume of assets and information available through public databases and open sources);

(b) update customer identification and beneficial owner identification;

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

(d) obtain additional information on the sources of the customer's wealth and funds;

(e) obtain information on the reasons for the expected transactions or the transactions that have been carried out;

(f) obtain senior management approval before establishing or continuing a business relationship;

(g) implement additional and continuous controls by identifying transactions and patterns of transactions that need additional scrutiny and review;

(h) make the first of any required payments to the customer through an account in a bank that 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.

4.4.3 Measures in addition to enhanced CDD and ongoing monitoring

In addition to the enhanced CDD and enhanced ongoing monitoring in this Part, a firm must conduct, on a risk-sensitive basis:

(a) countermeasures proportionate to the risks specified in circulars published by the NAMLTF Committee based on relevant findings of international organisations, governments and other bodies; and

(b) other measures determined by the NAMLTF Committee on its own initiative.

Part 4.5 Simplified CDD and ongoing monitoring

4.5.1 Simplified CDD—general

Except if there is a suspicion of money laundering or terrorism financing, a firm may conduct, for a customer, simplified CDD under rules 4.5.2 to 4.5.4 when:

(a) it establishes a business relationship with the customer; or

(b) it conducts a one-off transaction for the customer to which rule 4.3.2 (1) (b) (When CDD required—basic requirement) applies.

4.5.2 Customer with low level of risk

A firm may conduct simplified CDD for a customer who presents a low level of risk. The CDD must be commensurate to the level of risk and may include:

(a) despite rule 4.3.5, verifying the identity of the customer or beneficial owner after (rather than before) the business relationship has been established;

(b) despite rule 4.3.6, verifying the identity of the customer or beneficial owner after (rather than before) a one-off transaction with a value of at least QR 50,000;

(c) reducing the intensity, extent and frequency of updates of customer identification; and

(d) not collecting information, or not carrying out measures, to determine the purpose and intended nature of the business relationship, and instead inferring that purpose and nature from the transactions carried out under that relationship.

4.5.3 Listed, regulated public companies

A firm may conduct simplified CDD 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.

4.5.4 Certain life insurance contracts

A firm may conduct simplified CDD for a customer in relation to a life insurance contract if:

(a) either:

(i) the annual premium is not more than QR 3,000; or

(ii) if there is a single premium—the premium is not more than QR 7,500;

(b) the contract is in writing;

(c) the beneficiary is not anonymous;

(d) the nature of the contract allows for the timely CDD if there is a suspicion of money laundering or terrorism financing; and

(e) the benefits of the contract or a related transaction cannot be realised for the benefit of third parties, except on death or survival to a predetermined advanced age, or similar events.

4.5.5 Simplified ongoing monitoring

This Part applies to ongoing monitoring in relation to a customer that presents a low level of risk. The ongoing measures must be commensurate to the level of risk and may include the reduction, based on a reasonable threshold determined by the firm, of the intensity, extent and frequency of:

(a) the firm's scrutiny of the customer's transactions; and

(b) the firm's review of its records of the customer.

Part 4.6 Customer identification documentation

Division 4.6.A Customer identification documentation—general

4.6.1 Elements of customer identification documentation

Customer identification documentation relates to 2 distinct elements, namely:

(a) the customer; and

(b) the nature of the customer's economic activity.

Note See rule 4.1.3 (Customer identification documents).

4.6.2 Records of customer identification documentation etc

(1) A firm must make and keep a record of all the customer identification documentation that it obtains in conducting CDD and ongoing monitoring for a customer.

(2) Without limiting subrule (1), a firm must make and keep a record of how and when each of the steps of the CDD for a customer were satisfactorily completed by the firm.

(3) This rule applies in relation to a customer irrespective of the nature and risk profile of the customer.

Division 4.6.B Customer identification documentation—the economic activity

4.6.3 Risks associated with the economic activity—general

(1) A firm 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 crime and the business relationship will be used to channel these funds; or

(b) proceeds of crime will be mixed with proceeds of legitimate economic activity to disguise their origin.

(2) A firm 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 firm substantially mitigates the customer risk.

