The State of Qatar
Qatar Central Bank

Anti-Money Laundering and Combating Terrorism Financing Instructions for Financial Institutions

May 2020 Edition

Contents

1. Legal Basis and Effect

1.1 Legal basis for these Instructions

Upon reviewing Law No (13) of 2012 on Qatar Central Bank and the Regulation of Financial Institutions, Law No (20) of 2019 on Combating Money Laundering and Terrorism Financing and the Implementing Regulations issued as per Prime Minister decree no. 41 of 2019, the Qatar Central Bank has decided to issue the following Instructions to financial institutions to become an integral part of each financial institution's systems and procedures, in order to detect, control, report and prevent money laundering and terrorism financing.

These Instructions are issued under the QCB Law and the AML/CFT Law. Any violation thereof penalties stepulated in the AML/CFT Law shall be applied.

1.2 Commencement and effect on previous instructions

(1) These Instructions come into force from the date of issue.

(2) All other instructions to financial institutions on AML/CFT (including the Anti-Money Laundering and Combating Terrorist Financing Regulations for Financial Institutions issued on 15 June 2010) are deemed cancelled and replaced by instrucions herein.

2. Objectives of the Instructions

(1) The objectives of these Instructions include:

(a) to maintain, enhance and protect the credibility, integrity and reputation of financial institutions in Qatar;

(b) to ensure that financial institutions in Qatar comply with the AML/CFT Law and these Instructions;

(c) to protect financial institutions operating in Qatar from being exploited as channels for passing illegal transactions arising from ML/TF and other illicit activities; and

(d) to ensure the implementation of policies, procedures, systems and controls to prevent, detect, control and report ML/TF.

(2) All financial institutions are under legal obligations to comply with the AML/CFT Law and the specific requirements included in these Instructions.

3. Definitions

(1) Without prejudice to the definitions given under the QCB Law and the AML/CFT Law, the following words and terms have the meaning assigned to them, unless the context implies otherwise.

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

beneficial owner means:

(a) for an account—the individual who ultimately owns, or exercises effective control, over the account;

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

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

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).

The ***beneficial owner*** for a corporation includes:

(a) an individual who, directly or indirectly, owns or controls at least 20% of the shares or voting rights of the corporation; and

(b) an individual who, directly or indirectly, otherwise exercises control over the corporation's management.

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.

Board means the board of directors **(**or an equivalent authority**)** of a financial institution.

business relationship, in relation to a financial institution, is a continuous business, relationship between the financial institution and a customer or DNFBPs other than a temporary relationship.

correspondent banking is the provision of a banking service by a financial institution (the ***correspondent***) to another financial institution (the ***respondent***).

customer: Any person or legal arrangement that deals with financial institutions or specific non-financial business or professions.

customer due diligence (CDD) means:

1) identification measures taken by a financial institution of a customer, such as verifying identity or establishing if the customer is acting on behalf of another person (in particular whether the customer is acting as a trustee); and

(b) if the customer is a legal entity—establishing the beneficial owner, obtaining information on the purpose and intended nature of the business relationship, etc.

financial institution, as defined under the QCB Law and The AML/CFT Law,

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

full originator information means:

(a) the originator's name;

(b) the originator's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the originator); and

(c) the originator's address, national identity number, customer identification number, or date and place of birth, the purpose of the transaction, and the relationship with the beneficiary.

full recipient information means the recipient's name and the recipient's account number or, if there is no account number, a unique reference number (being numbers that are traceable to the recipient).

jurisdiction means any kind of legal jurisdiction, which may include the State, a foreign country (whether or not an independent sovereign jurisdiction) or, province or other territory of a foreign country.

legal arrangement means an express trust or similar legal arrangement.

ML/TF means money laundering or terrorism financing.

money laundering (***ML***)means any of the following acts:

1) the conversion or transfer of funds, by any person who knows, should have known or suspects that such funds are the proceeds of crime, for the purpose of:
   (i) concealing or disguising the illicit origin of such funds; or
   (ii) assisting any person who is involved in the commission of the predicate offence to evade the legal consequences of his actions;
2) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to funds by any person who knows, should have known or suspects that such funds are the proceeds of crime;
3) the possession, acquisition, or use of funds by any person who knows, should have known or suspects that such funds are the proceeds of crime.
4) Participation in, association with or conspiracy to commit, attempt, or aid, abet, facilitate, counsel in, cooperate in, or contribute to the commission of any of the acts stipulated in this definition.

money or value transfer service (***MVTS***) means a financial service that involves the acceptance of cash, cheques and other monetary instruments or other stores of value and payment of a corresponding sum in a cash or other form to a beneficiary by means of a communication, message, transfer or through a clearing network to which the MVTS provider belongs.

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 identity and analyse the threats faced by the State and its financial systems from ML/TF and the financing of the proliferation of weapons of mass destruction encountered by Qatar State and its financial system.

non-profit organisation includes an entity, other than an individual, that primarily engages in raising or distributing funds for charitable, religious, cultural, educational, social, fraternal or similar purposes or carries out other types of charitable or similar acts.

Resident Customer:

(A) National companies and institutions, and Qatari citizens, which are by nature resident accounts.

(B) Foreigners who work within the country on contracts for a year or more.

(C) Branches of foreign companies and institutions licensed to operate inside the country permanently and have economic interests and their foreign workers.

(D) non-profit foreign institutions (other than foreign embassies and consulates, representative offices of international institutions, etc.) who are authorized to conduct business inside the country for more than a year.

(E) The foreign investor who owns a share in a national company, provided that he has a permanent residence in the country.

(F) The branches of foreign airlines and navigation.

Non-resident customer:

(A) foreign embassies and consulates, representative offices of international and regional institutions and their foreign workers, and sponsored by them.

(B) Foreigners who hold a visitor visa for a period of less than a year.

(C) Students who study in national schools and universities and who have come to the country primarily for study.

(D) Foreigners coming to the country for treatment in national or tourist hospitals.

(E) Foreign workers who work inside the country on a seasonal basis for a period not exceeding one year.

(F) Foreign companies licensed by an authority outside Qatar and wholly or partly owned by companies or institutions within Qatar, which do not conduct business inside the country or do business inside the country for a period of less than a year.

(G) Foreign companies operating under special contracts with the government or other residents for less than a year.

ongoing monitoring, in relation to a customer, means:

1) scrutinising transactions under the business relationship, the customer's business and risk profile, sources of income and wealth; and
2) when required—reviewing the records of a financial institution to keep the records up-to-date and relevant.

payable-through accounts are correspondent accounts that are used directly by third parties to transact business on their own behalf.

politically exposed person (PEP) Individuals entrusted to or assigned to prominent public functions in the state, or in a foreign country, such as heads of state, or governments, politicians, high-level government officials, judicial and military officials, and senior executives of state-owned companies, members of parliament and important political party officials, as well as members of senior management from Directors, deputy directors, members of the board of directors or equivalent positions in international organizations.

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

Individuals related to a PEP in the first or second degree include the PEP's father and mother, the PEP's father-in-law or mother-in-law, the PEP's son or daughter, the PEP's stepson or stepdaughter, the PEP's brother or sister, the PEP's brother-in-law or sister-in-law, and the PEP's grandson or granddaughter.

A ***close associate of a PEP*** means a person who is in a partnership with the PEP in a legal or legal arrangement, or is associated with the PEP through a business relationship, or is a beneficial owner of a legal entity or legal arrangement owned or effectively controlled by the PEP.

QCB Law means Law No (13) of 2012 on Qatar Central Bank and the Regulation of Financial Institutions, and includes any implementing regulations made under it.

shell bank means a bank that has no physical presence in the jurisdiction in which it is incorporated and licensed and is not affiliated with a regulated financial institution group that is subject to effective consolidated supervision. Physical presence means presence involving meaningful decision-making and effective management that has the authority to make decisions and not merely the presence of a local agent or low level staff.

State means the State of Qatar.

suspicious transaction report (STR) means a report to a financial institution's MLRO (in these Instructions referred to as ***internal STR***) or a report by the financial institution to the FIU (or its equivalent in another jurisdiction), on any suspicious transaction or suspicion of money laundering or terrorism financing.

terrorist means any natural person who:

(a) commits, or attempts to commit, terrorist acts, wilfully, by any means, either directly or indirectly;

(b) participates as an accomplice in terrorist acts;

(c) organises or directs others to commit terrorist acts; or

(d) contributes to the commission of terrorist acts with a group of persons acting with a common purpose where 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 means the definition mentioned in AML Law

terrorism financing (***TF***) means the definition mentioned in AML Law.

terrorist organisation means a group of terrorists.

4. General provisions

1. Financial institutions licensed by the QCB must apply the QCB Law, the AML/CFT Law and these Instructions, as are appropriate and applicable to them.
2. In case of any breach to theses Instructions, QCB will apply the sanctions stipulated in Article 44 of the AML Law no. 20 of 2019 as well as Articles (210) (216) (217) (218) of QCB Law.

3. In these Instructions, the specification of an amount of money in Qatari Riyals is also taken to specify the equivalent sum in any other currency at the relevant time

5. Key Principles

5.1 Principle One – Responsibility of the Board and Top Management

The Board of a financial institution is responsible for approving the policies, procedures, systems and controls necessary to ensure the effective prevention of ML/TF. The senior management of the financial institution 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 Instructions.

5.2 Principle Two – Risk-based approach

A financial institution must adopt a risk-based approach to the requirements of these Instructions.

5.3 Principle Three – Know your customer

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

5.4 Principle Four – Effective reporting

A financial institution must have effective measures in place to ensure internal and external reporting whenever ML/TF is known or suspected.

5.5 Principle Five – High standard screening and appropriate training

A financial institution must have adequate screening procedures to ensure high standards when appointing or employing officers and employees and must also have an appropriate ongoing AML/CFT training programme for its officers and employees.

5.6 Principle Six – Evidence of compliance

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

6. General responsibilities – AML/CFT

6.1 AML/CFT programmes

(1) A financial institution must develop and update AML/CFT programmes.

