QFMA's Board Decision

No. (1) Of 2020

Concerning the Issuance of

Anti-Money Laundering and Combating Terrorist Financing Rules

The Board of Directors,

Having considered Law No. (8) Of 2012 of Qatar Financial Markets Authority; as amended by Decree-Law No. (22) Of 2018;

Law No. (20) of 2019 on Anti-Money Laundering and Combating Terrorist Financing and Council of Ministers Decision No. (41) of 2019 on the Promulgating of its Implementing Regulations issued by Law No. (20) of 2019;

QFMA's Board Decision No. (2) of 2010 concerning the Issuance of Anti-Money Laundering and Combating Terrorism Financing Rules issued on 31/5/2010;

QFMA's Board approval at its 6th meeting of 2019 on 16th of December 2019;

And proposal of the QFMA's Chief Executive Officer;

We have decided the following:

Article (1)

Anti-Money Laundering and Combating Terrorist Financing Rules annexed to this decision shall come into force and effect.

Article (2)

Decision No. (2) of 2010 shall hereby be repealed.

Article (3)

All competent authorities, each within its jurisdiction, shall implement this decision. The decision shall be effective from the date of issuance and shall be published in the Official Gazette.

Mohammed Bin Hamad Bin Qassim Al-Thani

Chairman of the Board of Directors

Issued on 07/05/1440 H

Corresponding to: 02/01/2020

This is a translation of the Official Arabic version. In case of any discrepancies, the Arabic version shall prevail.

Anti-Money Laundering and Combating Terrorism Financing Rules

made under Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its Implementing Regulations issued by Council of Ministers' decision No. (41) of 2019 on Combating Money Laundering and Terrorism Financing.

Amended by QFMA's Board Decision No. (2) Of 2023

Contents

Page

Chapter 1 General provisions

Part 1.1 Introductory

1.1.1 Name of rules

These rules are the *Anti-Money Laundering and Combating Terrorism Financing Rules*.

1.1.2 General application of these rules

(1) These rules apply to licensed parties that conduct business or activities in State of Qatar in accordance with the QFMA Law.

(2) A reference in these rules to a ***licensed party*** is a reference to such a party that conducts, and so far as it conducts, business or activities in State of Qatar, subject to the QFMA Law.

(3) In this rule:

QFMA Law means the Qatar Financial Markets Authority Law (Law No. (8) of 2012), and includes regulations issued by the QFMA.

(4) In the case of any violation of the provisions of these rules, the QFMA may take any of the actions and sanctions mentioned in the AML/CFT Law and in the QFMA Law and other relevant legal ligislations.

(5) The provisions of the AML/CFT Law and its impleminting regulations shall apply to whatever is not specifically provided for in these rules.

1.1.3 Annex of definitions

The Annex of definitions at the end of these rules is part of these rules.

1.1.4 Notes and examples

(1) A note in or to these rules is explanatory and is not part of the rules.

(2) An example in these rules:

(a) is not exhaustive; and

(b) may extend, but does not limit, the meaning of the rules or the particular part of the rules to which it relates.

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

1.2.3 Principle 3—know your customer

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

1.2.4 Principle 4—effective reporting

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

1.2.5 Principle 5—high standard screening and appropriate training

A licensed party:

(1) must have adequate screening procedures to ensure high standards when appointing or employing officers and employees; and

(2) must have an appropriate ongoing AML/CFT training programme for its officers and employees.

1.2.6 Principle 6—evidence of compliance

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

Part 1.3 Key terms

1.3.1 What is the *Regulator*?

The Regulator is the Qatar Financial Markets Authority.

1.3.2 What is a *licensed party*?

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

1.3.3 Who is a *customer*?

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

(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 that the party (or a member of the party's group) offers in the normal course of its business; and

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

1.3.4 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);

(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 financial institution'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.

1.3.5 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

a Heads of State or of government

b senior politicians

c senior government, judicial or military officials

d members of Parliament

e important political party officials

f senior executives of state owned companies

g members of senior management (directors, deputy directors and members of the board or equivalent functions) in international organisations.

(2) 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.

1.3.6 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.

Note ***Jurisdiction*** is defined in the Annex of definitions.

1.3.7 What is a *correspondent securities relationship*?

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

Examples of services:

the buying, selling, lending or otherwise holding of securities

Examples of financial institutions:

Financial services, financial markets, custodians and central depositories of securities (however described)

Chapter 2 General AML and CFT responsibilities

Part 2.1 The licensed party

2.1.1 Licensed parties to develop AML/CFT programme

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

(2) The type and extent of the measures adopted by the party 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 the following:

(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;

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

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

(e) appropriate compliance management arrangements;

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

(4) The review and testing of the party's compliance with its AML/CFT policies, procedures, systems and controls must be adequately resourced and must be conducted at least once a year by the party's external auditor.

Note Testing would include, for example, sample testing the licensed party's AML/CFT programme, screening of employees, record making and retention and ongoing monitoring for customers.

(5) The party must make and keep a record of the results of its review and testing under subrule (4).

(6) The external auditor – even if they are more - must submit to the Regulator one report attached to the annual financial report and audited accounts with responsibility for the validity of data contained therein. The external auditor's report must include statements as to the following:

(a) the appropriateness and effectiveness of the licensed party's AML/CFT programme, the related policies and procedures and the implemented internal control systems;

(b) the licensed party's ability in continuously engaging activities and implementation of its obligations under these rules;

(c) the licensed party's cooperation with the external auditor in providing access to the necessary information to complete its duties.

(7) The external auditor must inform the party's senior management, in writing, about any risk to which the party is exposed or is expected to be exposed, and about all of the violations immediately upon identification, and must send a copy of that notice to the Regulator.