(b) identify the purpose and intended nature of the business relationship.

Note By establishing this, the firm 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 firm can better work out whether money laundering or terrorism financing is taking place.

4.6.4 Risks associated with the economic activity—source of wealth and funds

(1) In conducting CDD for an applicant for business who is seeking to establish a business relationship, a firm must obtain, and document, information on the source of the applicant's wealth and funds.

Note Information obtained can assist the firm in establishing the money laundering and terrorism financing risks posed by both the customer risk

and the jurisdiction risk. In certain cases the product risk will also be affected by establishing the source of the wealth and funds.

(2) The firm must obtain, and document, the information to an appropriate level having regard to the applicant's risk profile and must document this information.

(3) If the applicant's risk profile is not low risk, the firm must verify the source of the applicant's wealth and funds using reliable, independent source documents, data or information, and must document this verification.

(4) Information documented under this rule forms part of the firm's customer identification documentation.

4.6.5 Risks associated with the economic activity—purpose and intended nature of business relationship

(1) In conducting CDD for an applicant for business who is seeking to establish a business relationship, a firm 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 firm:

(a) to readily identify differences between the actual transactions conducted under the relationship and the stated purpose and intended nature of the relationship;

(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 firm's customer identification documentation.

Division 4.6.C Customer identification documentation—particular applicants for business

4.6.6 Customer identification documentation—individuals

(1) This rule applies if an applicant for business for a firm is an individual.

(2) If the individual's risk profile is low risk, the firm may satisfy the customer identification 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;

Examples

1 a valid Qatari ID card

2 a valid passport

3 a valid driving licence with a photograph

(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 sources.

4.6.7 Customer identification documentation—multiple individual applicants

(1) This rule applies if 2 or more individuals are joint applicants for business for a firm.

(2) The identities of all of them must be verified in accordance with these rules.

4.6.8 Customer identification documentation—corporations

(1) This rule applies if an applicant for business for a firm is a corporation.

(2) If the corporation's risk profile is low risk, the firm may, subject to subrule (3), satisfy the customer identification requirements by:

(a) either:

(i) obtaining a copy of the certificate of incorporation or trade (or an 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);

(b) confirming the corporation's registered office business address;

(c) obtaining a copy of the corporation's latest available report and audited accounts; and

(d) obtaining a copy of the board resolution authorising:

(i) the establishing of the relationship with the firm; and

(ii) persons to act on its behalf in relation to the relationship, including by operating any accounts.

(3) If the corporation has a multi-layered ownership or control structure, the firm:

(a) must 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) must 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 firm must comply with subrule (3) and (4) in relation to B as well as C.

(5) The firm must conduct additional CDD if the corporation:

(a) is incorporated in a foreign jurisdiction; or

(b) has no direct business links to Qatar.

(6) If the corporation, or the corporation's parent entity, is listed in a stock exchange that has disclosure requirements that enable the customer's or owner's identity to be verified in a fully transparent way, the firm:

(a) need not identify, nor verify the identity of, the shareholders of the corporation or the shareholders of the parent entity; and

(b) may instead satisfy the customer identification requirements by obtaining information from a public register, the corporation or parent entity itself, or other reliable sources.

4.6.9 Customer identification documentation—unincorporated partnerships and associations

(1) This rule applies if an applicant for business for a firm is an unincorporated partnership, or an association that conducts business (the ***applicant***).

(2) If the firm does not know the applicant's partners or directors, the firm must verify the identity of all of the partners or directors using reliable, independent source documents, data or information.

(3) If the applicant is a partnership with a formal partnership agreement, the firm must obtain a mandate from the partnership authorising:

(a) the establishing of the relationship with the firm; and

(b) persons to act on behalf of the partnership in relation to the relationship, including by operating any accounts.

4.6.10 Customer identification documentation—charities

(1) This rule applies if an applicant for business for a firm is a charity.

(2) The firm must conduct CDD for the charity according to its legal form.

Examples of legal forms of charities

1 company limited by shares

2 trust

3 unincorporated association

4.6.11 Customer identification documentation—legal arrangements

(1) This rule applies if an applicant for business for a firm is a legal arrangement.