(2) The type and extent of measures adopted by a financial institution must have appropriate regard to the risk of ML/TF and the size, complexity and nature of business.

(3) The programmes must include as a minimum:

(a) establishing, developing and managing internal policies, procedures, systems and controls that are commensurate with the risks , volume, nature and complexity of financial institution's businesses to prevent ML/TF and inform all relevant officers and employees of them;

(b) appropriate compliance management arrangements (for example, appointing a designated MLRO and DMLRO at management level);

(c) having timely access to customer identification data, all data related to CDD, transaction records and other relevant AML/CFT information;

(d) adequate screening procedures when appointing and employing officers and employees;

(e) appropriate ongoing training programme for officers and employees;

(f) an adequately resourced and independent audit function to test compliance with the AML/CFT policies, procedures and controls, including sample testing;

(g) ongoing assessment and review of the financial institution's policies, procedures, systems and controls; and

(h) an independent review and testing of the financial institution's compliance with its AML/CFT policies and procedures, systems and controls.

(4) In addition to the risk based approach implementation and periodic update, the appropriate ongoing assessment and review of a financial institution's policies, procedures, systems and controls must as a minimum cover the following :

(a) CDD and ongoing monitoring;

(b) record keeping and retention;

(c) detection of suspicious transactions;

(d) internal and external reporting obligations;

(e) the internal communication of the financial institution's policies, procedures, systems and controls to its officers and employees; and

(f) any other issues that may be required under the AML/CFT Law or these Instructions.

6.2 Requirements for AML/CFT policies

The AML/CFT policies, procedures, systems and controls of a financial institution must be risk-sensitive, appropriate and adequate, and must have regard to the risk of ML/TF and the size, complexity and nature of business.

6.3 Issues covered in AML/CFT policies

A financial institution's AML/CFT policies, procedures, systems and controls must as a minimum:

(a) provide for identification or security of complex or unusually large transactions, unusual transactions that have no clear economic or lawful purpose, and any other transaction that the financial institution suspects to be related to ML/TF;

(b) require enhanced CDD for products and transactions that might favour anonymity for the purpose of ML/TF;

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

(d) provide appropriate measures to reduce the risks associated with establishing a business relationship with a PEP;

(e) require, before any function or activity is outsourced:

(i) assessment and documentation of the ML/TF risk associated with the outsourcing; and

(ii) monitoring of the risks on an ongoing basis;

(f) ensure that there are appropriate systems and measures to enable the financial institution to implement any targeted financial sanction that may be required under Law No (27) of 2019 on Combating Terrorism; and

(g) require all officers and employees of the financial institution to comply with the AML/CFT Law and these Instructions when making STRs.

6.4 Annual assessment and review of policies

1- A financial institution must carry out assessments of the adequacy and effectiveness of its AML/CFT policies, procedures, systems and controls in preventing ML/TF on an annual basis or whenever necessary.

2- A financial institution must make and keep a record of the results of its review and testing and must give the QCB a copy of the record before the end of the first quarter of the ensuing year.

6.5 Application of AML/CFT requirements – officers and employees

(1) A financial institution must ensure that its officers and employees, wherever they are, comply with:

(a) the AML/CFT Law and these Instructions; and

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

(2) The policies, procedures, systems and controls:

(a) must require the officers and employees, wherever they are, to provide the financial institution's MLRO with internal STRs for transactions; and

(b) must provide timely, unrestricted access by the financial institution's Board and MLRO, and by the QCB and FIU, to documents and information of the financial institution, wherever they are held, that relate directly or indirectly to its customers or accounts or to transactions;

(3) A financial institution may apply requirements that impose higher and consistent standards to its AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend over a number of jurisdictions.

(4) If the law of another jurisdiction prevents a provision of this item from applying to an officer or employee, the financial institution must immediately inform the MLRO in the head office. The MLRO must then inform the financial institution's Board.

6.6 Application of AML/CFT requirements – branches and subsidiaries

(1) This item applies to a financial institution if:

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

(b) it has a branch in a foreign jurisdiction; or a subsidiary in a foreign jurisdiction over which it can exercise control.

(2) The financial institution must ensure that the branch or subsidiary, and the officers and employees of the branch or subsidiary, wherever they are, comply with:

(a) the AML/CFT Law and these Instructions; and

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

except so far as the law of another jurisdiction prevents this sub-item from applying.

(3) The policies, procedures, systems and controls:

(a) must require the branch or subsidiary, and its officers and employees, wherever they are, to provide the financial institution's MLRO with STRs for transactions in, from or to this jurisdiction; and

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

except so far as the law of another jurisdiction prevents this sub-item from applying.

(4) A financial institution may apply the requirements that impose higher and consistent standards to its AML/CFT policies, procedures, systems and controls in relation to customers whose transactions or operations extend over a number of jurisdictions.

(5) If the law of another jurisdiction prevents a provision of this item from applying to the branch or subsidiary or any of its officers or employees, the financial institution:

(a) must immediately inform the QCB about the matter; and

(b) must apply additional measures to manage the ML/TF risks (for example, by requiring the branch or subsidiary to give to the financial institution additional information and reports).

(6) If the QCB is not satisfied with the additional measures applied by the financial institution, the QCB may, on its own initiative, apply additional supervisory measures by, for example, directing the financial institution:

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

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

(7) The financial institution must pay particular attention to procedures in branches, or subsidiaries, in jurisdictions that do not apply, or that do not sufficiently apply, FATF recommendations and special recommendations.

6.7 Application of AML/CFT requirements – outsourced activities

(1) This item applies if a financial institution outsources any of its functions or activities to a third party.

(2) The financial institution, and its Board, remain responsible for ensuring that the AML/CFT Law and these Instructions are complied with.

(3) The financial institution 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 AML/CFT Law and these Instructions;

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

(4) The financial institution'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 the financial institution's MLRO with STRs for transactions in, from or to this jurisdiction involving the financial institution (or the third party on the financial institution's behalf); and

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

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

(a) the third party must immediately inform the financial institution about the matter; and

(b) the financial institution must then inform the QCB.

7 Board of Directors

7.1 Overall responsibility of the Board

The Board of the financial institution is responsible for the effectiveness of the policies, procedures, systems and controls in preventing ML/TF.

7.2 Specific responsibilities of the Board

(1) The Board of a financial institution must ensure that:

(a) the financial institution establishes, develops and maintains effective AML/CFT policies, procedures, systems and controls in accordance with the AML/CFT Law and these Instructions;

(b) the financial institution has in place adequate screening procedures to ensure high standards when appointing officers and employees;

(c) the financial institution identifies, designs, delivers and maintains an appropriate ongoing AML/CFT training programmes for its officers and employees and keep records thereof;

(d) the financial institution has an independent and adequately resourced audit function to test compliance with a financial institution's AML/CFT policies, procedures, systems and controls, including sample testing;

(e) regular and timely information is made available to the Board about the management of ML/TF risk;

(f) the financial institution's ML/TF risk management policies and methodology are appropriately documented including their applications by the financial institution;

(g) there is an MLRO designated to attend to the issues of ML/TF who has:

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

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

(iii) sufficient resources, including appropriate staff and technology, to carry out his responsibilities effectively, objectively and independently, and

(iv) timely, unrestricted access to all information of the financial institution that are relevant to AML/CFT which may include CDD, ongoing monitoring, all transactions and all other documents;

(h) a Deputy MLRO is available to carry out the functions without interruption during the absence of the MLRO;

(i) the financial institution has an AML/CFT compliance culture;

(j) that appropriate measures are taken to ensure that ML/TF risks are taken into account in the day-to-day operation of the financial institution, including in relation to:

(i) the development of new products;

(ii) the taking on of new customers; and

(iii) changes in the business profile of the financial institution; and

(k) all reasonable steps have been take so that a report required to be given to the QCB for AML/CFT purposes is accurate, complete and given on a timely manner.

(2) The Board must ensure that the position of the MLRO is never vacant. If the position becomes vacant, the Board must appoint a replacement after obtaining the QCB's approval.

(3) The above responsibilities are indicative and do not limit the Board from putting in place stringent measures to counter ML/TF risks in the financial institution.

8 Money Laundering Reporting Officer (MLRO) and his Deputy

8.1 Appointment

(1) A financial institution must appoint a MLRO who will be responsible for the oversight of countering ML/TF risks at all times, in terms of the AML/CFT Law.

(2) The position of the MLRO may be combined with other similar functions in a financial institution (such as that of the compliance officer) when the size and geographical spread of the financial institution is limited, and the demands are not likely to require a full-time MLRO.

(3) The position of the MLRO must not be combined with other functions that would create a potential conflict of interests.

(4) The position of the MLRO must not be outsourced.

(5) The name and designation of the MLRO and Deputy MLRO must be reported to the AML/CFT Department, under the Supervision and Control Department of the QCB and must be updated when necessary and communicated to QCB and the FIU.

(6) A financial institution must seek the approval of the QCB when appointing and removing a MLRO and a Deputy MLRO, and if either resign from their position.

(7) The Deputy MLRO functions and acts as the MLRO during the absence of the MLRO and while the position of MLRO is vacant. The roles and responsibilities that apply to the MLRO apply to the Deputy as MLRO.

8.2 Eligibility of MLRO

An MLRO of a financial institution who is designated to oversee ML/TF issues must:

(a) be employed at a management level;

(b) have sufficient seniority, knowledge, experience and authority to carry out responsibilities independently;

(c) report directly to the Board of the financial institution; and

(d) be resident in Qatar.

8.3 General responsibilities – MLRO

The MLRO is responsible for:

(a) overviewing the implementation of the financial institution's AML/CFT policies, procedures, systems and controls, including the risk-based approach to ML/TF risks;

(b) ensuring that appropriate policies, procedures, systems and controls are established, developed and maintained across the financial institution:

(i) to monitor day-to-day operations and compliance with the AML/CFT Law, these Instructions, and the financial institution's policies, procedures, systems and controls; and

(ii) to regularly assess and review (at least once a year or when necessary) their effectiveness in relation to preventing ML/TF.