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

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

2.1.3 Matters to be covered by policies etc

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

(a) 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 licensed party's officers and employees;

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

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

(a) must provide for the identification and scrutiny of:

(i) complex or unusual large transactions, and unusual patterns of transactions, that have no apparent economic or visible lawful purpose; and

(ii) any other transactions that the licensed party considers particularly likely by their nature to be related to money laundering or terrorism financing;

(b) must 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) must provide appropriate measures to reduce the risks associated with establishing business relationships with politically exposed persons;

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

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

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

(g) must 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;

(h) ensure that there are appropriate systems and measures to enable the licensed party to implement, immediately within 24 hours, 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

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

2.1.4 Assessment and review of policies etc

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

2.1.5 Compliance by officers, employees, agents etc

(1) A licensed party must ensure that its officers, employees, agents and contractors, wherever they are, comply with:

(a) the requirements of the AML/CFT Law and these rules; and

(b) its AML/CFT policies, procedures, systems and controls;

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

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

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

(b) must provide timely, unrestricted access by the licensed party's senior management and MLRO, and by the

Regulator and FIU, to documents and information of the licensed party, wherever they are held, that relate directly or indirectly to its customers or accounts or to transactions in, from or to State of Qatar;

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

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

(4) This rule does not prevent the licensed party from applying higher, consistent standards in its AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend over 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 licensed party, the licensed party must immediately tell the Regulator in writing about the matter.

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

(1) This rule applies to a licensed party if:

(a) it has a branch or associate in State of 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 licensed party must ensure that the branch or associate, and the officers, employees, agents and contractors of the branch or associate, wherever they are, comply with:

(a) the requirements of the AML/CFT Law and these rules; and

(b) the party's AML/CFT policies, procedures, systems and controls;

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

(3) Without limiting subrule (2), the licensed party'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 suspicious transaction reports for transactions in, from or to State of Qatar to the licensed party's MLRO; and

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

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 that jurisdiction.

(5) Despite subrule (2), if the AML/CFT requirements of State of Qatar 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 licensed party and its branches or associates, or the party and the other members of its group, from applying higher and more consistent standards in their AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend across the licensed party and its branches or the licensed party and the other members of its group.

(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 licensed party:

(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 the licensed party additional information and reports).

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

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

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

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

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

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

(3) The licensed party must, through a service level agreement 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 licensed party'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 licensed party'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 State of Qatar involving the licensed party (or the third party on its behalf) to the licensed party's MLRO; and

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

except so far as the law of another jurisdiction prevents 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 State of Qatar.

(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 licensed party about the matter; and

(b) the licensed party must immediately tell the Regulator in writing about the matter.

Part 2.2 Senior management

Note for Part 2.2

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

2.2.1 Overall senior management responsibility

The senior management of a licensed party is responsible for the effectiveness of the licensed party'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 licensed party must ensure the following:

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

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

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

(d) that independent review and testing of the licensed party'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 licensed party's money laundering and terrorism financing risks;

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

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

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

(2) is resident in State of Qatar;

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

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

(5) has timely, unrestricted access to all information of the party 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

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

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

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

(i) the development of new products;

(ii) the taking on of new customers; and

(iii) changes in the party's business profile;

(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 party.

Part 2.3 MLRO and deputy MLRO

Division 2.3.A Appointment of MLRO and deputy MLRO

2.3.1 Appointment—MLRO and deputy MLRO

(1) A licensed party must appoint an individual as its MLRO and another individual as its deputy MLRO.

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

2.3.2 Eligibility to be MLRO or deputy MLRO

The MLRO and deputy MLRO for a licensed party:

(1) must be employed at the management level by the licensed party; and

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

(a) to act independently; and

(b) to report directly to the licensed party's senior management.

Division 2.3.B Roles of MLRO and deputy MLRO

2.3.3 General responsibilities of MLRO

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

(1) oversighting the implementation of the licensed party's AML/CFT policies, procedures, systems and controls in relation to the jurisdiction, including the operation of the licensed party's risk-based approach;

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

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

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

(3) being the licensed party's key person in implementing the licensed party's AML/CFT strategies in relation to Qatar;

(4) supporting and coordinating senior management work on managing the licensed party's money laundering and terrorism financing risks in its business areas;

(5) helping to ensure that the licensed party's responsibility for preventing money laundering and terrorism financing is addressed centrally;

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

2.3.4 Particular responsibilities of MLRO

(1) The MLRO for a licensed party is responsible for the following:

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

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

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

(d) responding promptly to any request for information by the FIU, the Regulator and other State concerned authorities regarding the access AML and CFT information;

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

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

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

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

(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 licensed party's senior management. The licensed party must make and retain 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

The deputy MLRO for a licensed party acts as the licensed party's MLRO during absences of the MLRO and whenever there is a vacancy in the MLRO's position.

2.3.6 How MLRO must carry out role

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

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

(2) deciding whether to make, and making, suspicious transaction reports to the FIU.

Division 2.3.C Reporting by MLRO to senior management

2.3.7 MLRO reports

(1) The senior management of a licensed party must, on a regular basis, decide what reports should be given to it by the MLRO, and when the reports should be given to it, to enable the licensed party to discharge its responsibilities under the AML/CFT Law and these rules.

(2) However, a report that complies with rule 2.3.8 (Minimum annual report by MLRO) must be given to the senior management by the MLRO for each financial year of the licensed party and with sufficient promptness to enable the senior management to comply with rule 2.3.9 (2).

(3) To remove any doubt, subrule (2) does not limit the reports:

(a) that the senior management may require to be given to it; or

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

2.3.8 Minimum annual report by MLRO

(1) This rule sets out the minimum requirements that must be complied with in relation to the report that must be given to the senior management by the MLRO for each financial year of a licensed party (see rule 2.3.7 (2)).

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

(e) areas where the licensed party's AML/CFT policies, procedures, systems and controls should be improved, and proposals for making appropriate improvements;

(f) a summary of the AML/CFT training delivered to the licensed party's officers and employees;

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

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

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

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

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

2.3.9 Consideration of MLRO reports

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

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

(b) if the report identifies deficiencies in the licensed party's compliance with the AML/CFT Law or these rules—make, approve, or document an action plan to remedy the deficiencies in a timely way.

(2) For the report that must be given for each financial 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 licensed party's MLRO must give the Regulator a copy of the report and confirmation with the annual financial report and audited accounts.

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

3.1.1 Licensed parties must conduct risk assessment and decide risk mitigation

(1) A licensed party:

(a) must conduct, at least twice a year, at regular and appropriate intervals, an assessment (a ***business risk assessment***) and must determine the 5 most serious 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***); and

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

(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 licensed party 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 licensed party 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.

(4) The licensed party must submit a semi-annual report to the Regulator before the end of the following month containing the result of the licensed party risk assessment and its mitigation plan, in accordance with subrules (1), (2) and (3).