(2) In conducting a risk assessment for the legal arrangement, the firm must take into account the different money laundering and terrorism financing risks that are posed by arrangements of different sizes and areas of activity. This subrule does not limit the matters the firm may take into account.

Examples

Some legal arrangements have a limited purpose (for example, inheritance tax planning) or have a limited range of activities. Others have more extensive activities and connections including financial links with other jurisdictions.

(3) The firm must, as a minimum, obtain the following information about the legal arrangement:

(a) the arrangement's full name;

(b) the nature and purpose of the arrangement;

Examples of the nature of arrangements

discretionary, testamentary, bare

(c) the jurisdiction where the arrangement was established;

(d) the identities of the parties to the arrangement;

Examples of parties to a trust

settlor, trustee, protector and beneficiary

(e) the beneficial owner of the arrangement.

Note Under rule 1.3.5 (1) (c) and 1.3.5 (4), the ***beneficial owner*** of a legal arrangement is the individual who ultimately owns, or exercises effective control over, the arrangement and includes:

(a) if the beneficiaries and their distributions have already been decided—an individual who is to receive at least 20% of the funds of the arrangement; and

(b) if the beneficiaries or their distributions have not already been decided—the class of individuals 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 20% (by value) of the property of the arrangement.

(4) The firm must verify the identity of an applicant that is a legal arrangement using reliable, independent source documents, data or information that show:

(a) the name, nature and proof of existence of the arrangement; and

(b) the terms of the arrangement.

(5) The firm must verify that any person purporting to act on behalf of the legal arrangement is so authorised, and must identify and verify the identity of that person.

(6) The firm:

(a) must understand, and if necessary obtain information on, the purpose and intended nature of the business relationship; and

(b) must understand the nature of the business of the legal arrangement and its ownership and control structure.

4.6.12 Customer identification documentation—clubs and societies

(1) This rule applies if an applicant for business for a firm is a club or society (the ***applicant***).

(2) In conducting a risk assessment for the applicant, the firm must take into account the different money laundering and terrorism 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 firm may take into account.

(4) If the applicant's risk profile is low risk, the firm 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 firm must also verify the identities of the applicant's officers who have authority:

(a) to establish a relationship with the firm 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.

4.6.13 Customer identification documentation—governmental bodies

(1) This rule applies if an applicant for business for a firm is a multi-jurisdictional entity, a government department or a local authority (the ***applicant***).

(2) The firm must, as a minimum, obtain the following information about the applicant:

(a) the applicant's legal status;

(b) the applicant's ownership and control, as appropriate;

(c) the applicant's main address.

(3) The firm must also verify the identities of the persons who have authority:

(a) to establish a relationship with the firm 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.

4.6.14 Other requirements for customer identification of legal persons

(1) In addition to the customer identification documentation required for particular applicants under this Division, a firm must verify the identity of an applicant that is a legal person using reliable, independent source documents, data or information that show:

(a) the name, legal form and proof of existence of the legal person;

(b) the mandates, declarations, resolutions and other sources of power that regulate and bind the legal person;

(c) the names of the persons holding senior management positions in the legal person; and

(d) the address of the registered office of the legal person and, if different, its principal place of business.

(2) The firm must verify that any person purporting to act on behalf of the legal person is so authorised, and must identify and verify the identity of that person.

(3) The firm must:

(a) understand, and if necessary obtain information on, the purpose and intended nature of the business relationship; and

(b) understand the nature of the business of the legal person and its ownership and control structure.

(4) For subrule (3) (b), the firm must identify, and verify the identity of:

(a) the individual who is the beneficial owner of the legal person; or

(b) if no individual can be identified as the beneficial owner of the legal person (or if there is doubt that an individual is the beneficial owner)—the legal person's most senior manager.

Note Under rule 1.3.5 (1) (c) and 1.3.5 (3), the ***beneficial owner*** of a legal person is the individual who ultimately owns, or exercises effective control over, the person and includes, for a corporation:

(a) an individual who, directly or indirectly, owns or controls at least 20% 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.