(c) having timely, unrestricted access to all information of a financial institution including information related to customers' transactions, in order to identify, analyse, and monitor transactions effectively;

(d) implementing the financial institution's AML/CFT strategies;

(e) supporting and coordinating the Board's focus on managing a financial institution's ML/TF risks in individual business areas;

(e) ensuring that a financial institution's wider responsibility for preventing ML/TF is addressed centrally; and

(f) promoting an institution-wide view of the need for AML/CFT monitoring and accountability and keeping abreast with the latest international and local AML/CFT developments.

8.4 Specific responsibilities of MLRO

(1) The specific MLRO responsibilities are:

(a) receiving, investigating and assessing the internal STRs of a financial institution;

(b) making STRs to the FIU and informing the QCB about them upon request;

(c) acting as a central point of contact between a financial institution, the FIU, the QCB and other State authorities in relation to AML/ CFT issues;

(d) ensuring prompt response to any request for information by the FIU, QCB, and State authorities in relation to AML/CFT issues;

(e) receiving and acting on the QCB's and international findings about AML/CFT issues;

(f) monitoring appropriateness and effectiveness of a financial institution's AML/CFT training programmes;

(g) reporting to the Board of the financial institution on AML/CFT issues;

(h) exercising all other functions given to the MLRO under the AML/CFT Law, these Instructions or on issues relating to AML/CFT; and

(i) keeping the Deputy MLRO informed of the significant AML/CFT developments (whether internal or external).

(2) The MLRO must execute his responsibilities honestly, reasonably and independently, particularly while receiving, investigating and assessing internal STRs and deciding whether to make an STR to the FIU.

(3) If the QCB issues guidance, the MLRO must bring it to the attention of the financial institution's Board. The financial institution must make and keep a record of:

(a) whether the Board took the guidance into account;

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

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

8.5 MLRO reports to the Board

1. The Board of a financial institution must, on a regular basis, decide what general reports must be given to it by the MLRO, in order to discharge its responsibilities under the AML/CFT Law and these Instructions.
2. At a minimum, the MLRO must give the Board an Annual Report for each fiscal year. The report must be given to enable the Board to consider it within four (4) month.
3. Nothing in this item limits the reports that may be required by the Board or the reports that may be submitted by the MLRO on his own initiative in the discharge of his responsibilities.
4. The MLRO must keep a record of all reports submitted to the board and actions taken on these reports.

8.6 Minimum requirements for MLRO report

(1) The Annual Report must assess the adequacy and effectiveness of a financial institution's AML/CFT policies, procedures, systems and controls in preventing ML/TF.

(2) The Annual Report must include as a minimum:

(a) the number and types of STRs made to the MLRO;

(b) the number of STRs that were passed, or not passed, to the FIU and the reasons why they were passed or not passed;

(c) the number and types of contraventions made by the financial institution of the AML/CFT Law, these Instructions and its policies, procedures, systems and controls;

(d) the areas of, and proposals for, improvement to the financial institution's AML/CFT policies, procedures, systems and controls;

(e) a summary of the training given by the financial institution to their officers and employees;

(f) the areas of, and proposals for, improvement to the financial institution's AML/CFT training programmes;

(g) the number and types of customers who are categorised as high risk;

(h) a summary of the progress in implementing AML/CFT action plans (such as plans resulting from consideration by the Board of the Annual Report, and from assessment and review of the financial institution's training programme and any other issues related to AML/CFT);

(i) outcome of any audit review mandated by the financial institution in relation to AML/CFT policies, procedures, systems and controls;

(j) outcome of any review or assessment of risk, polices, procedures, systems and controls and any risk mitigation policies and procedures.

8.7 Consideration of Annual Reports

(1) The Board of a financial institution must consider the Annual Report made by the MLRO in a timely manner and in no case later than 4 months after the end of the fiscal year to which the report relates.

(2) If the report identifies any deficiencies in the financial institution's compliance with the AML/CFT Law, these Instructions or the financial institution's training programme, the Board must prepare or approve an action plan to remedy the deficiency promptly.

9 Risk-based approach

9.1 Risk assessment – general

(1) A financial institution:

(a) must conduct, at regular and appropriate intervals, and at least once a year, a business risk assessment of the ML/TF risks that it faces including risks identified in the National Risk assessment, sectorial risk assessment and those that may arise from:

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

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

(iii) the technologies that it uses (and proposes to use) to provide those products and services (interface and/or delivery channel risk); and

(iv) jurisdictions where the financial institution have or will conduct transactions with

(b) must develop approporiate policies, procedures and controls to be able to manage the identified risks and decide what action is needed to mitigate those risks as well as moniotor the applicatiohn of such procedures and controls and update them on a regular basis as per the risk assessment results.

(2) The monitoring systems must be configured to identify significant or abnormal transactions or patterns of activity, and must include:

(a) limits on number, types or size of transactions undertaken outside the expected norms; and

(b) limits for cash and non-cash transactions.

9.2 Threat Assessment Methodology

(1) A financial institution must adopt a threat assessment methodology to mitigate the risk of ML/TF that is suitable to the size, business profile and risk profile of the financial institution and approved from the Board.

(2) The financial institution must be able to demonstrate to the QCB that its threat assessment methodology:

(a) is capable of:

(i) assessing the risk profile of the business relationship with each customer;

(ii) identifying the changes in the financial institution's ML/TF risks posed by new products and services introduced by the financial institution in applying new technologies to its services;

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

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

(v) assessing risk posed by new products and services, and new or developing technologies;

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

(c) is designed to enable the financial institution to identity and recognise any changes in its ML/TF risk; and

(d) any changes as may be needed.

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

9.3 Risk Profiling – business relationships

(1) When risk profiling a business relationship with a customer, a financial institution must consider the following risk elements:

(a) customer risk;

(b) product risk;

(c) interface or delivery channel risk;

(d) jurisdiction or geographical area risk.

(2) The financial institution must also assess and identify any other risks that may be relevant to the specific type of business relationship, taking into account the size, complexity and nature of its business in relation to the business of its customers.

(3) The financial institution must determine the intensity of CDD and ongoing monitoring taking into account the risk profile of the business relationship.

10 Customer Risk

10.1 Assessment for customer risk

(1) A financial institution must assess and document the risks of ML/TF, or other illicit activities, posed by different customers.

(2) The intensity of CDD and ongoing monitoring required for a particular type of customer must be proportionate to the perceived or potential level of risk posed by the relationship with the customer.

10.2 Policies and procedures for customer risk

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

(2) The financial institution must conduct enhanced CDD and ongoing monitoring if it suspects that a customer is an individual, charity, non-profit organisation or other entity, regardless of the risk profile of the customer:

(a) that is associated with, or involved in, terrorist acts or TF; or

(b) that is subject to sanctions or other international initiatives relating to AML/CFT.

(3) Any decision to enter into a business relationship with a non-profit organisation or a customer requiring enhanced CDD must only be made after seeking the approval of the Board, or whom they delegate, and only after completing enhanced CDD.

(4) If a financial institution suspects that a customer is involved in TF or is subject to sanctions, the financial institution must not maintain that relationship unless ordered to do so by the appropriate competent authority or law enforcement agency.

10.3 Measures for PEPs

(1) A financial institution must adopt the following measures to reduce the risk associated with establishing and maintaining business relationships with PEPs:

(a) a PEP customer acceptance policy that takes into account the reputational and other risks involved;

(b) clear policies, procedures, systems and controls for establishing business relationships with PEPs;

(c) 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.

(2) The measures must include seeking relevant information from customers, reference to publicly available information, and having access to, and referring to, commercial electronic databases of PEPs.

(3) The financial institution must establish a methodology and reasonable measures to establish the sources of wealth and funds of customers and beneficial owners identified as PEPs.

(4) The financial institution's decision to enter into a business relationship with a PEP must be taken only after approval of the Board, or whom they delegate, and after enhanced CDD has been conducted.

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

(6) In case an existing customer, or the beneficial owner of an existing customer, is subsequently found to be or has become a PEP, the relationship may be continued only with the approval of the Board or whom they delegate.

(7) The financial institution must, on an ongoing basis, check whether the customer is a person listed under a relevant resolution of the UN Security Council or under a Terrorism Designation Order published by the National Counter Terrorism Committee. If the customer is listed, the financial institution must immediately (within 24 hours)inform the QCB, and consider making an STR to the FIU, about the matter.

(8) The financial institution must take measures required by this item in relation to a family member or close associate of a PEP.

10.4 Measures for persons in sanctions list

(1) A financial institution must, from the outset of its dealings, and on an ongoing basis during the business relationship, check whether a person is listed:

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

(b) in a Terrorist Designation Public Prosecutor Order circulated by the National Counter Terrorism Committee.

(2) If the person is listed, the financial institution:

(a) must not establish, or continue, a relationship with, or carry out a transaction with or for, the person and this should be done immediately (within 24 hours);

(b) must make an STR to the FIU; and

(c) must immediately(within 24 hours)inform the QCB.

10.5 Assessment process for legal entities

(1) A financial institution's risk assessment processes and methodology must include recognition of risks posed by legal entities, arrangements and facilities, such as companies, groups, partnership, trusts, nominee shareholdings and powers of attorney.

(2) In assessing the risk posed by legal entities, arrangements and facilities, the financial institution must ensure that the risks posed by beneficial owners, officers, shareholders, trustees, settlors, beneficiaries, managers or any other entities relating to them are reflected in the risk profile of the entity, arrangement or facility.

(3) The risk profile must capture the risks posed by such entities due to reduction in transparency or through an increased ability to conceal the risks.

10.6 Risk mitigation procedures

(1) A financial institution must conduct, at regular and appropriate intervals (at least once a year) an assessment of the ML/TF risks that it faces, including risks identified in the National Risk Assessment and those that may arise from:

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

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

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

(d) the jurisdictions with which its customers are (or may become) associated (***jurisdiction risk***).