3.1.2 Approach to risk mitigation must be based on suitable methodology

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

(2) A licensed party 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;

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

(c) is designed to enable the licensed party:

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

3.1.3 Risk profiling a business relationship

(1) In developing the risk profile of a business relationship with a customer, a licensed party must consider at least the following 4 risk elements in relation to the relationship:

(a) customer risk;

(b) product risk;

(c) interface risk;

(d) jurisdiction risk.

(2) The licensed party must identify any other risk elements that are relevant to the business relationship, especially because of the size, complexity and nature of its business and any business of its customer.

(3) The licensed party must also consider the risk elements (if any) identified under subrule (2) in relation to the business relationship.

(4) Together the 4 risk elements mentioned in subrule (1), and any other risk elements identified under subrule (2), combine to produce the risk profile of the business relationship.

(5) This risk profile must be taken into account in deciding the intensity of the CDD and ongoing monitoring to be conducted for the customer.

Part 3.2 Customer risk

Note for Part 3.2

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

3.2.1 Risk assessment for customer risk

(1) A licensed party must assess and document the risks of money laundering, 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 politically exposed persons

(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 the due diligence measures and ongoing monitoring.

3.2.2 Policies etc for customer risk

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

3.2.3 Scoring business relationships - sources of wealth and funds

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

Example

The risk to the party from a salaried employee whose only transactions are those derived from electronic payments made by the employee's employer are going to be much lower than the risk to the party from an individual whose transactions are cash-based with no discernible source for this activity.

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

(1) This rule applies to a customer of a licensed party if the party knows or suspects that the customer is:

(a) an individual, charity, non-profit organisation or other entity that is associated with, or involved in, terrorist acts, terrorism financing or a terrorist organisation; or

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

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

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

3.2.5 Measures for politically exposed persons

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

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

(b) the licensed party must establish and maintain an appropriate risk management system to decide whether a potential or existing customer, or the beneficial owner of a potential or existing customer, is a PEP;

Examples of measures forming part of a risk management system

1 seeking relevant information from customers

2 referring to publicly available information

3 having access to, and referring to, commercial electronic databases of PEPs.

(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 with senior management approval;

(e) the licensed party 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 licensed party must take the measures required by subrule (1) in relation to a family member or close associate of a PEP.

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

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

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 licensed party must ensure that the risks posed by any beneficial owners, officers, shareholders, trustees, settlors, beneficiaries, managers and other relevant entities are reflected in the risk profile of the person or arrangement.

(3) In assessing the risks posed by a facility, a licensed party must ensure that the risks posed by any reduction in transparency, or any increased ability to conceal or obscure, are reflected in the facility's risk profile.

(4) Subrules (2) and (3) do not limit the matters to be reflected in the risk profile of a legal person, legal arrangement or facility.

3.2.7 Measures for persons in terrorists' list

(1) A licensed party 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.

(2) If the person is listed, the licensed party:

(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

Note for Part 3.3

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

2 Product includes the provision of a service

3.3.1 Risk assessment for product risk

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

(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 volume of transactions and operations that a customer has may affect the intensity of the due diligence measures and ongoing monitoring.

3.3.2 Policies etc for product risk

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

3.3.3 Scoring business relationships—types of products

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

3.3.4 Products with fictitious or false names or no names

(1) A licensed party must not permit any of its products to be used if the product:

(a) uses a fictitious or false name for a customer; or

(b) does not identify the customer's name.

(2) Subrule (1) does not prevent the licensed party from providing a level of privacy to the customer within the licensed party itself by not including the customer's name or details on the account name or customer file if:

(a) records of the customer's details are kept in a more secure environment in the licensed party itself; and

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

(3) Without limiting subrule (1), if the licensed party has numbered accounts, the licensed party 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 licensed party could properly identify the customer for an account in accordance with the AML/CFT Law and these rules and make the customer identification records available to the MLRO of the licensed party, the Regulator and the FIU.

3.3.5 Correspondent securities relationships generally

(1) Before a licensed party (the ***correspondent***) establishes a correspondent securities relationship with a financial institution in a foreign jurisdiction (the ***respondent***), the licensed party 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 licensed party, the respondent:

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

(ii) will conduct ongoing monitoring for the customers;

(iii) will be able to provide to the licensed party, on request, the documents, data or information obtained in conducting CDD and ongoing monitoring for the customers.

(2) Without limiting subrule (1) (b), in making a decision for that subrule, the licensed party 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 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 politically exposed person).

(3) If the licensed party establishes a correspondent securities relationship with the respondent, the licensed party 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 licensed party must not enter into, or continue, a correspondent securities relationship with a shell bank.

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

3.3.7 Payable through accounts

(1) The rule applies if:

(a) a licensed party (the corrspondant) has a correspondent securities relationship with a broker or dealer (foreign financial institution) (the ***respondent***) in a foreign jurisdiction; and

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

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

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

(b) conducts ongoing monitoring for the customer; and

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

(3) If:

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

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

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

3.3.8 Power of attorney

(1) This rule applies to a power of attorney if it authorises the holder to exercise control over assets of the grantor.

(2) Before dealing in a transaction involving the power of attorney, a licensed party must conduct 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 licensed party.

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 a cheque, promissory note, or money order that is either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title to it passes on 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 licensed party must have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to the use of bearer instruments.

(3) Before becoming involved in or associated with a transaction involving the conversion of a bearer instrument to registered form, or the surrender of coupons for a bearer instrument for payment of dividend, bonus or a capital event, a licensed party must conduct enhanced 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 licensed party.

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 licensed party are started or conducted.

Division 3.4.A Interface risks—general

3.4.1 Risk assessment for interface risk

(1) A licensed party must assess and document the risks of money laundering, 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 licensed party 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, or by telephone or fax, and other electronic means.

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

1 requiring third party certification of identification documents presented by or for non-face-to-face customers

2 requiring additional identification documents for non-face-to-face customers

3 developing independent contact with non-face-to-face customers

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

3.4.3 Scoring business relationships—interface risk

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

3.4.4 Electronic verification of identification documentation

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

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

3.4.5 Payment processing using on-line services

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

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

(2) the same risk-based methodology.

Division 3.4.B Reliance on others generally

3.4.6 Activities to which Division 3.4.B does not apply

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

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

(2) by an agent under a contractual arrangement between the licensed party and the agent; or

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

(4) under a correspondent securities relationship to which the licensed party is a party.

