هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE REGULATORY AUTHORITY

Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019

QFCRA Rules 2019-9

The Board of the Qatar Financial Centre Regulatory Authority makes the following rules, and gives the following guidance, under Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing and the *Financial Services Regulations*.

Dated 2 January 2020.

Abdulla Bin Saoud Al-Thani
Chairman

VZ

هيئة تنظيم مركز قطر للمال
QATAR FINANCIAL CENTRE REGULATORY AUTHORITY

Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019

QFCRA Rules 2019-9

made under

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

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

Financial Services Regulations

Contents

Chapter 1 General provisions

Part 1.1 Introductory

1.1.1 Name of rules

These rules are the *Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019* (AMLG).

1.1.2 Commencement

These rules commence on 1 February 2020.

1.1.3 Repeal of 2012 AMLG

(1) The *Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012* is repealed.

(2) A reference to the *Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012* or to any of its provisions in other Rules or any instrument that has not been specifically changed is taken to be a reference to the *Anti-Money Laundering and Combating the Financing of Terrorism (General Insurance) Rules 2019* or to their equivalent provisions as necessary to give effect to those Rules, instrument or provisions.

1.1.4 Application of these rules

These rules apply to general insurance firms.

1.1.5 Effect of definitions, notes and examples

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

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

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

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

Part 1.2 Key AML/CFT principles

1.2.1 Principle 1—responsibilities

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

1.2.2 Principle 2—risk-based approach

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

1.2.3 Principle 3—know your customer

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

1.2.4 Principle 4—effective reporting

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

1.2.5 Principle 5—high standard screening and appropriate training

A firm must:

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

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

1.2.6 Principle 6—evidence of compliance

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

Part 1.3 Key terms

1.3.1 What are a *firm* and a *general insurance firm*?

(1) A ***general insurance firm*** (or ***firm***) is an entity that has an authorisation (granted under the *Financial Services Regulations*, Part 5) to conduct, in or from the QFC, only either or both of the following regulated activities:

(a) general insurance business;

(b) insurance mediation (within the meaning given by IMEB, rule 1.2.2) in relation to either or both of:

(i) general insurance contracts; and

(ii) pure protection contracts.

Note A firm that conducts any other regulated activity (whether or not it also conducts a regulated activity mentioned in rule 1.3.1) in or from the QFC must comply with the *Anti-Money Laundering and Combating the Financing of Terrorism Rules 2019*—see those rules.

(2) In subrule (1):

general insurance business and ***general insurance contract*** have the same respective meanings as in PINS.

pure protection contract means a long term insurance contract (within the meaning given by PINS) that meets all of the following conditions:

(a) the benefits under the contract are payable only on death or for incapacity due to injury, sickness or infirmity;

(b) either:

(i) the contract has no surrender value; or

(ii) the consideration for the contract consists of a single premium and its surrender value does not exceed that premium;

(c) the contract makes no provision for its conversion or extension in a way that would result in it ceasing to comply with paragraph (a) or (b);

(d) the contract is not a reinsurance contract (within the meaning given by PINS).

regulated activities has the same meaning as in the *Financial Services Regulations*.

1.3.2 Who is a *customer*?

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

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

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

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

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

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

Chapter 2 General AML and CFT responsibilities

Part 2.1 The firm

2.1.1 Firms to develop AML/CFT programme

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

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

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

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

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

Note See also Part 6.1 (Screening procedures).

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

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

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

(e) appropriate compliance management arrangements; and

Note See:

- rule 2.1.5 (Compliance by officers, employees, agents)
- rule 2.1.6 (Application of AML/CFT Law requirements, policies to branches and associates)
- rule 2.1.7 (Application of AML/CFT Law requirements, policies to outsourced functions and activities).

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

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

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

(a) the function being reviewed; and

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

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

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

2.1.2 Policies must be risk-sensitive, appropriate and adequate

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

2.1.3 Matters to be covered by policies

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

(a) CDD and ongoing monitoring;

(b) record making and retention;

(c) detection of suspicious transactions;

(d) internal and external reporting obligations;

(e) communication of the policies, procedures, systems and controls to the firm's officers and employees; and

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

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

(a) provide for the identification and scrutiny of:

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

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

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

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

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

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

(f) 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;

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

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

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

2.1.4 Assessment and review of policies

A firm must annually assess the adequacy and effectiveness of its AML/CFT policies, procedures, systems and controls in identifying and preventing money laundering and terrorism financing.