(2) The financial institution 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 financial institution fails to take into account the National Risk Assessment or sectorial risk assessment and / or 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 QCB.

10.7 Powers of Attorney

(1) These Instructions apply to a power of attorney if it authorises the holder to exercise control over assets of the grantor.

(2) The holder and the grantor are both taken to be customers of a financial institution.

(3) The financial institution must conduct CDD for the holder and the grantor before getting involved in, or associating with, any transaction involving the power of attorney.

11 Product and service risk

11.1 Assessment of product and service risk

(1) A financial institution must assess and document the risks of ML/TF and other illicit activities posed by the type of products and services it offers and proposes to offer to its customers (such as savings accounts, e-money products, payable-through accounts and MVTS).

(2) The intensity of CDD and ongoing monitoring for each type of product and service must be commensurate with and proportional to the perceived and potential risk that may be posed by each type of product or a service.

11.2 Policies for product and service risk

(1) A financial institution must have policies, procedures, systems and controls to address specific risks of ML/ TF and other illicit activities posed by different types of products and services offered by the financial institution and that it proposes to offer to its customers.

(2) The financial institution must include in its methodology the basis on which business relationships with customers will be scored based on the different types of products it offers (and proposes to offer).

11.3 Products and services with fictitious, false or no names

A financial institution must not permit any of its products or services to be used if the product or the service:

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

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

(c) is not used for the intended purpose (for example using personal account for commercial purposes)

11.4 Correspondent banking relationships

(1) Before establishing a correspondent banking relationship with a financial institution in a foreign jurisdiction (the ***respondent***) a financial institution (the ***correspondent***) must undertake:

(a) to decide from publicly available information the respondent's reputation and the quality of its regulation and supervision;

(b) to gather (using a structured questionnaire or by other means) all information on the respondent to understand the nature of its business;

(c) to gather information about the respondent's ownership structure and management;

(d) to gather information on major business activities of the respondent (and any parent company) and whether it is located in a FATF-compliant jurisdiction;

(e) to determine the purpose of opening the account;

(f) to assess the respondent's AML/CFT policies, procedures, systems and controls to ensure that they are adequate and effective;

(g) to document the respective responsibilities of the respondent and correspondent, including those in relation to AML/CFT matters; and

(h) to obtain the approval of the Board to establish a correspondent banking relationship.

(2) Before establishing a business relationship, the correspondent must also consider:

(a) whether the respondent has been or is subject of any investigation or civil or criminal proceeding relating to ML/TF;

(b) the financial position of the respondent and ensure that Board members and Executives are not listed on any international sanctions list ;

(c) whether the respondent is regulated and supervised in its home jurisdiction by a regulatory or governmental authority, body or agency equivalent to the QCB; and

(d) whether the jurisdiction in which the respondent is operating has an effective AML/CFT regime.

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

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

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

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

(4) If the respondent is a subsidiary of another legal entity, the correspondent must seek information about:

(a) the other entity's domicile and location (if different);

(b) its reputation;

(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 QCB in each jurisdiction in which it operates;

(d) whether each foreign jurisdiction in which it operates has an effective AML/CFT regime; and

(e) its ownership, control and management structure (including whether it is owned, controlled or managed by a PEP).

(5) If the respondent is operating in a high risk jurisdiction, the correspondent must conduct enhanced ongoing monitoring on the transactions conducted under the relationship and must review the relationship on an annual basis.

(6) The additional measures to be taken by each financial institution before opening a correspondent banking relationship must include a signed agreement that outlines the respective responsibilities and obligations of each institution in relation to ML/TF detection and monitoring responsibilities.

(7) The correspondent must have and take appropriate policies and procedures in case a financial institution is listed on an international sancitons list and/or have been subject to any regulatory action as a result of any weaknesses in the AML/CFT regime.

11.5 Shell banks

(1) A financial institution must not establish or continue business relationships with banks which have no physical presence or "mind and management" in the jurisdiction in which they are licensed and which are not affiliated with a regulated financial group subject to effective consolidated supervision.

(2) A financial institution must make an STR to the FIU if the financial institution is approached by a shell bank or any institution that the financial institution has reason to suspect is a shell bank.

(3) A financial institution must not enter into or continue a business relationship with a respondent financial institution in a foreign jurisdiction if it permits its accounts to be used by banks registered in jurisdictions where they are not physically present and are not affiliated with a regulated financial group subject to effective consolidated supervision.

11.6 Payable-through accounts

(1) This item applies if:

(a) a financial institution (the ***correspondent***) has a correspondent banking relationship with a 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 correspondent may have direct access to an account of the correspondent.

(2) Whenever a correspondent relationship involves the maintenance of payable-through accounts, the correspondent must ensure:

(a) that the respondent has performed all normal CDD obligations on those of its customers who have direct access to the accounts of the correspondent;

(b) that the respondent conducts ongoing monitoring in relation to each such customer; and

(c) that the respondent will be able to provide to the correspondent relevant customer identification information upon request and that the customer is not high risk or suspicious .

(3) If the correspondent asks for documents, data or information under paragraph (2) (c) and the respondent fails to comply with the request, the correspondent must terminate the customer's access to the accounts of the correspondent and consider making an STR to the FIU.

11.7 Bearer negotiable instruments

(1) ***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 and money order that is in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title to it passes upon delivery;

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

(d) a bearer share; or

(e) a share warrant to bearer.

(2) A financial institution must have adequate AML/CFT CDD policies, procedures, systems and controls for risks related to the use of bearer negotiable instruments.

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

(4) The holder and any beneficial owner are taken to be customers of the financial institution.

11.8 Non-profit organisations

(1) A financial institution must not offer any financial services to non-profit organisations, unless the financial institution:

(a) obtains all details on all customer identification data such as the name of the association or society, legal form, address of head office and branches, types of activities, date of establishment, names and nationalities of representatives authorised to access the account, contact details, purpose of the business relationship, sources and uses of funds, approval of appropriate competent authority for opening the account at the financial institution, and any other information required by the competent authority;

(b) verifies the presence and legal form of the society or the association through information contained in its official documents; and

(c) obtains supporting documents indicating the presence of an authorisation issued by the association or the society to the persons authorised to access the account, and

(d) identifies those persons authorised to access the account in accordance with the customer identification measures in these Instructions.

12 Interface or delivery channel risk

12.1 Assessment for interface risk

(1) A financial institution must assess and document the risks of ML/TF and other illicit activities posed by the mechanisms, electronic banking operations, and other operations undertaken electronically or in a similar way, through which business relationships are started, conducted and maintained as well as before introducing any product or service or use of a new technology while taking appropriate measuers to manage and reduce any risks involved.

(2) The intensity of the CDD and ongoing monitoring in relation to a particular interface must be appropriate and proportionate to the perceived and potential level of risk that may be posed by that interface.

12.2 Policies and procedures for interface risk

(1) A financial institution must have policies, procedures, systems and controls to address specific risks of ML/TF, or other illicit activities, posed by the different types of interface and technological developments through which business relationships are started, conducted and maintained. This must be done also before offering any new service or a product or new technology while setting the appropriate risk mitigation policies, procedures and controls.

(2) The policies, procedures, systems and controls must include measures:

(a) to prevent misuse of technological developments in ML/TF schemes; and

(b) to manage specific risks associated with non-face-to-face business relationship transactions.

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

(4) The financial institution must include in its methodology how the customers will be scored in relation to the interface through which the business is started, conducted and maintained.

12.3 Non-face-to-face business relationships and new technologies

(1) Non-face-to-face business relationships or transactions are:

(a) those types of relationships or transactions concluded over the internet, or other means of technological development;

(b) services or transactions provided or conducted over the internet, through the use of ATMs and other similar means; and

(c) electronic point of sale (POS) using prepaid (re-loadable) or account link cards.

(2) The policies, procedures, systems and controls for the relationships or transactions mentioned in sub-item (1) must include seeking additional identification documents, applying supplementary measures to verify documents supplied, and developing independent contacts.

(3) A financial institution must have specific and effective due diligence procedures that can be applied to non-face-to-face customers. In particular, the financial institution must have measures to ensure that the customer is the same person as claimed to be and also ensure that the address provided is genuinely that of the customer.

(4) The measures may include, but are not limited, to:

(a) contacting the customer on an independently verified home, employment or business number;

(b) contacting, with the customer's consent, the employer to confirm employment; and

(c) procuring the customer's salary details through official channels or similar means.

(5) The financial institution permitting payment processing through on-line services must ensure that monitoring is the same as for its other services and that it has a risk-based methodology to assess ML/TF risks of such services.

(6) The financial institution must refer to the instructions issued to them by QCB from time to time with regard to Modern Technology and E-Banking Risks, and must comply with any e-banking regulations issued by QCB.

12.4 Reliance on third parties

(1) A financial institution may rely on introducers, intermediaries or other third parties to conduct some elements of CDD for a customer, or to introduce business to the financial institution, if it does so under, and in accordance with, the AML/CFT Law and these Instructions. However, the financial institution (and, in particular, its Board) remains responsible for the proper conduct of CDD and ongoing monitoring for its customers.

(2) In determining whether to rely on a third party, the financial institution must have regard to any relevant findings published by international organisations, governments and other bodies about the jurisdiction where the third party is located.

12.5 Introducers

(1) This item applies in relation to a customer introduced to a financial institution by a third party (the ***introducer***) if:

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

(b) the financial institution is satisfied that the introducer:

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

(ii) is subject to the AML/CFT Law and these Instructions 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 financial institution from obtaining any information or original documentation about the customer that the financial institution may need for AML and CFT purposes.

(2) The financial institution 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, a financial institution must not start a business relationship with the customer relying on sub-item (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.

12.6 Group introductions

(1) These Instructions apply in relation to a customer introduced to a financial institution in Qatar (the ***local financial institution***) by another financial institution in the same group (the ***introducer***), whether in or outside Qatar, if:

(a) the introducer or another financial institution in the group (either of whom being referred to in this item as the ***relevant financial institution)*** has conducted CDD for the customer; and

(b) the local financial institution is satisfied that all of the following conditions have been met:

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

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

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

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

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

(2) The local financial institution need not satisfy itself that all of the conditions in paragraph (1) (b) have been met if the QCB (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 Instructions;

(b) the group's implementation of the programme and compliance with the requirements are subject to effective consolidated supervision by the QCB 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.

