Chapter Ten

Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT)

(AML) and (CFT)

[282]Regulations on Anti-Money Laundering (AML) And Combating Financing of Terrorism (CFT)

First: Regulations:

1- Legal Basis for the regulations

Having perused QCB Law and Law 4 of 2010 on Anti-Money Laundering and Combating Financing of Terrorism, Qatar Central Bank has decided to issue the following regulations to the financial institutions as defined under Article 1 of QCB Law in order that the financial institutions make these regulations an integral part of their systems and procedures aimed at controlling, detecting, preventing and reporting of ML/FT activities.

These regulations are issued under the provisions of Article 121 read with Articles, (7-8) and para (9) of article (33) QCB Law and Article 41 of Law (4) of 2010 of Anti-Money Laundering and Combating Financing of Terrorism. Any contravention of the regulations shall attract the provisions of Law (4) of 2010.

2- Objectives of the Regulations

1. To ensure that the financial institutions functioning in the State of Qatar comply with the provisions of Law (4) of 2010 on Anti-Money Laundering and Combating the Financing of Terrorism and provisions of these regulations.
2. All financial institutions are under statutory obligation of Law 4 of 2010 in addition to the specific requirements contained in these regulations.
3. To ensure implementation of policies, procedures, systems and controls for prevention, detection, control and reporting of money laundering and terrorist financing in accordance with the FATF 40+9 Recommendations on AML/CFT.
4. To protect financial institutions operating in the State of Qatar from being exploited as channels for passing illegal transactions arising from money laundering, terrorist financing and any other illicit activities.

[282] Refer to circular no. (59/2010) dated 15/6/2010, to all banks. All articles are amended as per QCB Law

5. To maintain, enhance and protect the credibility, integrity and reputation of financial institutions in the State of Qatar.

3- Definitions

Beneficial Owner	The natural person who owns, or exercises effective control, over the client, or the person on whose behalf, the transaction is conducted, or the person who exercises effective control over a legal person, or legal arrangement.
Board	Board of Directors of a FI or equivalent authority
Business relationship	In relation to a financial institution, is a business, professional or commercial relationship between the financial institution and a customer other than a temporary relationship.
Correspondent banking	Is the provision of banking services by a financial institution (the correspondent) to another financial institution (the respondent).
Customer[283]	Any person dealing with financial institutions.
Customer due diligence	In relation to customers of FIs, it means identification measures taken by FI of a customer, verifying identity, establishing if the customer is acting on behalf of another person, if the customer is a legal person, establishing the beneficial owner, obtaining information on the purpose and intended nature of business relationship etc.
Financial Institutions[284]	As defined under QCB Law, which is any bank or a financial services institution or an offshore unit read with Article 1 of Law (4) of 2010 which is an entity who conducts as business one or more of the following

[283] Person :Physical or legal person, as the case may be.
Customer: Any physical or legal person who receives or deals in any financial services with financial institutions. A Customer is every person who commences receiving or dealing in any financial services, with financial companies.

[284] For all definitions, refer to QCB Law, article no. (1).

	activities or operations for or on behalf of a customer: (1) operation accepting deposits and other repayable funds such as private banking services. (2) lending. (3) financial leasing. (4) transferring money or things of value. (5) issuing or managing means of payment, such as credit and debit cards, cheques, traveller's cheques, money orders, banker's drafts and electronic money. (6) financial guarantees and commitments. (7) trading in money market instruments, such as cheques, bills, certificates of deposit and derivatives, foreign exchange, exchange instruments, interest rate, index instruments, transferable securities, and commodity futures trading. (8) participating in securities issues and providing financial services related to securities issues. (9) undertaking individual or collective portfolio management. (10) safekeeping or administering cash or liquid securities on behalf of other persons. (11) investing, administering or managing funds or money on behalf of other persons. (12) underwriting or placing life insurance and other investment-related insurance, whether as insurer or insurance contract intermediary. (13) money or currency changing. (14) any other activity or operation prescribed by resolution issued by the Prime Minister upon the proposal of the Committee.
Jurisdiction	Any kind of legal jurisdiction, which may include the State, a foreign country (whether or not an independent sovereign jurisdiction) or a State, province or other

	territory of a foreign country, QFC or any similar authority.
Money Laundering	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 concealing or disguising the illicit origin of such funds or of 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.
Non-Profit Organization	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.
Non-resident customer	Natural or legal person residing outside the State of Qatar and / or present in Qatar on temporary basis (for tourism / or for visit)
On-going monitoring	In relation to a customer means scrutinizing transactions under the business relationship, customer's business and risk profile, sources of income and wealth, when required, review of the records by the FIs to keep the records up-to-date and relevant.
Politically Exposed Persons (PEPs)	Persons who are or have been entrusted with prominent public functions in a foreign country or territory, as well