Chapter 5 Reporting and tipping-off

Part 5.1 Reporting requirements

Note for Part 5.1

Principle 4 (see rule 1.2.4) requires a firm to have effective measures in place to ensure there is internal and external reporting whenever money laundering or terrorism financing is known or suspected.

Division 5.1.A Reporting requirements—general

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 firm to know its customers well enough under Chapter 4 (Know your customer).

Note 2 A firm's AML/CFT policies, procedures, systems and controls must provide for the identification and scrutiny of certain transactions (see rule 2.1.3 (2) (a)).

(2) A firm 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 or is for a one-off transaction;

(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 firm may consider.

Division 5.1.B Internal reporting

5.1.2 Internal reporting policies etc

(1) A firm must have clear and effective policies, procedures, systems and controls for the internal reporting of all known or suspected instances of money laundering or terrorism financing.

(2) The policies, procedures, systems and controls must enable the firm to comply with the AML/CFT Law and these rules in relation to the prompt making of internal suspicious transaction reports to the firm's MLRO.

5.1.3 Access to MLRO

A firm must ensure that all its officers and employees have direct access to the firm'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 firm (see rule 2.3.4 (a)).

5.1.4 Obligation of officer or employee to report to MLRO etc

(1) This rule applies to an officer or employee of a firm if, in the course of his or her office or employment, the officer or employee knows or suspects, or has reasonable grounds to know or suspect, that funds are:

(a) the proceeds of crime;

(b) related to terrorism 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 firm's MLRO.

(3) The officer or employee must make the report:

(a) irrespective of the amount of any transaction relating to the funds;

(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 firm in relation to the funds;

(ii) for an applicant for business—no business relationship has been, or will be, entered into by the firm with the applicant;

(iii) for a customer—the firm has terminated any relationship with the customer; and

(iv) any attempted money laundering or terrorism 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:

(a) may commit an offence against the AML/CFT Law; and

(b) may also be dealt with under the *Financial Services Regulations*, Part 9 (Disciplinary and enforcement powers).

5.1.5 Obligations of MLRO on receipt of internal report

(1) If the MLRO of a firm receives a suspicious transaction report (whether under this Division or otherwise), the MLRO must promptly:

(a) if the firm'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;

(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);

(c) consider the report in light of all other relevant information held by the firm about the applicant for business, customer or transaction to which the report relates;

(d) decide whether the transaction is suspicious; and

(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 firm to report to FIU etc) in relation to the making of a report on the firm's behalf.

Note Under rule 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.

Division 5.1.C External reporting

5.1.6 External reporting policies etc

(1) A firm must have clear and effective policies, procedures, systems and controls for reporting to the FIU all known or suspected instances of money laundering or terrorism financing.

(2) The policies, procedures, systems and controls must enable the firm:

(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.

5.1.7 Obligation of firm to report to FIU etc

(1) This rule applies to a firm if the firm knows or suspects, or has reasonable grounds to know or suspect, that funds are:

(a) the proceeds of crime;

(b) related to terrorism financing; or

(c) linked or related to, or are to be used for, terrorism, terrorist acts or by terrorist organisations.

(2) The firm must promptly make a suspicious transaction report to the FIU and must ensure that any proposed transaction mentioned in the report does not proceed without consulting with the FIU.

(3) The report must be made on the firm'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 (1) (a)) at the management level by the firm, or by a legal person in the same group, and who has sufficient seniority, knowledge, experience and authority to investigate and assess internal suspicious transaction reports.

Note Under rule 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 firm must make the report:

(a) whether or not an internal suspicious transaction report has been made under Division 5.1.B (Internal reporting) in relation to the funds;

(b) irrespective of the amount of any transaction relating to the funds;

(c) whether or not any transaction relating to the funds involves tax matters; and

(d) even though:

(i) no transaction has been, or will be, conducted by the firm in relation to the funds;

(ii) for an applicant for business—no business relationship has been, or will be, entered into by the firm with the applicant;

(iii) for a customer—the firm has terminated any relationship with the customer; and

(iv) any attempted money laundering or terrorism financing activity in relation to the funds has failed for any other reason.