12.7 Intermediaries

(1) This item applies to a financial institution in relation to a customer of an intermediary, wherever located, if the customer is introduced to the financial institution by the intermediary.

Example of intermediary

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

(2) The financial institution may treat the intermediary as its customer, and need not conduct CDD itself for the intermediary's customer, if the financial institution 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 QCB or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction;

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

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

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

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

13 Jurisdiction risk

13.1 Assessment for jurisdiction risk

(1) A financial institution must assess and document the risks of involvement in ML/TF and other illicit activities posed by different jurisdictions with which its customers are associated or may become associated. This includes where the customer lives, or where the business is incorporated, or otherwise established, in a foreign jurisdiction.

(2) The intensity of CDD and ongoing monitoring required for customers in other jurisdictions must be proportionate to the perceived or potential risk posed by the respective jurisdictions.

(3) Jurisdictions requiring enhanced CDD include:

(a) jurisdictions with ineffective AML/CFT regimes;

(b) jurisdictions with impaired international cooperation;

(c) jurisdictions listed as non-cooperative by FATF;

(d) jurisdictions subject to international sanctions; and

(e) jurisdictions with high propensity for corruption.

(4) A financial institution must have policies, procedures, systems and controls to address the specific risks of ML/TF and other illicit activities posed by different jurisdictions with which, or to which the customers of, the financial institution may be associated.

(5) The financial institution must include in its methodology the basis on which business relationships with customers will be scored, having regard to the types of jurisdictions with which customers are or may be associated.

13.2 Effectiveness of AML/CFT regimes

(1) When assessing the effectiveness of AML/CFT regimes in other jurisdictions, a financial institution must consider:

(a) legal framework;

(b) enforcement and supervision mechanism; and

(c) international cooperation.

(2) For sub-item (1), the financial institution must consult publications of international organisations, governments and other bodies such as FATF.

13.3 Non-cooperative or sanctioned jurisdictions

A financial institution must conduct enhanced CDD and enhanced ongoing monitoring in relation to transactions or business relationships arising from jurisdictions identified by FATF as having strategic deficencies, or jurisdictions subject to international sanctions. Counter and /or preventative measures should be applied and commensurate with the risks, sanction level or weaknesses.

13.4 Jurisdictions with high propensity for corruption

(1) A financial institution must have in place a methodology to assess and document jurisdictions that are vulnerable to corruption.

(2) The financial institution must conduct enhanced CDD and enhance ongoing monitoring for customers from high risk jurisdictions whose lines of business are vulnerable to corruption.

(3) If the financial institution's policy permits the acceptance of PEPs as customers, the financial institution must take additional measurers to mitigate the additional risk posed by PEPs from jurisdictions with high propensity for corruption.

Without prejedice to any of the abovementioned instructions, financial institutions should comply with the Guidance paper issued by QCB on July 2018 on the risk based approach and any other updates thereof.

14 Know your customers

14.1 General principle of KYC

The know your customer (***KYC***) principle requires that every financial institution know who its customers are, by having the necessary identification documents, and other relevant information including the physical presence of the customer upon commencing the business relationship.

14.2 Customer acceptance policy

(1) A financial institution must develop a clear customer acceptance policy taking into consideration all factors related to customers, their activities and accounts and any other indicators associated with customer risk.

(2) The policy must include a detailed description of:

(a) the types of customers according to their degrees of risk;

(b) the basis on which business relationships with customers will be scored taking into account the sources of their wealth and funds; and

(c) when persons are regarded as occasional customers seeking to carry out one-off transactions.

(3) The policy must include effective systems and internal procedures for establishing and verifying the identity of the financial institution's customers and the sources of their wealth and funds.

(4) The policy must be in writing and approved by the financial institution's Board.

14.3 Customer due diligence requirments

(1) Customer due diligence (***CDD***), in relation to a customer of a financial institution, is all of the following measures:

(a) identifying the customer and obtaining a acknowledgement from the customer that he/she will update his/her information as soon as it happens or upon request from the bank ;

(b) verifying the customer's identify 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) and obtaining an acknowledgment that the customer is the ultimate beneficial owner;

(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.

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

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

(b) identifying the principal; and

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

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

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

(b) identifying the agent;

(c) verifying the agent'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 the agent is a beneficial owner.

(4) If the customer is a legal entity 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) Examples of the measures required to determine the ultimately ownership or control of a customer 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

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

(6) The financial institution must verify the identity of the legal entity using reliable, independent source documents, data or information that show:

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

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

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

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

14.4 Timing and requirements of CDD

(1) The financial institution must conduct CDD when:

(a) establishing a business relationship with a new customer;

(b) there is a change to the signatory or the beneficiary of an existing account or business relationship;

(c) a significant transaction is made;

(d) there are material changes in the way the account with the financial institution is operated or in the manner of conducting business relationships;

(e) the documentation standards changes substantially;

(f) the financial institution has doubts about the veracity or adequacy of previously obtained CDD information or documents;

(g) carrying out a one-off transaction for a customer with a value of at least QR 50,000;

(h) carrying out for a customer a series of one-off transactions that are or appear (whether at the time or later) to be linked and with a total value of at least QR 50,000;

(i) carrying out MVTS above QR 3,500; and

(j) there is a suspicion of ML/TF.

(2) A financial institution must not establish a business relationship with a customer unless:

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

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

(3) Once the relationship has been established, the regular business undertaken by the customer must be assessed at regular intervals against expected patterns of business activity.

(4) Any unexpected activity must be examined to decide whether any suspicions arise in relation to ML/TF. In order to assess unexpected activities, the financial institution must obtain and maintain information on:

(a) the nature of the business likely to be undertaken;

(b) the pattern of transactions;

(c) the purpose and reason for opening the account;

(d) the nature and level of activity; and

(e) the signatories of the account.

(5) A financial institution must conduct CDD if it has any doubt about the genuineness of the accuracy or adequacy of any customer identification obtained earlier.

(6) A financial institution must conduct CDD if it suspects the customer of ML/TF.

14.5 General requirements on CDD

(1) A financial institution must decide the extent of CDD for a customer on a risk-sensitive basis depending on customer risk, product risk, interface or delivery channel risk and jurisdiction risk, among other factors.

(2) The financial institution must be in a position to demonstrate to the QCB that the extent of CDD is appropriate and proportional to the risk of ML/TF.

14.6 Extent of CDD—legal entities and arrangements

(1) This item applies if a financial institution is required to conduct CDD for a legal entity or a legal arrangement.

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

(3) However, if the CDD is required to be conducted for a legal arrangement and the beneficiaries and their contributions have already been decided, the financial

institution must identify each beneficiary who is to receive at least 20% of the funds of the arrangement (by value).

14.7 CDD for beneficiaries of life insurance policies—general

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

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

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

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

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

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

14.8 CDD for PEPs as beneficiaries of life insurance policies

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

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

(a) inform its senior management;

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

(c) make an STR to the FIU.

14.9 CDD in later stage cases

(1) Verification of identity for CDD purposes can be completed at a later stage in accordance with the AML/CFT Law if:

(a) this is necessary in order not to interrupt the normal conduct of business;

(b) there is little risk of ML/TF and any risks are effectively managed;

(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.

(2) A financial institution 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 required, the financial institution must justify to the QCB that the delay in conducting the CDD is necessary so as not to interrupt the normal conduct of business or for any other reasons if any.

14.10 Incompleted CDD

If a financial institution is unable to complete CDD for a customer, it:

(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 must make an STR to the FIU.

(d) keep separate records of the customers where they were unable to establish the business relationship with and the reasons thereof.

14.11 General requirements of ongoing monitoring

(1) A financial institution must, for each of its customers, conduct ongoing monitoring consisting of:

(a) scrutinising transactions conducted under the business relationship with the customer to ensure that the transactions are consistent with the financial institution'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 financial institution's records of the customer to ensure that documents, data and information collected during CDD and ongoing monitoring for the customer are kept up-to-date and relevant.

(2) A financial institution must pay particular attention to all complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

(3) A financial institution must examine the background and purpose of such transactions and record its findings. The records must be maintained in accordance with section 22 (on documents, record keeping and retention).

(4) A financial institution must have policies, procedures, systems and controls for conducting ongoing monitoring. Systems and controls must include flagging of transactions for further examination.

(5) Any further examination may be performed by a senior independent officer of the financial institution, and appropriate follow-up action must be taken on the findings of such examination. In case of knowledge or suspicion of ML/ TF raised by such examination, a report by the senior officer must be made to the MLRO.

(6) The system for ongoing monitoring must have the ability to review transactions in real time, as they take place.

(7) The ongoing monitoring may be by reference to a particular type of transaction or related to a customer's risk profile; or by comparing the transactions of the particular customer or the risk profile of the particular customer with that of his

peers or similar customers; or a combination of these approaches. A financial institution may not limit the approaches as given here and may use stringent ongoing monitoring processes.

14.12 Monitoring of one-off linked transactions

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

(2) The financial institution must make an STR to the FIU if the it knows, or suspects, or has reasonable grounds to know or suspect, that a series of one-off transactions:

(a) are linked and intended to circumvent the QR 50,000 threshold for CDD; or

(b) otherwise involves ML/TF.

15 Customer identification documentation

15.1 General requirements for customer identification

(1) A financial institution must ensure that the customer identification documentation relates to the customer and the nature of the customer's economic activity.

(2) A financial institution must make and keep a record of all customer identification documentation that is obtained during CDD and ongoing monitoring of the customer's business relationship.

(3) A financial institution must make and keep a record of how and when each of the steps of CDD for a customer was satisfactorily completed. This must be applied in relation to a customer irrespective of the nature and risk profile of the customer.