Note For other annual assessments and reviews, see:

- rule 2.3.8 (Minimum annual report by MLRO)
- rule 2.3.9 (Consideration of MLRO reports)

2.1.5 Compliance by officers, employees, agents

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

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

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

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

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

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

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

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

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

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

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

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

(1) This rule applies to a firm if:

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

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

(2) The firm must ensure that the branch or associate, and the officers, employees, agents and contractors of the branch or associate, wherever they are, comply with:

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

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

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

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

(a) 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 this jurisdiction to the firm's MLRO; and

(b) provide timely, unrestricted access by the firm's senior management and MLRO, and by the Regulator and FIU, to documents and information of the branch or associate, wherever

they are held, that relate directly or indirectly to its customers or accounts or to transactions in, from or to this jurisdiction;

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

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

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

(6) Also, this rule does not prevent the firm and its branches, or the firm and the other members of its group, from applying higher, consistent standards in their AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend across the firm and its branches or the firm and the other members of its group.

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

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

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

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

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

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

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

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

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

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

(3) The firm must, through a service level agreement or otherwise, ensure that the third party, and the officers, employees, agents and contractors of the third party, wherever they are, comply with the following in relation to the outsourcing:

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

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

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

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

(a) require the third party, and the officers, employees, agents and contractors of the third party, wherever they are, to provide suspicious transaction reports for transactions in, from or to this jurisdiction involving the firm (or the third party on its behalf) to the firm's MLRO; and

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

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

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

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

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

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

(7) This rule is in addition to any other provision of the Regulator's Rules about outsourcing.

Part 2.2 Senior management

Note for Part 2.2

Principle 1 (see rule 1.2.1) requires the senior management of a firm to ensure that the firm's policies, procedures, systems and controls are implemented, and that they appropriately and adequately address the requirements of the AML/CFT Law and these rules.

2.2.1 Overall senior management responsibility

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

2.2.2 Particular responsibilities of senior management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(C) all transaction records; and

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

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

Guidance

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

- senior management consistently enforces a top-down approach to its AML/CFT responsibilities;
- there is a demonstrable and sustained firm-wide commitment to the AML/CFT principles and compliance with the AML/CFT Law, these rules and the firm's AML/CFT policies, procedures, systems and controls;

- AML/CFT risk management and regulatory requirements are embedded at all levels of the firm and in all elements of its business or activities.

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

(i) the development of new products;

(ii) the taking on of new customers; and

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

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

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

Part 2.3 MLRO and Deputy MLRO

Division 2.3.A Appointment of MLRO and Deputy MLRO

2.3.1 Appointment—MLRO and Deputy MLRO

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

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

2.3.2 Eligibility to be MLRO or Deputy MLRO

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

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

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

(i) to act independently; and

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

(2) If a general insurance firm proposes to appoint as MLRO an individual who is not ordinarily resident in Qatar, the firm must satisfy the Regulator that the MLRO function can be adequately exercised by an MLRO who is not resident in Qatar.

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

Division 2.3.B Roles of MLRO and Deputy MLRO

2.3.3 General responsibilities of MLRO

The MLRO for a firm is responsible for:

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

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

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

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

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

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

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

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

2.3.4 Particular responsibilities of MLRO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3.5 Role of Deputy MLRO

(1) The Deputy MLRO for a firm acts as the firm's MLRO during absences of the MLRO and whenever there is a vacancy in the MLRO's position.

(2) When the Deputy MLRO acts as MLRO, these rules apply in relation to the Deputy MLRO as if the Deputy MLRO were the MLRO.

2.3.6 How MLRO must carry out role

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

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

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

Division 2.3.C Reporting by MLRO to senior management

2.3.7 MLRO reports

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

(2) However, the MLRO must give the senior management a report that complies with rule 2.3.8 (Minimum annual report by MLRO) for each calendar year. The report must be given in time to enable compliance with rule 2.3.9 (2).

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

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

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

2.3.8 Minimum annual report by MLRO

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

(2) The report must assess the adequacy and effectiveness of the firm's AML/CFT policies, procedures, systems and controls in identifying and preventing money laundering and terrorism financing.

(3) The report must include the following for the period to which it relates:

(a) the numbers and types of internal suspicious transaction reports made to the MLRO;

(b) the number of these reports that have, and the number of these reports that have not, been passed on to the FIU;

(c) the reasons why reports have or have not been passed on to the FIU;

(d) the numbers and types of breaches by the firm of the AML/CFT Law, these rules, or the firm's AML/CFT policies, procedures, systems and controls;

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

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

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

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

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

Note These provisions require action plans:

- rule 2.3.9 (1) (b) (Consideration of MLRO reports)
- rule 6.2.2 (3) (b) (Training must be maintained and reviewed).