(5) The report must be made in the form (if any) approved by the FIU, and in accordance with the unit's instructions. The report must include a statement about:

(a) the facts or circumstances on which the firm's knowledge or suspicion is based or the grounds for the firm's knowledge or suspicion; and

(b) if the firm 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 firm's knowledge or suspicion.

Note A firm that fails to make a report under this rule:

(a) may commit an offence against the AML/CFT Law; and

(b) may also be dealt with under the *Financial Services Regulations*, Part 9 (Disciplinary and enforcement powers).

(6) If a firm makes a report to the FIU under this rule about a proposed transaction, it must immediately tell the Regulator that it has made a report to the FIU under this rule.

5.1.8 Obligation not to destroy records relating to customer under investigation etc

(1) This rule applies if:

(a) a firm makes a suspicious transaction report to the FIU in relation to an applicant for business or a customer; or

(b) the firm knows that an applicant for business or customer is under investigation by a law enforcement agency in relation to money laundering or terrorism financing.

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

5.1.9 Firm may restrict or terminate business relationship

(1) This Division does not prevent a firm from restricting or terminating, for normal commercial reasons, its business relationship with a customer after the firm makes a suspicious transaction report about the customer to the FIU.

(2) The firm must ensure that restricting or terminating the business relationship does not inadvertently result in tipping-off the customer.

(3) If the firm restricts or terminates a business relationship with a customer, it must immediately tell the Regulator about the restriction or termination.

Division 5.1.D Reporting records

5.1.10 Reporting records to be made by MLRO etc

The MLRO of a firm must make and keep records:

(a) showing the details of each internal suspicious transaction report the MLRO receives;

(b) 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

(c) showing the details of each suspicious transaction report made to the FIU by the firm.

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 firm, is the unauthorised act of disclosing information that:

(a) 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:

(i) a suspicious transaction report; or

(ii) an investigation relating to money laundering or terrorism financing; and

(b) 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 terrorism financing.

5.2.2 Firm must ensure no tipping-off occurs

(1) A firm 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 within the firm or its group.

(2) If a firm believes, on reasonable grounds, that an applicant for business or a customer may be tipped off by conducting CDD or ongoing monitoring, the firm may make a suspicious transaction report to the FIU instead of conducting CDD or monitoring.

(3) If the firm acts under subrule (2), the MLRO must make and keep records to demonstrate the grounds for the belief that conducting CDD or ongoing monitoring would have tipped off an applicant for business or a customer.

5.2.3 Information relating to suspicious transaction reports to be safeguarded

(1) A firm 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 firm's senior management) without the consent of the firm'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.

5.2.4 When advice not considered to be tipping-off

(1) This rule applies to lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals.

(2) The act of a lawyer, notary, other legal professional or accountant in disclosing relevant information in the course of advising a person against engaging in an illegal act does not constitute tipping-off.

Chapter 6 Screening and training requirements

Part 6.1 Screening procedures

Note for Part 6.1

Principle 5 (see rule 1.2.5 (a)) requires a firm to have adequate screening procedures to ensure high standards when appointing or employing officers and employees.

6.1.1 Screening procedures—particular requirements

(1) In this rule:

higher-impact individual, in relation to a firm, means an individual who has a role in preventing money laundering or terrorism financing under the firm's AML/CFT programme.

Examples

1 a senior manager of the firm

2 the firm's MLRO or Deputy MLRO

3 an individual whose role in the firm includes conducting any other activity with or for a customer

(2) A firm's screening procedures for the appointment or employment of officers and employees must ensure that an individual is not appointed or employed unless:

(a) for a higher-impact individual—the firm is satisfied that the individual has the appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently; or

(b) for any other individual—the firm is satisfied about the individual's integrity.

(3) The procedures must, as a minimum, provide that, before appointing or employing a higher-impact individual, the firm must:

(a) obtain references about the individual;

(b) obtain information about the individual's employment history and qualifications;

(c) obtain details of any regulatory action taken in relation to the individual;

(d) obtain details of any criminal convictions of the individual; and

(e) take reasonable steps to confirm the accuracy and completeness of information that it has obtained about the individual.