(4) To mitigate the risks associated with ML/TF from using the business relationship and mixing proceeds of crime with proceeds of legitimate economic activity in order to disguise their origin, the financial institution must:

(a) identify sources of customer's income and wealth and establish that such sources are not from criminal activity; and

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

(5) The financial institution must identify the matters in sub-item (4):

(a) to establish customer and jurisdiction risks, and monitor the transactions in real time; and

(b) to ensure that the transactions correspond to the transactions intended under the business relationship.

(6) If an assessment identifies differences between the actual transactions conducted under the business relationship and the stated purpose and intended nature:

(a) the financial institution must ensure and satisfy itself that they are not intended for ML/TF purposes; and

(b) if the financial institution is not satisfied about the variation in the intended transactions, the financial institution must consider making an STR to the FIU.

(7) The financial institution must maintain the documents set out as the minimum requirements for the types of customers in items 15.2 to 15.5.

15.2 Customer identification – individuals

For individuals, customer identification data must include the customer's full name, other aliases, permanent address, contact details, profession, work address and

location, nationality, ID number for Qataris and residents, passport number for non-residents[1], date and place of birth, name and address of sponsor, purpose of the business relationship, and names and nationalities of representatives authorised to access the account. Financial institutions should verify the above data through the following:

- confirming the identity of the customer or the beneficial owner from a valid official document (eg. National identification card, passport, driver's licence)
- confirming the date and place of birth from an official document (eg birth certificate, passport, identity card);
- confirming the residential address (eg utility bill, , bank statement, letter from a public authority).
- contacting the customer by telephone or by letter to confirm the information provided, after an account has been opened (eg a disconnected phone, returned mail etc should warrant further investigation);
- confirming the validity of official documentation provided through certification by an authorised person (eg embassy official, public notary);

15.3 Customer identification – legal entities

(1) For legal entities, customer identification data must include the legal entity's name, CR data, type of activity, date and place of establishment, certified copies thereof, capital, names and nationalities of authorised signatories, names of the authorised persons , contact details, address, purpose of the business relationship, and expected size of business and names persons holding top management positions.

(2) The data must include the legal form of the legal entity and:

(a) for an individual institution—the name and address of the institution's owner;

(b) for a joint venture—the names and addresses of the joint partners; and

(c) for a joint stock company—the names and address of the shareholders whose shares exceed 10% of the company's capital.

(3) If the legal entity has a multi-layered ownership and control structure, the financial institution must obtain, and document, the ownership and control structure at each level.

(4) If the legal entity is an unincorporated partnership or association, the identity of all partners or directors must be obtained and verified.

(5) In the legal entity is a partnership with a formal partnership agreement, the financial institution must obtain from the partnership the mandates:

(a) authorising the establishment of the business relationship with the financial institution; and

(b) authorising persons to act on behalf of the partnership (including by operating any accounts).

(6) Financial institutions must verify the identity of the legal persons established though informantion mentioned above the following and as deemed necessary:

[1] Unless for other persons stipulated as per any circular issued by QCB or any future cirulars

- for established legal persons – reviewing a copy of the latest financial statements (audited, if available).
- undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated
- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (eg lawyers, accountants);
- obtaining prior bank references;
- visiting the legal person, where practical;
- contacting the legal person by telephone, mail or e-mail

15.4 Customer identification – legal arrangements

(1) For legal arrangements, a financial institution must obtain:

(a) the arrangement's full name;

(b) the nature and purpose of the arrangement (for example, whether discretionary, testamentary or bare);

(c) the jurisdiction where the arrangement was established;

(d) the identities of the parties to the arrangement (such as the settlor, trustee, protector and beneficiary in the case of a trust); and

(e) the beneficial owner(s) of the arrangement.

(2) The financial institution must verify the identity of the legal arrangement using reliable, independent source documents, data or information that show:

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

(b) the terms of the arrangement.

(3) The financial institution 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.

(4) The financial institution:

(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.

15.5 Customer identification – clubs and societies and NPOs

For clubs, societies and NPOs, a financial institution must obtain, and document, the information required under items 15.1 to 15.3 insofar as they apply to the customer.

16 Enhanced CDD and ongoing monitoring

16.1 Scope of enhanced CDD and ongoing monitoring

A financial institution 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 Instructions and the Guidances;

(b) if required by the QCB or the NAMLTF Committee or the QFIU;

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

(d) in any other case that by its nature can present a higher risk of ML/TF.

16.2 Cases of Conducting enhanced CDD and ongoing monitoring

(1) Enhanced CDD and ongoing monitoring must be conducted in relation to:

(a) non-face-to-face business and new technologies;

(b) politically exposed persons;

(c) correspondent banking relationships;

(d) bearer negotiable instruments;

(e) clubs, societies and NPOs; and

(f) jurisdiction risks (from impaired international cooperation, non-cooperative or sanctioned or high risk jurisdictions and jurisdictions with high propensity for corruption and known for criminal activities such as drug trafficking);

(g) interface or delivery channel risks;

(h) third party reliance for CDD; and

(i) private banking services.

(2) The financial institution must pay particular attention to any transaction with an entity or person who is domiciled in a jurisdiction that has been identified by FATF as non-cooperative and/or having strategic deficiencies. The background and purpose of a transaction with the entity or person must be re-examined if the transaction has no apparent or visible economic or lawful purpose.

(3) When conducting enhanced CDD in relation to private banking services, a financial institution must take into consideration:

(a) the nature of the services;

(b) the purpose of the application for private banking; and

(c) the development of the business relationship.

(4) The financial institution must conduct enhanced CDD on non-resident customers and develop internal monitoring systems commensurate with the risks anticipated with relationship and prepare a regular reports on such category including a classification and analysis as to their jurisdiction whether by residency or nationality. The following measures must be included as a minimum during customer identification:

(a) identify the purpose of the business relationship;

(b) verify the validity of the entry visa initially while initiating business relationship;

(c) obtain a copy of the passport;

(d) in the case of a legal entity, obtain a copy of the memorandum of association certified by the competent authorities in the country of origin or the embassy of country of origin in Qatar;

(e) obtain a copy of the commercial registration or registration documents certified by the competent authorities in the country of origin or the embassy of the country of origin in Qatar.

(5) The financial institution, in all cases, must document its findings on the re-examination and make an STR to the FIU if it has reason to suspect that the transaction involves ML/TF.

16.3 Requirements for conducting enhanced CDD and ongoing monitoring

A financial institution 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 QCB or by an equivalent regulatory or governmental authority, body or agency in another jurisdiction.

16.4 Measures in addition to enhanced CDD and ongoing monitoring

(1) In addition to the enhanced CDD and enhanced ongoing monitoring, a financial institution must conduct, on a risk-sensitive basis:

(a) countermeasures proportionate to the risks specified in circulars published by QCB or upon recommendation of 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 motion.

17 Simplified CDD

17.1 Customers with low level of risk

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

(a) the verification of the identity of the customer or beneficial owner after (rather than before) the business relationship has been established;

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

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

(d) not collecting information, or not carrying out of 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.

(2) The financial institution may conduct simplified CDD on Ministries, Government Authorities and semi-government companies in the GCC countries.

(3) A financial institution wishing to apply simplified CDD on the above customers must retain documentary evidence supporting its categorisation of the customer.

17.2 Listed, regulated public companies

A financial institution may conduct simplified CDD for a customer if the customer is a public company whose securities are listed on a regulated financial market that subjects public companies to disclosure obligations consistent with international standards of disclosure.

17.3 Certain life insurance contracts

A financial institution may conduct simplified CDD for a customer in relation to an insurance contract if:

(a) either:

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

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

(b) the contract is in writing;

(c) the beneficiary is not anonymous;

(d) the nature of the contract allows for timely CDD if there is a suspicion of ML/TF; and

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

17.4 Simplified ongoing monitoring

1- A financial institution may conduct simplified 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 financial institution, of the intensity, extent and frequency of:

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

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

2- Without prejedice to any of the abovementioned instructions, financial institutions should comply with the Guidance paper issued by QCB on July 2018 on the customer due diligence and beneficial ownership and any other updates thereof.

18 Money and value transfer services and wire transfers

(1) This item applies to an MVTS including wire transfer conducted by an MVTS provider or a financial institution (the ***ordering***) on behalf of a person (the ***originator***) with a view to making money or value available to a person (the ***recipient***) at another MVTS provider or a financial institution (the ***beneficiary)***.

(2) This item applies to an MVTS and/or a FI whether or not:

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

(b) the MVTS or the FI is conducted through an agent for an MVTS provider and/ or FI; or

(c) the ordering provider or FI, the beneficiary provider or any such agent is outside Qatar.

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

(a) the card number accompanies all transfers flowing from the transaction (such as withdrawals from a bank account through an ATM, cash advances from a credit card and payments for goods and services); and

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

(4) Also, this rule does not apply:

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

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

(5) If the ordering provider or financial institution and the beneficiary MTV or FIs and all customers of the MTV and/or the FI are in Qatar, the ordering provider or FI must accompany all information as well as conducting all CDD for the originator and recipient. However, full originator information need not accompany the transfer, with the exception of the name of the originator, the name of the recepiant, and an account number for each, or a unique transaction reference when:

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

(b) provided that the following condictions be met

i. All information on the originator and recipient are provided to the beneficiary FI or MTV, QCB, FIU within three days after request

ii. All information are provided to Law Enforcement Authorities immediately and upon request.

(6) If the ordering provider is in Qatar and the beneficiary provider or any agent is outside Qatar, the ordering provider must include full originator information and full recipient information in a message or payment form accompanying the transfer.

(7 If a beneficiary provider or FI is in Qatar and is aware that full originator information or full recipient information has not been provided in a message or payment form accompanying the transfer (and is not fully traceable using a batch file mentioned in the above sub-item , the beneficiary provider must:

(a) either

i. reject the transfer or

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

(b) using a risk-sensitive approach, decide whether an STR must be made to the FIU.