3.4.7 Reliance on certain third parties generally

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

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

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

3.4.8 Introducers

(1) This rule applies in relation to a customer introduced to a licensed party by a third party (the ***introducer***) if:

(a) the introducer's function in relation to the customer is merely to introduce the customer to the licensed party; and

(b) the licensed party is satisfied that the introducer:

(i) is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction;

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

(2) The licensed party 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 licensed party must not start a business relationship with the customer relying on subrule (2) unless:

(a) it has received from the introducer an introducer's certificate for the customer;

(b) it has received from the introducer all information about the customer obtained from the CDD conducted by the introducer for the customer that it would need if it had conducted the CDD itself; and

(c) it has, or can immediately obtain from the introducer on request, a copy of every document relating to the customer that it would need if it were conducting CDD itself for the customer.

3.4.9 Group introductions

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

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

(b) subject to subrule (2), the licensed party is satisfied that all of the following conditions have been met:

(i) the relevant financial institution is regulated and supervised (at least for AML and CFT purposes) by

the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction;

(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 State of Qatar or a foreign jurisdiction that has an effective AML/CFT regime;

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

(v) the licensed party has, or can immediately obtain from the relevant financial institution on request, a copy of every document relating to the customer that it would need if it were conducting CDD itself for the customer.

(2) The licensed party 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 the 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 licensed party 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.

3.4.10 Intermediaries

(1) This rule applies to a licensed party in relation to a customer of an intermediary, wherever located, if the customer is introduced to the licensed party by the intermediary.

Example of intermediary

a fund manager who has an active, ongoing business relationship with a customer in relation to the customer's financial affairs in the securities field and holds assets on the customer's behalf

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

(a) the intermediary is a financial institution;

(b) it is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction;

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

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

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

(f) the licensed party has, or can immediately obtain from the intermediary on request, a copy of every document relating to the customer that it would need if it were conducting CDD itself for the customer.

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

Division 3.4.C Third party certification—identification documents

3.4.11 Third party certification of identification documents

(1) A licensed party must not rely, for 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 licensed party must not rely on the certification of an identification document by a third party unless the third party is an individual approved under subrule (3).

(3) The senior management of the licensed party may approve an individual under this subrule if the licensed party's MLRO has certified that the MLRO is satisfied, on the basis of satisfactory documentary evidence, that the individual:

(a) adheres to appropriate ethical or professional standards;

(b) is readily contactable; and

(c) conducts his or her occupation or profession in State of 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 licensed party 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 licensed party 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.

3.5.3 Scoring business relationships—types of associated jurisdictions

A licensed party must include, in its methodology, a statement of the basis on which business relationships with customers will be

scored, having regard to the types of jurisdictions with which customers are (or may become) associated.

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

(1) This rule applies to a licensed party in making a decision about whether a jurisdiction has an effective AML/CFT regime.

(2) The licensed party must consider the following 3 factors in relation to the jurisdiction:

(a) legal framework;

(b) enforcement and supervision;

(c) international cooperation.

(3) In considering these 3 factors, the licensed party must have regard to the relevant findings about jurisdictions published by international organisations (for example, FATF), governments and other bodies.

3.5.5 Jurisdictions with impaired international cooperation

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

3.5.6 Non-cooperative, high risk and sanctioned jurisdictions

A licensed party 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:

(1) that is identified by FATF as a non-cooperative country or territory, or

(2) that is subject to international sanctions.

3.5.7 Jurisdictions with high propensity for corruption

(1) A licensed party must:

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

(b) conduct enhanced 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 licensed party's policy permits the acceptance of politically exposed persons as customers, the licensed party must take additional measures to mitigate the additional risk posed by PEPs from jurisdictions with a high propensity for corruption.

Chapter 4 Know your customer

Part 4.1 Know your customer—general

Note for Part 4.1

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

4.1.1 Know your customer principle—general

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

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

4.1.2 Overview of CDD requirements

Amended by QFMA's Board Decision No. (2) Of 2023

(1) As a general rule, a licensed party must not establish a business relationship with a customer unless:

(a) all the relevant parties (including any beneficial owner) have been identified and verified;

(b) the purpose and intended nature of the business expected to be conducted with the customer has been clarified; and

(c) the customer has a bank account at a bank in the State of Qatar or in the country of residence regulated and supervised by a regulatory authority, through which all payments for or from the customer for trading securities are made.

(2) The bank account referred to in paragraph (1) (c) must be identified in the licensed party's account opening form for the customer in accordance with rule 8.1.2.

(3) 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.

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

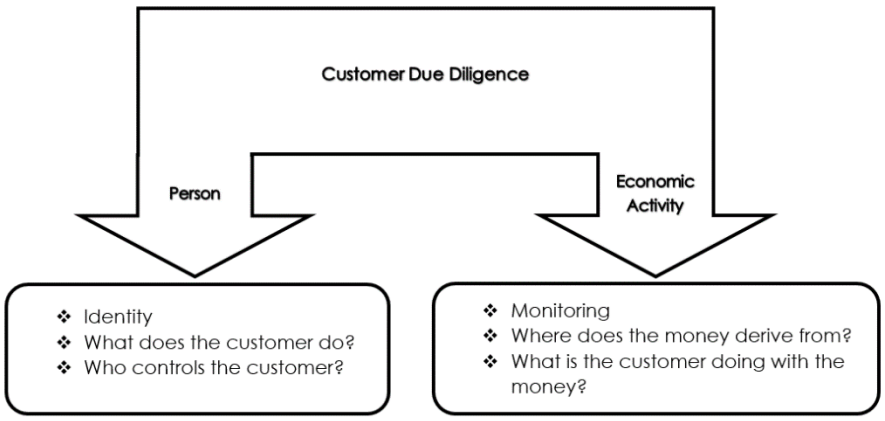
(5) This rule provides a simplified explanation of some of the customer due diligence requirements in this Chapter and is subject to the more detailed provisions of this Chapter.

4.1.3 Customer identification documents

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

ongoing monitoring that the licensed party must conduct for the customer.

Figure 4.1.4 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 licensed party, 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 4.4 (Customer identification documentation). For the extent and detail of the information to be obtained, see rule 4.4.3 (Risks associated with the economic activity—general), rule 4.4.4 (2) (Risks associated with the economic activity—source of wealth and funds) and rule 4.4.5 (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 4.4.8 (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 4.4.11 (Customer identification documentation—legal arrangements).