Part 6.2 AML/CFT training programme

Note for Part 6.2

Principle 5 (see rule 1.2.5 (b)) also requires a firm 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 etc

(1) A firm 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 firm's officers and employees are aware, and have an appropriate understanding, of:

(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 terrorism financing, and the liability that they, and the firm, may incur for:

(i) involvement in money laundering or terrorism financing; and

(ii) failure to comply with the AML/CFT Law and these rules;

(c) how the firm is managing money laundering and terrorism financing risks, how risk management techniques are being applied by the firm, the roles of the MLRO and Deputy MLRO, and the importance of CDD and ongoing monitoring;

(d) money laundering and terrorism financing threats, techniques, methods and trends, the vulnerabilities of the products offered by the firm, and how to recognise suspicious transactions; and

(e) the firm's processes for making internal suspicious transaction reports, including how to make effective and efficient reports to the MLRO whenever money laundering or terrorism financing is known or suspected.

(3) The training must enable the firm'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 firm must consider:

(a) their differing needs, experience, skills and abilities;

(b) their differing functions, roles and levels in the firm;

(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 firm's business and the risk of money laundering and terrorism financing;

(f) the outcome of reviews of their training needs; and

(g) any analysis of suspicious transaction reports showing areas where training needs to be improved.

Examples

1 training for new employees needs to be different to the training for employees who have been with the firm for some time and are already aware of the firm'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 firm may consider.

6.2.2 Training must be maintained and reviewed

(1) A firm's AML/CFT training must include ongoing training to ensure that its officers and employees:

(a) maintain their AML/CFT knowledge, skills and abilities;

(b) are kept up to date with new AML/CFT developments, including the latest money laundering and terrorism financing techniques, methods and trends; and

(c) are trained on changes to the firm's AML/CFT policies, procedures, systems and controls.

(2) A firm must, at regular and appropriate intervals, carry out reviews of the AML/CFT training needs of its officers and employees and must ensure that the needs are met.

(3) The firm's senior management must promptly:

(a) consider the outcomes of each review; and

(b) if a review identifies deficiencies in the firm's AML/CFT training—prepare or approve an action plan to remedy the deficiencies.

Note It is the MLRO's responsibility to monitor the firm's AML/CFT training programme (see rule 2.3.4 (f)).

Chapter 7 Providing documentary evidence of compliance

Note for Chapter 7

Principle 6 (see rule 1.2.6) requires a firm 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 firm 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 the firm has complied with the AML/CFT Law and these rules.

(2) Without limiting rule (1) (b), the firm must make the records necessary to demonstrate how:

(a) the key AML/CFT principles in Part 1.2 have been complied with;

(b) the firm's senior management has complied with responsibilities under the AML/CFT Law and these rules;

(c) the firm's risk-based approach has been designed and implemented;

(d) each of the firm's risks have been mitigated;

(e) CDD and ongoing reviews were conducted for each customer; and

(f) CDD and ongoing monitoring were enhanced where required by the AML/CFT Law or these rules.

Examples of records that must be kept

1 documents and data obtained while conducting CDD

2 account files

3 business correspondence

4 results of analysis of suspicious transaction reports

Note See also rule 5.1.10 for reporting records to be made by MLRO and rule 4.3.13 (4) for records on monitoring of complex, unusual or large transactions.

7.1.2 How long records must be kept

(1) All records made by a firm for the AML/CFT Law or these rules must be kept for at least 10 years after the day they are made.

(2) All records made by a firm in relation to a customer for the purposes of the AML/CFT Law or these rules must be kept for at least the longer of the following:

(a) if the firm has (or has had) a business relationship with the customer—10 years after the day the business relationship with the customer ends;

(b) if the firm has not had a business relationship with the customer or had a business relationship with the customer and carried out a one-off transaction for the customer after the relationship ended—10 years after the day the firm 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 firm last completed a transaction with or for the customer.

(4) This rule is subject to rule 5.1.8 (Obligation not to destroy records relating to customer under investigation etc).

7.1.3 Retrieval of records

(1) A firm 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 firm 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 10 years, a business relationship with any person; and

(b) the nature of the relationship.