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

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

2.3.9 Consideration of MLRO reports

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

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

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

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

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

2.3.10 Annual reports

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

2.3.11 Visits by non-resident MLRO

A firm whose MLRO is not ordinarily resident in Qatar must ensure that the MLRO inspects the firm's operations in Qatar frequently enough to allow him or her to assess the accuracy and reliability of the information supplied to the Regulator in the reports required by rule 2.3.10.

2.3.12 Regulator may direct firm to appoint resident MLRO

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

(2) The Regulator may direct the firm:

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

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

Chapter 3 The risk-based approach

Note for Chapter 3

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

3.1.1 Firms must conduct risk assessment and decide risk mitigation

(1) A firm:

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

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

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

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

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

Examples of 'associated' jurisdictions for a customer

1 the jurisdiction where the customer lives or is incorporated or otherwise established

2 each jurisdiction where the customer conducts business or has assets.

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

(2) The firm must be able to demonstrate:

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

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

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

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

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

3.1.2 Approach to risk mitigation must be based on suitable methodology

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

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

(a) includes:

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

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

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

(c) is designed to enable the firm:

(i) to identify and recognise any changes in its money laundering and terrorism financing risks; and

(ii) to change its threat assessment methodology as needed; and

(d) includes assessing risks posed by:

(i) new products and services; and

(ii) new or developing technologies.

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

Chapter 4 Know your customer

Part 4.1 Know your customer—general

Note for Part 4.1

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

4.1.1 Know your customer principle—general

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

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

Part 4.2 Know your customer—key terms

4.2.1 What is *ongoing monitoring*?

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

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

(b) reviewing the firm's records of the customer to ensure that documents, data and information collected using CDD and ongoing monitoring for the customer are kept up-to-date and relevant.

4.2.2 Who is an *applicant for business*?

An ***applicant for business***, in relation to a firm, is a person seeking to form a business relationship, or carry out a one-off transaction, with the firm.

Examples of applicants for business

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

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

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

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

Part 4.3 Enhanced CDD and ongoing monitoring

4.3.1 Enhanced CDD and ongoing monitoring—general

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

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

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

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

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

Examples

A greater degree of CDD and monitoring would be necessary in the following cases:

- a customer who is associated with terrorist acts
- a customer from a jurisdiction with impaired international cooperation
- a customer from a non-cooperative, high risk or sanctioned jurisdiction
- a customer from a jurisdiction with high propensity for corruption.

4.4.2 Measures required for enhanced CDD or ongoing monitoring

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

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

(b) update customer identification and beneficial owner identification;

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

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

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

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

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

(h) make the first of any required payments to the customer through an account in a bank that is regulated and supervised (at least for AML and CFT purposes) by the Regulator or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction.

4.4.3 Other measures in addition to enhanced CDD and ongoing monitoring

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

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

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

Chapter 5 Reporting and tipping-off

Part 5.1 Reporting requirements

Note for Part 5.1

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

Division 5.1.A Reporting requirements—general

5.1.1 Unusual and inconsistent transactions

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

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

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

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

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

(b) whether the transaction has no reasonable explanation;

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

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

(e) whether the transaction involves the use of a newly established business relationship or is for a one-off transaction;

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

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

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

Division 5.1.B Internal reporting

5.1.2 Internal reporting policies

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

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

5.1.3 Access to MLRO

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

Note The MLRO is responsible for receiving, investigating and assessing internal suspicious transaction reports for the firm (see rule 2.3.4 (a)).

5.1.4 Obligation of officer or employee to report to MLRO

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

(a) the proceeds of crime;

(b) related to terrorism financing; or

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

(2) The officer or employee must promptly make a suspicious transaction report to the firm's MLRO.

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

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

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

(c) even though:

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

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

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

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

(4) If the officer or employee makes a suspicious transaction report to the MLRO (the ***internal report***) in relation to the applicant for business or customer, the officer or employee must promptly give the MLRO details of every subsequent transaction of the applicant or customer (whether or not of the same nature as the transaction that gave rise to the internal report) until the MLRO tells the officer or employee not to do so.