4.2.2 What is *ongoing monitoring*?

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

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

(2) reviewing the licensed party's records of the customer to ensure that documents, data and information collected using 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 licensed party, is a person seeking to form a business relationship with the licensed party.

Examples of applicants for business

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

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 licensed party and A deals with the licensed party 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 licensed party.

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

4 If an intermediary introduces a client to a licensed party as a potential investor and gives the client's name as the investor, the client (and not the intermediary) is an applicant for business for the licensed party.

5 If a person seeks advice from a licensed party in his or her own name and on his or her own behalf, the person is an applicant for business for the licensed party.

6 If a professional agent introduces a third party to a licensed party so the third party can be given advice or make an investment in his or her own

name, the third party (and not the professional agent) is an applicant for business for the licensed party.

7 If an individual claiming to represent a company, partnership or other legal person applies to a licensed party to conduct business on behalf of the legal person, the legal person (and not the individual claiming to represent it) is an applicant for business for the licensed party.

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

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

4.2.4 What is a *business relationship*?

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

4.2.5 What is a *one-off transaction*?

A ***one-off transaction***, in relation to a licensed party, is a transaction carried out by the licensed party 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

Part 4.3 CDD and ongoing monitoring

4.3.1 Licensed party to assess applicants for business

A licensed party 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 licensed party or is an occasional customer seeking to carry out a one-off transaction.

Note See the following provisions that are relevant to this rule:

- rule 4.2.3 (Who is an *applicant for business*?)
- rule 4.2.4 (What is a *business relationship*?)
- rule 4.2.5 (What is a *one-off transaction*?).

4.3.2 When CDD required—basic requirement

(1) A licensed party 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 the threshold amount;

Note A licensed party must have systems and controls to identify one-off transactions that are linked to the same person (see rule 4.3.12 (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.

(2) In this rule:

threshold amount means 50,000 Riyals (or the equivalent in any other currency at the relevant time).

(3) This rule is subject to the following provisions:

- rule 3.4.8 (Introducers)
- rule 3.4.9 (Group introductions)
- rule 3.4.10 (Intermediaries)

- rule 4.3.4 (When CDD may not be required—acquired businesses)
- rule 5.2.2 (2) (Licensed party must ensure no tipping-off occurs).

4.3.3 Licensed party unable to complete CDD for customer

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

Examples

1 the licensed party is unable to verify the customer's identity using reliable, independent source, data or information

2 the customer exercises cancellation or cooling-off rights

(2) The licensed party:

(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 licensed party acquires the business of another licensed party, either in whole or as a product portfolio.

(2) The licensed party is not required to conduct 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 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 licensed party's senior management must prepare or approve, and document, an action plan that ensures that the licensed party 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 licensed party for all of the customers acquired with the business, the licensed party's senior management must prepare or approve, and document, an action plan that ensures that the licensed party conducts CDD for all of the customers for whom full customer records are not available to the licensed party as soon as possible.

4.3.5 Timing of CDD—establishment of business relationship

(1) A licensed party 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;

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 any 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 company 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) If the licensed party establishes a business relationship with the customer under subrule (2), but cannot complete CDD for the customer, the licensed party:

(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.

4.3.6 Timing of CDD—one-off transactions

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

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

(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 in accordance with Chapter 5 of these rules.

4.3.7 When CDD required—additional requirement for existing customers

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

(2) Without limiting subrule (1), a licensed party 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 licensed party must decide whether to conduct CDD for a customer if:

(a) the licensed party'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 licensed party becomes aware that it lacks sufficient information about the customer.

4.3.8 Extent of CDD—general requirement

(1) A licensed party 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, and the jurisdiction risk; and

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

(2) Without limiting subrule (1), a licensed party 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 licensed party is required to conduct CDD for a legal person (other than a corporation) or a legal arrangement.

(2) If the licensed party identifies the class of persons in whose main interest the legal person or legal arrangement is established or operated as a beneficial owner, the licensed party is not required to identify all the members of the class.

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

4.3.10 Ongoing monitoring required

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

(2) Without limiting subrule (1), the licensed party must pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose.

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 licensed party 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 (3) 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) (Licensed party must ensure no tipping-off occurs).

4.3.11 Procedures for ongoing monitoring

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

(2) The systems and controls:

(a) must flag transactions for further examination; and

(b) must provide:

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

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

(iii) if there is knowledge or suspicion of money laundering or terrorism financing raised by the findings—for a report to be made promptly to the licensed party's MLRO.

(3) The monitoring provided by the systems and controls may be:

(a) in real time (that is, transactions are reviewed as they take place or are about to take place); or

(b) after the event (that is, transactions are reviewed after they have taken place).

(4) The monitoring may be, for example:

(a) by reference to particular types of transactions or the customer's risk profile;

(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.

4.3.12 Linked one-off transactions

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

(2) If a licensed party knows, suspects, or has reasonable grounds to know or suspect, that a series of linked one-off transactions

involves money laundering or terrorism financing, the licensed party must make a suspicious transaction report to the FIU.

Part 4.4 Customer identification documentation

Division 4.4.A Customer identification documentation—general

4.4.1 Elements of customer identification documentation

Customer identification documentation relates to 2 distinct elements, namely:

(1) the customer as a physical person; and

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

4.4.2 Records of customer identification documentation etc

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

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

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

Division 4.4.B Customer identification documentation—the economic activity

4.4.3 Risks associated with the economic activity—general

(1) A licensed party must take into account that the risks associated with money laundering and the financing of terrorism arise from the fact that either:

(a) the funds that are going to be put through a business relationship derive from crime or 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 licensed party must properly address these risks using the following approach:

(a) identify the sources of the customer's wealth and funds;

Note By establishing that the sources are not from crime, the licensed party substantially mitigates the customer risk.

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

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

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

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

Note Information obtained can assist the licensed party in establishing the money laundering and 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 licensed party must obtain, and document, the information to an appropriate level having regard to the applicant's risk profile.

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

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

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

(1) In conducting CDD for an applicant for business a licensed party must obtain, and document, information about the purpose and intended nature of the business relationship.

(2) The extent and detail of this information must be sufficient to allow the licensed party:

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

(b) to increase information requirements to satisfy itself that money laundering or financing of terrorism has not taken place; and

(c) if it is not satisfied about the information received—to consider making a suspicious transaction report to the FIU.