	as members of such persons' family or those closely associated with those persons. The prominent public functions may in this regard include: Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, Members of Parliament, Senior politicians or important political party officials, Judicial officials, Members of boards of Central Banks, Ambassadors & Charges d' affaires, High ranking officers of armed forces, Senior executives of state owned corporations.
Shell Banks	Is a bank that has no physical presence in the jurisdiction in which it is incorporated and licensed and it is not affiliated with a regulated financial institution group that is subject to effective consolidated supervision. Physical presence would mean presence involving meaningful decision-making and management and not merely the presence of a local agent or low level staff.
Suspicious Transactions Report (STRs)	A report to be made by FIs to FIU on any suspicious transactions or any attempts under the provisions of Article 14 and 18 of Law (4) of 2010
Terrorist	any natural person who commits any of the following acts: 1) commits, or attempts to commit, terrorist acts, wilfully, by any means, either directly or indirectly. 2) participates as an accomplice in terrorist acts. 3) organizes or directs others to commit terrorist acts. 4) 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	1) An act which constitutes an offence as per the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997). 2) any other act intended to cause death or serious bodily injury to civilians, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist Financing	An act committed by any person who, in any manner, directly or indirectly, and willingly, provides or collects funds, or attempts to do so, in order to use them or knowing that these funds will be used in whole or in part for the execution of a terrorist act, or by a terrorist or terrorist organisation.

Terrorist Organization	any group of terrorists that commits any of the following: 1) commits, or attempts to commit, terrorist acts, wilfully, by any means, directly or indirectly. 2) acts as an accomplice in the execution of terrorist acts. 3) organises or directs others to commit terrorist acts. 4) 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.
Wire-transfer	Any transaction carried out on behalf of an originator (both natural persons and legal entities) through the FI by electronic means with a view to making an amount of money available to a beneficiary person at another FI. The originator and the beneficiary may be the same person.

Any other term used in the regulation will have the same meaning as given under QCB Law or Law (4) of 2010 or other regulations issued by QCB in that regard, unless specifically mentioned otherwise.

4- General Provisions

4.1. General Application

These regulations are applicable to all financial institutions, viz., **Banks, Investment and Finance Companies, Exchange Houses and offshore units,** licensed by Qatar Central Bank. Financial Institutions must implement and apply the specific provisions of QCB Law and Law 4 of 2010 and these regulations as appropriate and applicable to them.

5- Key AML/CFT Principles

5.1. Principle 1 – Responsibility of Board of the FI.

The Board of the FI should ensure that its policies, procedures, systems and controls appropriately and adequately address the requirements of AML / CFT Law and these regulations.

5.2. Principle 2 – Risk Based Approach

FIs should adopt a risk-based approach to the requirements of these regulations.

5.3. Principle 3 – Know Your Customer

The FIs should know each of its customers to the extent appropriate to the customer's risk profile.

5.4. Principle 4 – Effective Reporting

FIs must have effective measures in place to ensure internal and external reporting whenever money laundering or terrorist financing is known or suspected.

5.5. Principle 5 – High standard screening and appropriate training

An FI should have adequate screening procedure to ensure high standards when appointing or employing officers and employees and also should have an appropriate on-going AML/CFT training programme for its officers and employees.

5.6. Principle 6 – Evidence of Compliance

FIs should be able to provide documentary evidence of its compliance with the requirements of the AML / CFT Law and these regulations.

6- General AML and CFT Responsibilities

6.1. Develop AML/CFT Programme

1. Financial Institutions should develop programmes against money laundering and terrorist financing.
2. The type and extent of measures adopted by the FIs must be appropriate having regard to the risk of money laundering and terrorist financing, size, complexity and nature of the business of the FIs.