(8) If an ordering provider or FI has regularly failed to provide the required information about the originators or recipients of transactions and the beneficiary provider or FI is in Qatar, the beneficiary provider or a FI:

(a) must take appropriate steps (such as issuing warnings and setting deadlines for the provision of information, rejecting any future transfers from the ordering provider, and restricting or terminating any business relationship with the ordering provider) to ensure that the ordering provider does not contravene these Instructions; and

(b) must report the matter to the FIU when appropriate.

(9) It is prohibited that any transaction with any value be conducted through any MVTS or FI whether the originator and / or recipient is a person listed:

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

(b) in national sanctions lists published by the National Counter Terrorism Committee as per the Public Prosecutor order.

(10) It is prohibited that any transaction with any value be conducted through any MVTS or FI for charitable causes without getting previous approval and completing all requirments from the relevant authority.

(11) An agent for an MVTS provider or for a FI in a cross-border MVTS, and the beneficiary provider of FI that makes money available to the recipient after the cross-border MVTS, must take reasonable measures, on a risk-sensitive basis, to identify transfers to this jurisdiction that lack full originator information or full recipient information. The measures may include following-up (whether during, or after, the transfer) on information that is lacking about the originator or recipient

(12) An agent or beneficiary for an MVTS provider or FI must, using a risk-based approach, develop, establish and maintain policies, procedures, systems and controls to determine:

(a) when to execute, reject or suspend an MVTS or FI that lacks the full originator information or full recipient information; and

(b) when to take appropriate follow-up action

(13) An agent for an MVTS provider or for a FI in a cross-border transfer must ensure that all originator and recipient information accompanying the transfer is retained with it which are received in the form and are provided to the beneficiary financial institution.

(14) An MVTS provider or FI must keep full originator information and full recipient information for at least 10 years after:

(a) the day where the provider acted as ordering provider—the day the originator asked the financial institution to make the MVTS;

(b) the day where the provider acted as agent for another MVTS provider—the day the provider transmitted the information to another agent or to the beneficiary provider; or

(c) the day where the provider acted as beneficiary provider—the day the money received via MVTS is made available to the recipient.

(15) If an MVTS provider or FI is both ordering and beneficiary provider of an MVTS, or if a FI controls both the originator and the recipient of an MVTS, the MVTS provider and / or FI must take into account the information obtained from both sides of the transfer and consider whether to make an STR or not. If the MVTS provider suspects that the transfer may involve ML/TF, it must:

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

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

(16) For transfer of more than QR 3,500, the beneficiary provider must verify the identity of the recipient before making money available, unless the recipient's identity has previously been verified.

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

(18) To avoid increased ML/TF risks, the ordering provider or financial institution must ensure that non-routine transfers are not batched.

19 Reporting requirements

19.1 General reporting requirements

(1) A transaction that is unusual or inconsistent when compared to a customer's known legitimate business and risk profile is not by itself suspicious. To decide whether a transaction is suspicious, a financial institution must consider:

(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 transactions is not similar to the earlier size or pattern of the same or similar customer;

(d) whether the customer has failed to furnish adequate explanation or information on the transaction;

(e) whether the transaction is made from a newly established business relationship or is a one-off transaction;

(f) whether the transaction involves the use of off-shore accounts or companies that are not supported by the economic needs of the customer; and

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

(2) The list in sub-item (1) is indicative, and the financial institution may consider other relevant matters to assess whether a transaction is suspicious with a special attention to QFIU guidances.

19.2 Internal reporting requirements

(1) A financial institution must have clear and effective policies, procedures, systems and controls for internal reporting of the known or suspected instances of ML/TF.

(2) The policies, procedures, systems and controls for internal reporting must enable the financial institution to comply with the AML/CFT Law, these Instructions and also enable prompt making of internal STRs to the MLRO.

(3) The financial institution must ensure that all officers and employees have direct access to the financial institution's MLRO and that the reporting lines between the officers and employees and the MLRO are short.

(4) All officers and employees of a financial institution must immediately make an STR if they have reasonable grounds to suspect that funds channelled through the financial institution:

(a) are proceeds of crime;

(b) are related to TF;

(c) are linked or related to, or are to be used by, a terrorist organisation; or

(d) are linked or related to, or are to be used for, terrorism or terrorist acts.

(5) The officers and employees of a financial institution must promptly make an internal STR to the MLRO. On making the internal STR, the officers and employees must promptly report all subsequent transactions details of the customer for the period required by the MLRO.

(6) Internal STRs to the MLRO must be made irrespective of amount of the transaction.

(7) The MLRO must prepare strategic analysis reports that includes analysis for all techniques, typologies , and methods included in STRs

19.3 Obligation of the MLRO on receipt of internal STR

If the MLRO of a financial institution receives an internal STR, the MLRO must promptly:

(a) if a financial institution'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 section 20 (on tipping-off);

(c) consider the report in the light of all other relevant information held by the financial institution about the 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.

19.4 External reporting requirements

(1) A financial institution must have clear and effective policies, procedures, systems and controls for reporting all known or suspected instances of ML/TF to the FIU.

(2) The policies, procedures, systems and controls must comply with the AML/CFT Law and these Instructions in relation to:

(a) making STRs to the FIU promptly and speedily; and

(b) cooperating effectively with the FIU and law enforcement agencies in relation to STRs made to the FIU.

19.5 Obligation of financial institutions to report to FIU

(1) If a financial institution is aware, suspects or has reasonable grounds to know or suspect that funds:

(a) are proceeds of crime;

(b) are related to TF;

(c) are linked or related to, or are to be used by, a terrorist organisation; or

(d) are linked or related to, or are to be used for, terrorism or terrorist acts;

the financial institution must immediately make an STR to the FIU and ensure that any future or proposed transaction relating to the STR does not proceed without consultation with the FIU.

(2) The STR must be made by the MLRO or Deputy MLRO of the financial institution.

(3) The financial institution must make the STR to the FIU:

(a) whether or not an internal STR has been made;

(b) irrespective of the amount of the transaction;

(c) whether or not any transaction involves tax matters; and

(d) even though:

(i) no transaction has been, or will be, conducted by the financial institution;

(ii) no business relationship has been, or will be, entered into;

(iii) the financial institution has terminated any relationship with the customer; and

(iv) any attempted ML/TF activity has failed for any other reason.

19.6 STR information form

(1) An STR that is made to the FIU must be in the form (if any) approved by the FIU, and in accordance with the FIU's instructions. The report must include a statement about:

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

(b) if the financial institution 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 financial institution's knowledge or suspicion.

(2) If the financial institution makes an STR to the FIU under these Instructions about a proposed transaction, it must inform the QCB.

(3) A financial institution that fails to make an STR under these Instructions may commit an offence against the AML/CFT Law.

19.7 Obligation not to destroy records relating to customers under investigation

If a financial institution has made an STR to the FIU and the customer is under investigation by a law enforcement agency for ML/TF, the financial institution must not destroy any records relating to the customer or business relationship without consulting the FIU.

19.8 Restricting or terminating business relationship

(1) This item does not prevent a financial institution from restricting or terminating, for normal commercial reasons, its business relationship with a customer after a financial institution makes an STR about the customer to the FIU.

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

(3) If the financial institution restricts or terminates a business relationship with a customer, it must immediately inform the QCB about the restriction or termination.

19.9 Records to be maintained for STRs

The MLRO must make and maintain records relating to:

(a) details of each of the internal STR received;

(b) details relating to the obligations of the MLRO on receipt of internal STRs; and

(c) details of each STR made to the FIU.

20 Tipping-off

20.1 Tipping-off a customer

Tipping-off, in relation to a customer of a financial institution, is the unauthorised act of disclosing information that:

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

(i) an STR; or

(ii) an investigation relating to ML/TF; and

(b) may prejudice the prevention or detection of offences, the apprehension or prosecution of offenders, the recovery of proceeds of crime or the prevention of ML/TF.

20.2 Preventing Tipping off by Financial institutions

(1) A financial institution must ensure that:

(a) its officers and employees are aware of, and sensitive to the issues surrounding, tipping-off and the consequences of tipping-off; and

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

(2) If a financial institution believes, on reasonable grounds, that a customer may be tipped off by conducting CDD or ongoing monitoring, the financial institution may make an STR to the FIU instead of conducting CDD or monitoring.

(3) If the financial institution acts under sub-item (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 a customer.

20.3 Internal measures to safeguard information relating to STRs

(1) A financial institution must take all reasonable measures to ensure safeguarding information relating to internal STRs.

(2) In particular, the financial institution must ensure that information relating to internal STRs is not disclosed to any person, other than members of the Board of the financial institution, without the consent and permission of the MLRO.

(3) The MLRO must not consent to disclosure of information relating to an internal STR to any person, unless the MLRO is satisfied that such disclosure would not constitute tipping-off.

(4) Whenever the MLRO consents to disclose the information relating to an internal STR, the MLRO must make and maintain a record of having done so.

21 Screening and training requirements

21.1 Screening of individuals' requirements

(1) For the purpose of screening, an individual may be classified as:

(a) a higher-impact individual who has a role in preventing ML/TF under the financial institution's AML/CFT programme (such as a senior official, MLRO or Deputy MLRO, and any individual who may perform a controlled function, in the financial institution); and

(b) other individuals.

(2) A financial institution's screening procedures for appointment or employment of officers and employees must ensure that the officers and employees in the higher-impact category have appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently. For other individuals, the financial institution must ensure, and satisfy itself about, the individual's integrity.

(3) The screening procedures before appointment or employment must, as a minimum:

(a) obtain and confirm references about the individual;

(b) confirm the individual's employment history and qualifications;

(c) seek information or details about any criminal convictions of, or regulatory actions against, the individual, and verify the same; and

(d) take appropriate and reasonable steps to confirm the accuracy and completeness of the information obtained by the financial institution for screening purposes.

(4) Screening procedures must be continuous and regular for higher impact individuals (for example these procedures can include continuous monitoring their transactions and /or regularly checking their name matching aginst any sanctions list and / or monitoring any changes or developments in their profile that are not consistent with the initial provided information etc…)

(5) Financial institutions must document and provide evidence for the above mentioned requirements for all staff and employees.