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

Division 4.4.C Customer identification documentation—particular applicants for business

4.4.6 Customer identification documentation—individuals

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

(2) If the individual's risk profile is low risk, the licensed party 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

(b) a document from a reliable, independent source that bears the individual's name and a photograph of the individual; or

(c) other documents from reliable, independent data sources.

4.4.7 Customer identification documentation—multiple individual applicants

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

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

4.4.8 Customer identification documentation—corporations

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

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

(a) either:

(i) obtaining a copy of valid memorandum of association, articles of association and commercial register or the certificate of trade (or any equivalent document), which includes:

(A) the corporation's full name; and

(B) the corporation's registered number;

(C) any other documents requested by the licensed party.

(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 financial report and audited accounts; and

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

(i) the establishing of the relationship with the licensed party; and

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

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

(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 a corporation applicant for business (***A***) is a subsidiary of another corporation (***B***) that is in turn a subsidiary of a third corporation (***C***), the licensed party must comply with subrules (3) and (4) in relation to B as well as C.

(5) The licensed party must conduct additional customer due diligence if the corporation:

(a) is incorporated in a foreign jurisdiction; or

(b) has no direct business links to State of Qatar.

(6) If the corporation, or the corporation's parent entity, is listed in a stock exchange that has disclosure requirements that enable verification of the customer's or owner's identity in a fully transparent way, the licensed party:

(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.

4.4.9 Customer identification documentation—unincorporated partnerships and associations

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

(2) If the applicant's partners or directors are not known to the company, the identity of all of the partners or directors must be verified using reliable, independent source documents, data or information.

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

(a) the establishing of the relationship with the licensed party; and

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

4.4.10 Customer identification documentation—charities

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

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

4.4.11 Customer identification documentation—legal arrangements

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

(2) In conducting a risk assessment for the legal arrangement, the licensed party 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 licensed party 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 licensed party 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 legal arrangement.

Note Under rule 1.3.4 (1) (c) and rule 1.3.4 (4), the ***beneficial owner*** of a legal arrangement is the individual who ultimately owns, or exercises effective control over, the arrangement and includes:

(1) 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;

(2) 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

(3) an individual who, directly or indirectly, exercises control over at least 20% (by value) of the property of the arrangement.

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

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

(b) the terms of the legal arrangement;

(5) The licensed party 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 licensed party:

(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.

4.4.12 Customer identification documentation—clubs and societies

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

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

(4) If the applicant's risk profile is low risk, the licensed party must, as a minimum, obtain the following information about the applicant:

(a) the applicant's full name;

(b) the applicant's legal status;

(c) the applicant's purpose, including any constitution;

(d) the names of all of the applicant's officers.

(5) The licensed party must also verify the identities of the applicant's officers who have authority:

(a) to establish a relationship with the licensed party on the applicant's behalf; or

(b) to act on behalf of the applicant for the relationship, including by operating any account or by giving instructions about the use, transfer or disposal of any of the applicant's assets.

4.4.13 Customer identification documentation—government bodies

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

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

(a) the applicant's legal status;

(b) the applicant's ownership and control;

(c) the applicant's main address.

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

(a) to establish a relationship with the licensed party on the applicant's behalf; or

(b) to act on behalf of the applicant for the relationship, including by operating any account or by giving instructions about the use, transfer or disposal of any of the applicant's assets.

4.4.14 Other requirements for customer identification of legal persons

(1) In addition to the customer identification documentation required for particular applicants under this Division, a licensed party

must verify the identity of an applicant for business that is a legal person using reliable, independent source documents, data or information that show the following:

(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;

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

(2) The licensed party 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 licensed party:

(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 person and its ownership and control structure.

(4) For subrule (3) (b), the licensed party 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 1.3.4 (1) (c) and rule 1.3.4 (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.

Part 4.5 Enhanced CDD and ongoing monitoring

4.5.1 Enhanced CDD and ongoing monitoring

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

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

(2) if required by the Regulator or the NAMLTF Committee to do so;

(3) in cases where the Financial Action Task Force calls upon its members to require enhanced CDD and enhanced ongoing monitoring; and

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

4.5.2 Measures required for enhanced CDD or ongoing monitoring

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

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

(2) update customer identification and beneficial owner identification;

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

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

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

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

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

4.5.3 Other measures in addition to enhanced CDD and ongoing monitoring

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

(1) 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

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

Part 4.6 Reduced or simplified CDD and ongoing monitoring

4.6.1 Reduced or simplified CDD—general

Except if there is a suspicion of money laundering or terrorism financing, a licensed party may conduct, for a customer, reduced or simplified CDD under rules 4.6.2 and 4.6.3 when:

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

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

4.6.2 Customer with low level of risk

A licensed party may conduct reduced or 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:

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

(2) 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;

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

(4) 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.

4.6.3 Reduced or simplified CDD—listed, regulated public companies

A licensed party may conduct reduced or 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.

4.6.4 Reduced or simplified ongoing monitoring

The provisions of this Part apply 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 licensed party, of the intensity, extent and frequency of:

(1) the licensed party's scrutiny of the customer's transactions; and

(2) the licensed party's review of its records of the customer.

Chapter 5 Reporting and tipping-off

Part 5.1 Reporting requirements

Note for Part 5.1

Principle 4 (rule 1.2.4) requires a licensed party 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 licensed party to know its customers well enough under Chapter 4 (Know your customer).

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

(2) A licensed party must consider the following matters in deciding whether an unusual or inconsistent transaction is a suspicious transaction:

(a) whether the transaction has no apparent or visible economic or lawful purpose;

(b) whether the transaction has no reasonable explanation;

(c) whether the size or pattern of the transaction is out of line with any earlier pattern or the size or pattern of transactions of similar customers;

(d) whether the customer has failed to give an adequate explanation for the transaction or to fully provide information about it;

(e) whether the transaction involves the use of a newly established business relationship;

(f) whether the transaction involves the use of offshore accounts, companies or structures that are not supported by the customer's economic needs;

(g) whether the transaction involves the unnecessary routing of funds through third parties.

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

Division 5.1.B Internal reporting

5.1.2 Internal reporting policies

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

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

5.1.3 Access to MLRO

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

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

5.1.4 Obligation of officer or employee to report to MLRO

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

(a) the proceeds of crime;

(b) related to terrorism financing; or

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

(2) The officer or employee must promptly make a suspicious transaction report to the licensed party'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 licensed party in relation to the funds;

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

(iii) for a customer—the licensed party 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 may commit an offence against the AML/CFT Law.