3. The programme should include at a minimum the following:
    a. Developing, establishing and managing internal policies, procedures, systems and controls to prevent money laundering and financing of terrorism and to communicate the same to the employees of the FI.
    b. Appropriate compliance management arrangements, e.g. to designate Money Laundering Reporting Officer (MLRO) at the management level.
    c. The MLRO and other appropriate staff should have timely access to customer identification data and other customer due diligence information, transaction records and all other relevant information relating to AML/CFT.
    d. Adequate screening procedures to ensure high standards when appointing or employing officers and employees, and employees kept informed of developments on money laundering / financing of terrorism techniques, methods and trends and a clear explanation of all aspects of ML/FT Law and regulation, obligations arising out of these, in particular relating to CDD and STRs.
    e. Appropriate on-going training programme for its 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. Appropriate on-going assessment and review of FIs policies, procedures, systems and controls.
4. The policies, procedures, systems and controls must cover the following at a minimum:
    a. Customer due diligence measures and on-going monitoring
    b. Record making and retention
    c. Detection of suspicious transactions
    d. Internal and external reporting obligations
    e. Internal communication of FIs policies, procedures, systems and controls to its officers and employees
    f. Any other issues that may be required under the AML/CFT Law or regulations as may be appropriate and as applicable to FIs.

6.2. Policies etc should be risk sensitive, appropriate and adequate to risks

The FIs AML/CFT policies, procedures, systems and controls must be risk-sensitive, appropriate and adequate having regard to the risk of money laundering and terrorist financing and to the size, complexity and nature of business.

6.3. Issues to be covered by the policy on AML/CFT

The FIs AML/CFT policies, procedures, systems and controls must cover at a minimum the following:

1. Provide for identification and scrutiny of complex or unusually large transactions; unusual patterns of transactions that have no apparent economic or visible lawful purpose; any other transactions that FIs consider by their nature to be related to money laundering or terrorist financing,
2. Require enhanced customer due diligence measures to prevent use of money laundering or terrorist financing of products and transactions that might favour anonymity
3. Provide appropriate measures to reduce the risks associated with establishing business relationship with politically exposed persons
4. Prior to any function or activity that may be outsourced by the FIs, assessment and documentation of the ML/FT risks associated with outsourced functions; monitoring of these risks on an on-going basis.
5. Require all officers and employees of the FIs to comply with the requirements of Law 4 of 2010 on AML/CFT and regulations relating to making of Suspicious Transactions Report.

6.4. Annual assessment and review of policies

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

6.5. Application and Compliance of AML/CFT requirements by officers, employees

1. The FIs should ensure that its officers, employees comply with the requirements of the AML/CFT Law and the regulations, policies, procedures, systems and controls. In the context of the applicability in another jurisdiction, it may be

applied to the extent that local law of that jurisdiction's applicable laws and regulations permit.

2. Without limiting the applicability of above item at **6.5.1**, the policies, procedures, systems and control should require the officers and employees to provide suspicious transactions reports for transactions in, from or to its jurisdiction to their Money Laundering Reporting Officer, and ensure to provide timely, unrestricted access by the FI's Board and Money Laundering Reporting Officer, and by the Qatar Central Bank and FIU, to the documents and information of the FI, that may relate directly or indirectly to transactions in, from or to its jurisdiction.
3. FIs may apply the requirements that impose higher and consistent standards in its AML/CFT policies, procedures, systems and controls in relations to customers whose transactions or operations extend over a number of jurisdictions.
4. If the law or regulation of another jurisdiction prevents the application of a provision or provisions of the Law 4 of 2010 and these regulations, the officers of FI in that jurisdiction must immediately inform the Money Laundering Reporting Officer in the Head Office.

6.6. Application and Compliance of AML/CFT requirements to overseas branches and subsidiaries of financial institutions

1. FIs should ensure that the officers and employees of branch (s) or subsidiaries, comply with the requirements of the AML/CFT Law and the regulations, policies, procedures, systems and controls. In the context of the applicability in another jurisdiction, it may be applied to the extent that local law of that jurisdiction's applicable laws and regulations permit.
2. Without limiting the applicability of above item at **6.6.1**, the policies, procedures, systems and control should require the officers and employees of the branch (s) / Subsidiaries to provide suspicious transactions reports for transactions in, from or to its jurisdiction to their Money Laundering Reporting Officer, and ensure to provide timely, unrestricted access by the FI's Board and Money Laundering Reporting Officer, and by the Regulator and FIU, to the documents and information of the FI, that may relate directly or indirectly to transactions in, from or to its jurisdiction.

3. Branch (s) / subsidiaries of FIs may apply the requirements that impose higher and consistent standards in its AML/CFT policies, procedures, systems and controls in relations to customers whose transactions or operations extend over a number of jurisdictions.
4. If the law or regulation of another jurisdiction prevents the application of a provision or provisions of the Law 4 of 2010 and these regulations to the branch (s) / or subsidiaries, the officers of branch (s) / Subsidiaries of the FI in that jurisdiction must immediately inform the Money Laundering Reporting Officer in the Head Office.
5. FIs must pay particular attention to procedures in branches, or subsidiaries in countries that do not or insufficiently apply FATF Recommendations & Special Recommendations.