21.2 AML/CFT training programmes

(1) A financial institution must identify, design, deliver and maintain an appropriate and adequate ongoing training programme on AML/CFT for its officers and employees at a minimum on an annual basis for all staff and whenever necessary.

(2) The training programme must ensure that the officers and employees of the financial institution and its group understand:

(a) their legal and regulatory responsibilities and obligations under the AML/CFT Law and these Instructions;

(b) their role in preventing ML/TF and the liability devolving on officers, employees and the financial institution from their involvement in ML/TF and their failure to comply with the AML/CFT Law and these Instructions;

(c) ML/TF threats, techniques, methods and trends, the vulnerabilities of the products offered by the financial institution, and how to recognise suspicious transactions; and

(d) Procedures conducted by the financial institution to make internal STR, including how to make effective and efficient reports to the MLRO whenever ML/TF is known or suspected.

(3) The training must enable the financial institution'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 financial institution must consider:

(a) Their different needs, experience, skills and abilities;

(b) Their various functions, roles and levels in the financial institution;

(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 financial institution's business and the risk of ML/TF;

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

(g) any analysis of STRs showing areas where training needs to be improved.

21.3 Maintaining and reviewing training

(1) A financial institution's AML/CFT training programs must be ongoing to ensure that the officers and employees:

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

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

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

(2) The financial institution must carry out a review of training needs at regular intervals in order to ensure that the objectives mentioned in sub-item (1) are met.

(3) The Board of directors of the financial institution must consider the outcome of each such review. If the review identifies deficiencies in AML/CFT training requirements, the financial institution must prepare and approve an action plan to remedy the identified deficiencies promptly.

22 Documents and Record Keeping

22.1 Record Keeping Requirements

(1) A financial institution must keep and maintain all documents and records related to the following at least for the minimum period mentioned below:

(a) A financial institution must maintain all necessary records on transactions, both domestic and international, for a period of 10 years following the completion of the transaction (regardless of whether the account or business relationship is ongoing or has been terminated);

(b) As for the accounts opened for natural persons or legal entities or other banks and financial institutions, documents and records related to those accounts must be kept for a period of 10 years at least starting from the date of closing the account (for example official records, KYC identification documents as IDs, Passports, Driving licenses, other account files and correspondences including any questionnaires or analysis conducted to determine the background or purpose of the complicated or unusual transactions;

(c) As for the transactions executed for customers who do not hold any account at the bank or financial institution (occasional customers), documents and records related to any transaction must be kept for a period of 10 years at least from the date of executing the transaction;

(d) As for the unusual and suspicious transactions, records must be kept for a period of 10 years at least or until a judgment, in case of any judicial involvement or final decision is rendered with regard to the transaction, whichever is longer;

(e) Records relating to lack of originator information due to technical limitations during MVTS must be retained for 10 years;

(f) Training records must be retained for a period of 10 years;

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

(2) Financial institutions should ensure that the transaction records and regulations must be retrieved without undue delay. Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

(3) The financial institution must update these data periodically and ensure that the judicial authorities and competent authorities entrusted with the enforcement of the AML/CFT Law have timely access to these documents and records, as and when necessary.

22.2 Records about compliance

(1) A financial institution must make the records necessary:

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

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

(2) The financial institution must make the records necessary to demonstrate how:

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

(b) the financial institution has complied with its responsibilities under the AML/CFT Law and these Instructions;

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

(d) each of the financial institution'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 Instructions.

(3) Records that must be kept by the financial institution include:

(a) documents and data obtained while performing CDD;

(b) account files;

(c) business correspondence; and

(d) results of analysis of STRs.

(e) AML/CFT self risk assessment

23 Auditing and sanctions

23.1 Internal and external auditing

(1) The internal auditing function must review the effectiveness of the procedures and control systems applied in respect of AML/CFT on an annual basis by the financial institution for its branches and subsidiaries inside and outside Qatar. All appropriate actions must be taken to fill any gap or update and develop the procedures and systems to ensure their effectiveness and adequacy. Financial institutions must prepare an annual audit plan based on the risks identified and assess the level of compliance with the risk mitigation plan.

(2) The external auditor must, among other functions, ensure that a financial institution applies these Instructions and verify the adequacy of the policies and procedures applied by the financial institution in this regard. It must also include the results of

such review in the management letter and inform QCB immediately of any major violation of these Instructions.

(3) Internal and exteranal auditors must prepare appropriate work programs including the mechanisms and procedures used to assess the level of effectiveness of the AML/CFT regime.

23.2 Sanctions

Sanctions relating to AML/CFT must be applied in accordance with the AML/CFT Law.

Appendix

A. Miscellaneous issues for guidance

(1) Processes of money laundering

There are 3 stages of money laundering:

(a) placement – involves introduction of illegally obtained funds into the financial system, usually through a financial institution. This is achieved through cash deposits, purchase of financial instruments for cash, currency exchange, and purchase of security or insurance contracts, cheques cashing services, cash purchases or smuggling of cash between countries.

(b) layering – consists of a series of transactions, through conversions and movements of funds, designed to conceal the origin of funds. This may be accomplished by sending wire transfer to other banks, purchase and sale of investments, financial instruments, insurance contracts, phony or bogus investments or trade schemes.

(c) integration –involves re-entering of funds into the legitimate economy. This is accomplished through the purchase of assets, securities, financial assets, luxury goods, investments in real estates or business ventures.

(2) Money laundering through cash transactions

- Large cash deposits not in line with the customer's type of business or occupation.
- Numerous cash deposits of small amounts (which is known as structuring or smurfing) in order to avoid detection.
- Cash deposits followed by a transfer (wire transfer, bank cheques).
- Structured cash payments for outstanding credit card balances, with relatively large sums as payments.
- Depositing cash through multiple deposit coupons, in such a manner that each deposit operation is performed separately in small amounts so as not to draw the attention of authorities (but the total deposits would be a huge amount).
- Constant deposit operations through cheques, transfers or marketable instruments.
- Attempts to replace smaller denomination currency notes with higher denomination currency notes.
- Branches showing cash transactions that exceed the usual limits, in relation to their usual positions' statistics.
- Large cash deposits through electronic deposit systems, to avoid any direct contact with the officers of the banking and financial institutions.

(3) Money laundering through banking accounts

Such transactions are usually undertaken by:

(a) customers wishing to maintain a number of regular accounts and trust fund accounts while depositing large amounts of cash money in each of them and the nature of their activity does not correspond to the size of amounts deposited;

(b) cash settlement between external payments (payment orders, transfers) and the customers' balances on the same or previous day;

(c) deposit of cheques in large amounts by third parties endorsed in favour of the customer;

(d) large cash withdrawals from an account that was previously inactive, or from an account which was fed with unusual large amounts from outside; or

(e) multiple deposits by a large number of individuals into one account, without any clear explanation or clarification.

(4) Money laundering through financial transactions associated with investment activities

Such transactions are usually undertaken by:

(a) loan or deposit transactions with subsidiaries or affiliates of a financial institution located or operating in areas known to be affected by ML, drug trafficking or other criminal activities;

(b) applications submitted by customers for purchase or sale of investments or services (whether foreign currencies or financial instruments) with obscure source of funds, or sources that do not correspond with their apparent activity; and

(c) large cash settlements for purchase or sale of securities.

(5) Money laundering through cross-border activities may be represented in the following forms:

(a) Customer introduced to the bank by an external financial institution located in a country known to be affected by criminal drugs production or trafficking;

(b) customers paying or receiving regular large amounts in cash or by fax or telex transfer, without any indications to the legitimate sources of those funds, or customers connected to countries known to be affected by criminal drugs production or trafficking or in relation to the prohibited terrorist organisations, or countries offering opportunities for tax evasion;

(c) incoming or outgoing transfer operations executed by a customer without using any of his accounts at any bank; and

(d) constant and regular withdrawal or deposit of cheques issued in foreign currencies or travellers cheques into the account of the customer.

B. Typologies

(1) The various techniques or methods used to launder money or finance terrorism are generally referred to as typologies. Typology study is a useful tool to examine and provide insight and knowledge on emerging trends and threats and ways to mitigate them. Financial institution must update the new typologies applicable to its area of business. Such information is available from FATF and MENA FATF web-sites.

(2) Examples include:

(a) alternative remittances channels (such as hawala, hundi): which are informal mechanisms based on a network of trusts used to remit money. These often work parallel to the established banking channels. This system is exploited for ML/TF to move money without detection and obscure identity.

(b) structuring or smurfing: which involves numerous transactions like deposits, withdrawals, transfers, often involving various people, with high volume of small denomination transactions and numerous accounts to avoid transgressing the threshold limits or reporting obligations.

(c) currency exchanges or cash conversion: through use of travellers cheque or extensive usage of exchange houses.

(d) cash couriers or currency smuggling: concealed movement of currency across borders.

(e) purchase of valuable assets: proceeds of crime are invested in high value goods like real estate, shares and gold.

(f) use of wire transfer.

(g) trade-based ML involving invoice manipulations and using trade financing routes and commodities.

(h) mingling: by combining proceeds of crime with legitimate business proceeds.

(i) use of shell companies: used to obscure the identity of persons controlling funds.

References by international bodies

- FATF Recommendations - See www.fatf-gafi.org
- Basel Committee: Statement on Money Laundering and Customer Due Diligence for banks – December 1988 and October 2001 – see www.bis.org/publ
- Other websites for relevant AML/CFT information:
- Middle East North Africa Financial Action Task Force – www.menafatf.org
- The Egmont Group – www.egmontgroup.org
- The United Nations – www.un.org/terrorism
- The UN Counter-Terrorism Committee – www.un.org/Docs/sc/Committees/1373
- The UN list of designated individuals – www.un.org/Docs/sc/committees.1267/1267ListEng.htm
- The Wolfsberg Group – www.wolfsberg-principles.com
- The Association of Certified Anti-Money Laundering Specialists – www.acams.org
- Qatar Financial Information Unit – www.qfiu.gov.qa