5.1.5 Obligations of MLRO on receipt of internal report

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

(a) if the licensed party's policies, procedures, systems and controls allow an initial report to be made orally and the initial report is made orally—properly document the report;

(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 licensed party about the applicant for business, customer or transaction to which the report relates;

(d) decide whether the transaction is suspicious;

Note See rule 5.1.7 (Obligation of licensed party to report to FIU).

(e) give written notice of the decision to the individual who made the report.

(2) A reference in this rule to the ***MLRO*** includes a reference to a person acting under rule 5.1.7 (3) (b) (Obligation of licensed party to report to FIU) in relation to the making of a report on the party's behalf.

Division 5.1.C External reporting

5.1.6 External reporting policies

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

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

(a) to comply with the AML/CFT Law and these rules in relation to the prompt making of suspicious transaction reports to the FIU; and

(b) to cooperate effectively with the FIU and law enforcement agencies in relation to suspicious transaction reports made to the FIU.

5.1.7 Obligation of licensed party to report to FIU

(1) This rule applies to a licensed party if it knows, 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 or terrorist acts or by terrorist organisations.

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

(3) The report must be made on the licensed party's behalf by:

(a) the MLRO; or

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

(4) The licensed party 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;

(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 licensed party in relation to the funds;

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

(iii) for a customer—the licensed party 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 licensed party's knowledge or suspicion is based or the grounds for the licensed party's knowledge or suspicion; and

(b) if the licensed party knows or suspects that the funds belong to a third person—the facts or circumstances on which that knowledge or suspicion is based or the grounds for the licensed party's knowledge or suspicion.

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

(6) If a licensed party 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

(1) This rule applies if a licensed party:

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

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

5.1.9 Licensed party may restrict or terminate business relationship

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

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

Note ***Tipping-off*** is defined in rule 5.2.1.

(3) If the licensed party 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

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

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

(2) necessary to demonstrate how rule 5.1.5 (Obligations of MLRO on receipt of internal report) was complied with in relation to each internal suspicious transaction report; and

(3) showing the details of each suspicious transaction report made to the FIU by the licensed party.

Part 5.2 Tipping-off

5.2.1 What is *tipping-off*?

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

(1) may result in the applicant or customer, or a third party (other than the FIU or the Regulator), knowing or suspecting that the applicant or customer is or may be the subject of:

(a) a suspicious transaction report; or

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

(2) may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime, or the prevention of money laundering or terrorism financing.

5.2.2 Licensed party must ensure that no tipping-off occurs

(1) A licensed party must ensure that:

(a) its officers and employees are aware of, and sensitive to:

(i) the issues surrounding tipping-off; and

(ii) the consequences of tipping-off; and

(b) it has policies, procedures, systems and controls to prevent tipping-off within the company or its group.

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

(3) If the licensed party acts under subrule (2), the MLRO must make and keep records to demonstrate the grounds for the belief that conducting 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 licensed party must take all reasonable measures to ensure that information relating to suspicious transaction reports is safeguarded and, in particular, that information relating to a suspicious transaction report is not disclosed to any person (other than a member of the licensed party's senior management) without the consent of the licensed party's MLRO.

(2) The MLRO must not consent to information relating to a suspicious transaction report being disclosed to a person unless the MLRO is satisfied that disclosing the information to the person would not constitute tipping-off.

(3) If the MLRO gives consent, the MLRO must make and keep records to demonstrate how the MLRO was satisfied that disclosing the information to the person would not constitute tipping-off.

Chapter 6 Screening and training requirements

Part 6.1 Screening procedures

Note for Part 6.1

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

6.1.1 Screening procedures—particular requirements

(1) In this rule:

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

Examples

1 a senior manager of the licensed party

2 the licensed party's MLRO or deputy MLRO

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

Note The licensed party's AML/CFT programme must include internal policies, procedures, systems and controls to prevent money laundering and terrorism financing and screening procedures (see rule 2.1.1 (3) (a) and (b)).

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

(a) for a higher-impact individual—the licensed party 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 licensed party 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 licensed party:

(a) must obtain references about the individual;

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

(c) must obtain details of any criminal convictions of the individual;

(d) for a licensed individual—must obtain details of any regulatory action taken in relation to the individual; and

(e) must 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 (rule 1.2.5) also requires a licensed party to have an appropriate ongoing AML/CFT training programme for its officers and employees.

6.2.1 Appropriate AML/CFT training programme to be delivered

(1) A licensed party must identify, design, deliver and maintain an appropriate ongoing AML/CFT training programme for its officers and employees.

(2) The programme must ensure that the licensed party's officers and employees are aware, and have an appropriate understanding, of the following:

(a) their legal and regulatory responsibilities and obligations, particularly those under the AML/CFT Law and these rules;

(b) their role in preventing money laundering and terrorism financing, and the liability that they, and the licensed party, 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 licensed party is managing money laundering and terrorism financing risks, how risk management techniques are being applied by the licensed party, 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 licensed party, and how to recognise suspicious transactions;

(e) the licensed party's processes for making internal suspicious transaction reports, including how to make effective and efficient reports to the MLRO whenever

money laundering or terrorism financing is known or suspected.

(3) The training must enable the licensed party's officers and employees to seek and assess the information that is necessary for them to decide whether a transaction is suspicious.

(4) In making a decision about what is appropriate training for its officers and employees, the licensed party must consider the following:

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

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

(c) the degree of supervision over, or independence exercised by, them;

(d) the availability of information that is needed for them to decide whether a transaction is suspicious;

(e) the size of the licensed party's business and the risk of money laundering and terrorism financing;

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

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

Examples

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

2 the training for employees who deal with customers face to face needs to be different to the training for employees who deal with customers non-face to face

(5) Subrule (4) does not limit the matters that the licensed party may consider.

6.2.2 Training must be maintained and reviewed

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

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

(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 licensed party's AML/CFT policies, procedures, systems and controls.

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

(3) The licensed party's senior management must in a timely way:

(a) consider the outcomes of each review; and

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

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

Chapter 7 Providing documentary evidence of compliance

Note for Chapter 7

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

Part 7.1 General record-keeping obligations

7.1.1 Records about compliance

(1) A licensed party must make the records necessary:

(a) to enable it to comply with the AML/CFT Law and these rules; and

(b) to demonstrate at any time whether compliance with the AML/CFT Law and these rules has been achieved.