Note An officer or employee who fails to make a report under this rule:

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

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

5.1.5 Obligations of MLRO on receipt of internal report

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

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

(b) give the individual making the report a written acknowledgment for the report, together with a reminder about the provisions of Part 5.2 (Tipping-off);

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

(d) decide whether the transaction is suspicious; and

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

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

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

Division 5.1.C External reporting

5.1.6 External reporting policies

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

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

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

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

5.1.7 Obligation of firm to report to FIU

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

(a) the proceeds of crime;

(b) related to terrorism financing; or

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

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

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

(a) the MLRO; or

(b) if the report cannot be made by the MLRO (or Deputy MLRO) for any reason—by a person who is employed (as described in rule 2.3.2 (1) (a)) at the management level by the firm, or by a legal person in the same group, and who has sufficient seniority, knowledge, experience and authority to investigate and assess internal suspicious transaction reports.

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

(4) The firm must make the report:

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

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

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

(d) even though:

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

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

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

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

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

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

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

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

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

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

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

5.1.8 Obligation not to destroy records relating to customer under investigation

(1) This rule applies if:

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

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

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

5.1.9 Firm may restrict or terminate business relationship

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

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

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

Division 5.1.D Reporting records

5.1.10 Reporting records to be made by MLRO

The MLRO of a firm must make and keep records:

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

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

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

Part 5.2 Tipping-off

5.2.1 What is *tipping-off*?

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

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

(i) a suspicious transaction report; or

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

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

5.2.2 Firm must ensure no tipping-off occurs

(1) A firm must ensure that:

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

(i) the issues surrounding tipping-off; and

(ii) the consequences of tipping-off; and

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

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

(3) If the firm acts under subrule (2), the MLRO must make and keep records to demonstrate the grounds for the belief that conducting

CDD or ongoing monitoring would have tipped off an applicant for business or a customer.

5.2.3 Information relating to suspicious transaction reports to be safeguarded

(1) A firm must take all reasonable measures to ensure that information relating to suspicious transaction reports is safeguarded and, in particular, that information relating to a suspicious transaction report is not disclosed to any person (other than a member of the firm's senior management) without the consent of the firm's MLRO.

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

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

5.2.4 When advice not considered to be tipping-off

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

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

Chapter 6 Screening and training requirements

Part 6.1 Screening procedures

Note for Part 6.1

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

6.1.1 Screening procedures—particular requirements

(1) In this rule:

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

Examples

1 a senior manager of the firm

2 the firm's MLRO or Deputy MLRO

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

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

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

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

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

(a) obtain references about the individual;

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

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

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

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

Part 6.2 AML/CFT training programme

Note for Part 6.2

Principle 5 (see rule 1.2.5 (b)) also requires a firm to have an appropriate ongoing AML/CFT training programme for its officers and employees.

6.2.1 Appropriate AML/CFT training programme to be delivered

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

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

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

(b) their role in identifying and preventing money laundering and terrorism financing, and the liability that they, and the firm, may incur for:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

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

6.2.2 Training must be maintained and reviewed

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

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

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

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

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

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

(a) consider the outcomes of each review; and

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

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

Chapter 7 Providing documentary evidence of compliance

Note for Chapter 7

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

Part 7.1 General record-keeping obligations

7.1.1 Records about compliance

(1) A firm must make the records necessary:

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

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

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

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

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

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

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

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

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

Examples of records that must be kept

1 documents and data obtained while conducting CDD

2 account files

3 business correspondence

4 results of analysis of suspicious transaction reports

Note See also rule 5.1.10 for reporting records to be made by MLRO.

7.1.2 How long records must be kept

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

(2) All records made by a firm in relation to a customer for the purposes of AML/CFT Law or these rules must be kept for at least the longer of the following:

(a) if the firm has (or has had) a business relationship with the customer—10 years after the day the business relationship with the customer ends;

(b) if the firm has not had a business relationship with the customer or had a business relationship with the customer and carried out a one-off transaction for the customer after the relationship ended—10 years after the day the firm last completed a transaction with or for the customer.

(3) If the day the business relationship with the customer ended is unclear, it is taken to have ended on the day the firm last completed a transaction 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 firm must ensure that all types of records kept for the AML/CFT Law and these rules can be retrieved without undue delay.

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

(a) whether it maintains, or has maintained during the previous 10 years, a business relationship with any person; and

(b) the nature of the relationship.

Part 7.2 Particular record-keeping obligations

7.2.1 Records for customers and transactions

(1) A firm must make and keep records in relation to:

(a) its business relationship with each customer; and

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

(2) The records must:

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

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

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

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

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

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

(e) indicate the nature of any evidence that it obtained in relation to an applicant for business, customer or transaction; and

(f) for any such evidence—include a copy of the evidence itself or, if this is not practicable, information that would enable a copy of the evidence to be obtained.