Part 7.2 Particular record-keeping obligations

7.2.1 Records for customers and transactions

(1) A firm 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;

(b) enable an assessment to be made of the firm's compliance with:

(i) the AML/CFT Law and these rules; and

(ii) its AML/CFT policies, procedures, systems and controls;

(c) enable any transaction effected by or through the firm to be reconstructed;

(d) enable the firm 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;

(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.

7.2.2 Training records

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

(a) the dates the training was provided;

(b) the nature of the training; and

(c) the names of the individuals to whom the training was provided.

Glossary

(see rule 1.1.5)

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.

activity includes operation.

AML means anti-money laundering.

AML/CFT Law means Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and includes any Regulations made under it.

another jurisdiction means a jurisdiction other than this jurisdiction.

applicant for business has the meaning given by rule 4.2.3.

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.

authorised firm means a person that has an authorisation granted under the *Financial Services Regulations*, Part 5.

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.

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.

CDD means customer due diligence.

CFT means combating the financing of terrorism.

correspondent banking has the meaning given by rule 1.3.7.

correspondent securities relationship has the meaning given by rule 1.3.9.

customer has the meaning given by rule 1.3.4.

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

Deputy MLRO, in relation to a firm, means the firm's deputy money laundering reporting officer.

designated non-financial business or profession (or ***DNFBP***) has the meaning given by rule 1.3.3.

director, of a firm, means a person appointed to direct the firm's affairs, and includes:

(a) a person named as director; and

(b) any other person in accordance with whose instructions the firm is accustomed to act.

DNFBP means a designated non-financial business or profession.

document means a record of information in any form (including electronic form), and includes, for example:

(a) anything in writing or on which there is writing;

(b) anything on which there are figures, marks, numbers, perforations, symbols or anything else having a meaning for individuals qualified to interpret them;

(c) a drawing, map, photograph or plan; and

(d) any other item or matter (in whatever form) that is, or could reasonably be considered to be, a record of information.

employee, in relation to a person (***A***), means an individual:

(a) who is employed or appointed by A, whether under a contract of service or services or otherwise; or

(b) whose services are, under an arrangement between A and a third party, placed at the disposal and under the control of A.

entity means any kind of entity, and includes, for example, any person.

exercise a function means exercise or perform the function.

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

firm has the meaning given by rule 1.3.1.

financial institution has the meaning given by rule 1.3.2.

FIU means the Financial Intelligence Unit established under the AML/CFT Law.

foreign jurisdiction means a jurisdiction other than Qatar (which includes the Qatar Financial Centre).

full originator information means:

(a) the originator's name;

(b) the originator's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the originator);

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

full recipient information means the recipient's name and the recipient's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the recipient).

function means any function, authority, duty or power.

funds means assets or properties of every kind (whether physical or non-physical, tangible or intangible or movable or immovable, however acquired, and of any value), including:

(a) financial assets and all related rights;

(b) economic resources such as oil and other natural resources, and all related rights;

(c) legal documents or instruments in any form, including electronic or digital copies, evidencing title to, or share in, such assets or resources;

(d) any interest, dividends or other income on such assets or resources; and

(e) any value accruing from, or generated by, such assets or resources, which could be used to obtain funds, goods or services.

governing body, of a firm, means its board of directors, committee of management or other governing body (whatever it is called).

group, in relation to a firm, means 2 or more entities consisting of:

(a) a parent company or other legal person exercising control, and coordinating functions, over the rest of the group for the application of group supervision; and

(b) 1 or more branches or subsidiaries that are subject to AML/CFT policies, procedures systems and controls at group level.

instrument means an instrument of any kind, and includes, for example, any writing or other document.

insurance business has the meaning given by the *Insurance Business Rules 2006*.

jurisdiction means any kind of legal jurisdiction, and includes, for example:

(a) Qatar;

(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 Centre 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.

Examples

1 a company

2 any other corporation

3 a partnership, whether or not incorporated

4 an association or other undertaking, whether or not incorporated

5 a jurisdiction, its government or any of its organs, agencies or instrumentalities

MLRO, in relation to a firm, means the firm's money laundering reporting officer.

money laundering has the same meaning as in the AML/CFT Law, Chapter 2, Article (2).