(2) Without limiting subrule (1) (b), the licensed party must make the records necessary to demonstrate how:

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

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

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

(d) each of the licensed party'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.

Note See also rule 5.1.10 (Reporting records to be made by MLRO).

7.1.2 How long records must be kept

(1) All records made by a licensed party for the AML/CFT Law or these rules must be kept for at least 10 years after the day they are made.

(2) All records made by a licensed party 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 licensed party 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 licensed party 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 licensed party last completed a transaction with or for the customer.

(3) If the day the business relationship with the customer ended is unclear, it is taken to have ended on the day the licensed party last completed a transaction for or with the customer.

(4) This rule is subject to rule 5.1.8 (Obligation not to destroy records relating to customer under investigation).

7.1.3 Retrieval of records

(1) A licensed party must ensure that all types of records kept for the AML/CFT Law and these rules can be retrieved without undue delay.

(2) Without limiting subrule (1), a licensed party must establish and maintain systems that enable it to respond fully and quickly to inquiries from the FIU and law enforcement authorities about:

(a) whether it maintains, or has maintained during the previous 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 licensed party must make and keep records in relation to:

(a) its business relationship with each customer; and

(b) each transaction that it conducts with or for a customer.

(2) The records must:

(a) comply with the requirements of the AML/CFT Law and these rules;

(b) enable an assessment to be made of the licensed party's compliance with:

(i) the AML/CFT Law and these rules; and

(ii) its AML/CFT policies, procedures, systems and controls;

(c) enable any transaction effected by or through the licensed party to be reconstructed;

(d) enable the licensed party to comply with any request, direction or order by a competent authority, judicial officer or court for the production of documents, or the provision of information, within a reasonable time;

(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.

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 4.3.10 (4) for records on monitoring of complex, unusual or large transactions.

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

(1) the dates the training was provided;

(2) the nature of the training; and

(3) the names of the individuals to whom the training was provided.

Chapter 8 Miscellaneous

8.1.1 Approved forms to be used

(1) The Regulator may, by written notice, approve forms for the purposes of the AML/CFT Law or these rules.

(2) If a form is approved under subrule (1) for a particular purpose, the form:

(a) must be used for that purpose; and

(b) must be completed in accordance with rule 8.1.2.

8.1.2 Completion of forms

(1) Substantial compliance with a form approved by the Regulator for the purposes of the AML/CFT Law or these rules is sufficient.

(2) However, if a form requires:

(a) the form to be signed;

(b) the form to be prepared in a particular way (for example, on paper of a particular size or quality or in a particular electronic form);

(c) the form to be completed in a particular way;

(d) particular information to be included in the form, or a particular document to be attached to or given to a person with the form; or

(e) the form, information in the form, or a document attached to or given with the form, to be verified in a particular way;

the form is properly completed only if the requirement is complied with.

Annex of definitions

(see rule 1.1.4)

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

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 the State of Qatar.

Note ***Jurisdiction*** **is** defined in this Annex.

applicant for business has the meaning given by rule 4.2.3.

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

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

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

(a) a legal person in the same group as A;

(b) a subsidiary of A.

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

beneficial owner has the meaning given by rule 1.3.4.

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 the State of 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 securities relationship has the meaning given by rule 1.3.7.

customer has the meaning given by rule 1.3.3.

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

deputy MLRO, in relation to a licensed party, means the party's deputy money laundering reporting officer.

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

(a) a person named as director; and

(b) any other person in accordance with whose instructions the company is accustomed to act.

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; and

(b) anything on which there are figures, marks, numbers, perforations, symbols or anything else having a meaning for individuals qualified to interpret them; and

(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.

Note ***Writing*** is defined in this Annex.

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 entity, and includes for example any person.

external auditor, in relation to a licensed party and a review under rule 2.1.1 (4), means the external auditor making the review duly registered with the Regulator.

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.

financial institution has the meaning given by the AML/CFT Law, article 1.

FIU means the Financial Information Unit established under the AML/CFT Law.

foreign jurisdiction means a jurisdiction other than Qatar (which includes the Qatar Financial Centre).

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.

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

(a) A;

(b) any parent entity of A;

(c) any subsidiary (direct or indirect) of any parent entity.

jurisdiction means any kind of legal jurisdiction, and includes, for example:

(a) the State;

(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.

licensed party has the meaning given by rule 1.3.2.

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 the State 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.

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

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

(b) supply arrangements and functions, including, for example, the supply of electricity or water and the provision of catering and cleaning services; or

(c) the purchase of standardised services, including, for example, market information services and the provision of prices.

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

(a) a legal person that holds a majority of the voting power in A;

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

(c) a parent entity of any legal person that is a parent entity of A.

person means:

(a) an individual (including an individual occupying an office from time to time); or

(b) a legal person.

politically exposed person or ***PEP*** has the meaning given by rule 1.3.5.

predicate offence has the same meaning as in the AML/CFT Law, Chapter 1.

proceeds of crime means funds derived or obtained, directly or indirectly, from a predicate offence (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.

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

(a) money of any jurisdiction;

(b) bonds, commercial notes, drafts, letters of credit, money orders, securities, shares, travellers' cheques, and other negotiable or non-negotiable instruments of any kind;

(c) bank credits;

(d) any right to interest, dividends or other income on or accruing from or generated by property of any kind;

(e) any other things in action;

(f) any other charge, claim, demand, easement, encumbrance, lien, power, privilege, right, or title, recognised or protected by the law of any jurisdiction over, or in relation to, land or property of any other kind; and

(g) any other documents evidencing title to, or to any interest in, land or property of any kind.

product includes the provision of a service.

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

shell bank has the meaning given by rule 1.3.6.

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 licensed party, means a suspicious transaction report to the licensed party's MLRO or by the licensed party 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 Law No. (27) of 2019 on Combating Terrorism.

terrorism financing has the same meaning as in the AML/CFT Law, Chapter 2, Article (3).

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.

terrorist act has the same meaning as in the AML/CFT Law, Chapter 1.

the Regulator has the meaning given by rule 1.3.1.

the State means the State of Qatar.

tipping-off has the meaning given by rule 5.2.1.

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

(a) the giving of advice;

(a) the provision of any service; and

(b) 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).