(3) This rule is additional to any provision of the AML/CFT Law or any other provision of these rules.

7.2.2 Training records

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

(a) the dates the training was provided;

(b) the nature of the training; and

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

Glossary

(see rule)

activity includes operation.

AML means anti-money laundering.

AML/CFT Law means Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and includes any Regulations made under it.

another jurisdiction means a jurisdiction other than this jurisdiction.

applicant for business has the meaning given by rule 4.2.2.

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.

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

CDD means customer due diligence.

CFT means combating the financing of terrorism.

customer has the meaning given by rule 1.3.2.

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

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

(a) a person named as director; and

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

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.

employee, in relation to a person (***A***), means an individual:

(a) who is employed or appointed by A, whether under a contract of service or services or otherwise; or

(b) whose services are, under an arrangement between A and a third party, placed at the disposal and under the control of A.

entity means any kind of entity, and includes, for example, any person.

exercise a function means exercise or perform the function.

firm has the meaning given by rule 1.3.1.

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

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

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.

general insurance firm has the meaning given by rule 1.3.1.

governing body, of a firm, means its board of directors, committee of management or other governing body (whatever it is called).

group, in relation to a firm, means 2 or more entities consisting of:

(a) a parent company or other legal person exercising control, and coordinating functions, over the rest of the group for the application of group supervision; and

(b) 1 or more branches or subsidiaries that are subject to AML/CFT policies, procedures systems and controls at group level.

IMEB means the *Insurance Mediation Business Rules 2011*.

instrument means an instrument of any kind, and includes, for example, any writing or other document.

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

(a) Qatar;

(b) a foreign country (whether or not an independent sovereign jurisdiction), or a state, province or other territory of such a foreign country; and

(c) the Qatar Financial Centre or a similar jurisdiction.

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

(a) any entity that can establish a permanent customer relationship with a financial institution; and

(b) any entity that can own, deal with, or dispose of, property.

Examples

1 a company

2 any other corporation

3 a partnership, whether or not incorporated

4 an association or other undertaking, whether or not incorporated

5 a jurisdiction, its government or any of its organs, agencies or instrumentalities

MLRO, in relation to a firm, means the firm's money laundering reporting officer.

money laundering has the same meaning as in the AML/CFT Law, Chapter 2, Article (2).

NAMLTF Committee means the National Anti-Money Laundering and Terrorism Financing Committee established under the AML/CFT Law.

National Risk Assessment means the series of activities prepared and supervised by the NAMLTF Committee to identify and analyse the threats faced by Qatar and its financial system from money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction.

office includes position.

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

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

(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.

PINS means the *Insurance Business Rules 2006*.

proceeds of crime means funds derived or obtained, directly or indirectly, from a predicate offence (within the meaning given by the AML/CFT Law, Chapter 1), including any income, interest, revenue or other product from such funds, whether or not the funds have been converted or transferred, in whole or in part, into other properties or investment yields.

product includes the provision of a service.

QFC means Qatar Financial Centre.

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

senior manager, of a firm, means an individual employed by the firm, or by a member of the firm's group, who has responsibility either alone or with others for management and supervision of 1 or more elements of the firm's business or activities that are conducted in, from or to this jurisdiction.

subsidiary—a legal person (***A***) is a ***subsidiary*** of another legal person (***B***) if B is a parent entity of A.

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

targeted financial sanction means asset freezing or any prohibition to prevent funds from being made available, directly or indirectly, for the benefit of persons or entities listed in accordance with the Law No. (27) of 2019 on Combating Terrorism.

Note Under the Law on Combating Terrorism, the National Counter Terrorism Committee is responsible for implementing the requirements relating to targeted financial sanctions. For how to implement targeted financial sanctions, see guidelines under that Law.

terrorist means an individual who:

(a) commits, or attempts to commit, a terrorist act by any means, directly or indirectly, unlawfully and wilfully;

(b) participates as an accomplice in a terrorist act;

(c) organises or directs others to commit a terrorist act; or

(d) contributes to the commission of a terrorist act by a group of persons acting with a common purpose if the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

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

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

terrorist organisation means a group of terrorists.

the Regulator means the Qatar Financial Centre Regulatory Authority.

this jurisdiction means the QFC.

tipping-off has the meaning given by rule 5.2.1.

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

(a) the giving of advice;

(b) the provision of any service; and

(c) the conducting of any other business or activity.

writing means any form of writing, and includes, for example, any way of representing or reproducing words, numbers, symbols or anything else in legible form (for example, by printing or photocopying).