NAMLTF Committee means the National Anti-Money Laundering and Terrorism Financing Committee established under the AML/CFT Law.

National Risk Assessment means the series of activities prepared and supervised by the NAMLTF Committee to identify and analyse the threats faced by Qatar and its financial system from money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.

non-profit organisation means a legal person, legal arrangement or other organisation that engages in raising or disbursing funds for:

(a) charitable, religious, cultural, educational, social, fraternal or similar purposes; or

(b) carrying out other types of charitable works for public benefit.

office includes position.

one-off transaction has the meaning given by rule 4.2.5.

ongoing monitoring has the meaning given by rule 4.2.2.

outsourcing, in relation to a firm, is any form of arrangement that involves the firm 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 firm, 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.

PEP means a politically exposed person.

person means:

(a) an individual (including an individual occupying an office from time to time); or

(b) a legal person.

politically exposed person (or ***PEP***) has the meaning given by rule 1.3.6.

proceeds of crime means funds derived or obtained, directly or indirectly, from a predicate offence (within the meaning given by the AML/CFT Law, Chapter 1), including any income, interest, revenue

or other product from such funds, whether or not the funds have been converted or transferred, in whole or in part, into other properties or investment yields.

product includes the provision of a service.

QFC bank means an authorised firm that is:

(a) a deposit-taker, within the meaning of the *Banking Business Prudential Rules 2014*; or

(b) an Islamic bank or Islamic investment dealer, within the respective meanings of the *Islamic Banking Business Prudential Rules 2015*.

QFC captive insurer has the meaning given by the *Captive Insurance Business Rules 2011*.

QFC insurer means an authorised firm that has an authorisation to conduct insurance business.

senior management, of a firm, means the firm's senior managers, jointly and separately.

senior manager, of a firm, means an individual employed by the firm, or by a member of the firm's group, who has responsibility either alone or with others for management and supervision of 1 or more elements of the firm's business or activities that are conducted in, from or to this jurisdiction.

settlor, in relation to a trust, means the person who created the trust.

shell bank has the meaning given by rule 1.3.8.

subsidiary—a legal person (***A***) is a ***subsidiary*** of another legal person (***B***) if B is a parent entity of A.

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

targeted financial sanction means asset freezing or any prohibition to prevent funds from being made available, directly or indirectly, for

the benefit of persons or entities listed in accordance with the Law No. (27) of 2019 on Combating Terrorism.

Note Under the Law on Combating Terrorism, the National Counter Terrorism Committee is responsible for implementing the requirements relating to targeted financial sanctions. For how to implement targeted financial sanctions, see guidelines under that Law.

terrorist means an individual who:

(a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and wilfully;

(b) participates as an accomplice in a terrorist act;

(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.

terrorism financing has the same meaning as in the AML/CFT Law, Chapter 2, Article (3).

terrorist act has the same meaning as in the AML/CFT Law, Chapter 1.

terrorist organisation means a group of terrorists.

the Regulator means the Qatar Financial Centre Regulatory Authority.

the State means the State of Qatar.

this jurisdiction means the Qatar Financial Centre.

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;

(b) the provision of any service; and

(c) the conducting of any other business or activity.

writing means any form of writing, and includes, for example, any way of representing or reproducing words, numbers, symbols or anything else in legible form (for example, by printing or photocopying).

Endnotes

1 Abbreviation key

a	=	after	ins	=	inserted/added
am	=	amended	om	=	omitted/repealed
amdt	=	amendment	orig	=	original
app	=	appendix	par	=	paragraph/subparagraph
art	=	article	prev	=	previously
att	=	attachment	pt	=	part
b	=	before	r	=	rule/subrule
ch	=	chapter	renum	=	renumbered
def	=	definition	reloc	=	relocated
div	=	division	s	=	section
g	=	guidance	sch	=	schedule
glos	=	glossary	sdiv	=	subdivision
hdg	=	heading	sub	=	substituted

2 Rules history

Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019
made by

Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019 (QFCRA Rules 2019-8)
Made 29 December 2019
Commenced 1 February 2020
Version No. 1

3 Amendment history