6.7. Application and Compliance of AML/CFT requirements to outsourced activities.

The FIs when outsourcing any of its activities or functions should ensure the following:

1. The FI and its Board will be primarily responsible to ensure that the AML/CFT Law and regulations are complied
2. The FI should through a Service Agreement or any other means, ensure that when activities are outsourced to any company or firm that the company or firm's officers, employees or their agents, in any jurisdiction, comply with the requirements of AML/CFT Law and these regulations, the policies, procedures, systems and controls, as applicable to FIs. In the context of the applicability in another jurisdiction, it may be applied to the extent that local law of that jurisdiction's applicable laws and regulations permit.
3. The FIs AML/CFT policies, procedures, systems and controls should require the outsourcing company or firm, its officers and employees, in any jurisdiction, to provide suspicious transactions report to FI involving transactions from or to the outsourcing company or firm. The suspicious transactions report should be sent by the outsourced company or firm to the Money Laundering Reporting Officer of the financial institution outsourcing its activities.

4. FI should ensure that the outsourcing company or firm should provide timely, unrestricted access to its documents and information that may be directly or indirectly related to transactions with the FI, to the Money Laundering Reporting Officer, QCB and FIU.
5. In case the foreign jurisdiction prevents application of any of the provisions of the Law or regulations, the outsourcing company or firm should immediately inform the FI outsourcing its activities and the FI must immediately convey the same to QCB.

7- Board of Directors

7.1. Overall responsibility of Board

The Board of the FI will be responsible for the effectiveness of the policies, procedures, systems and controls in preventing money laundering and terrorist financing.

7.2. Particular responsibility of the Board

The Board of the FIs should ensure:

1. that the FI develops, establishes and maintains effective AML/CFT policies, procedures, systems and controls in accordance with the requirements of AML / CFT Law 4 of 2010 and these regulations,
2. that the FI have in place adequate screening procedures to ensure high standards when appointing or employing officers or employees,
3. that the FI identifies, designs, delivers and maintains an appropriate on-going AML/CFT training programme for its officers and employees.
4. that the FI has an adequately resourced and independent audit function to test compliance with the FI's AML/CFT policies, procedures, systems and control, including sample testing.
5. that regular and timely information is made available to the Board about the management of the FI's money laundering and terrorist financing risks,
6. that the FI's AML/CFT risk management policies and methodology are appropriately documented, including their application by the FIs,
7. that there is a Money Laundering Reporting Officer **(Item 8 on MLRO)** designated to attend to the issues of money laundering and terrorist financing, in terms of the provisions of Article 36 of Law 4 of 2010, who

a. has sufficient seniority, experience and authority,
b. has sufficient resources, appropriate staff and technology to carry out his responsibilities effectively, objectively and independently,
c. has timely, unrestricted access to all information of the FI which are relevant to AML and CFT, which may include customer identification documents, other documents, data and information, customer due diligence and on-going monitoring, all transaction records,

8. ensure that appropriate back up to the Money Laundering Reporting Officer is available to be able to carry on the functions without interruption during the absence of Money Laundering Reporting Officer, including a Deputy Money Laundering Reporting Officer **(Item 8.4.9 and 8.4.11)**. The Board of FI must ensure that if the position of Money Laundering Reporting Officer falls vacant, the FI should appoint a replacement after obtaining QCB approval.
9. ensure that the FIs have a AML/CFT compliance culture
10. ensure that appropriate measures are in place to account for the money laundering and terrorist financing risks and are taken into account in the day-to-day operations and also in relation to the development of new products, taking in new customers and with changes in the business profile of the FI.

The above particular responsibilities of Board of FI are only indicative and do not limit the Board from putting in place stringent measures to counter the money laundering and terrorist financing risks in the FI.

8- Money Laundering Reporting Officer [MLRO] and Deputy

8.1. Appointment

1. The FI should appoint a Money Laundering Reporting Officer who will be designated to oversee the countering of money laundering and terrorist financing risks in the FI at all times, in terms of the provisions of Article 36 of Law 4 of 2010.
2. The position of MLRO may otherwise be combined with other functions in FI, such as that of the Compliance Officer, in cases where the size and geographical spread of the FI is limited, and therefore, the demands of the function are not likely to require a full time MLRO.

3. The position of MLRO should not be combined with those functions that would create potential conflicts of interest.
4. The position of Money Laundering Reporting Officer should not be outsourced.
5. The name and designation of the official designated to be MLRO and Deputy MLRO should be reported to the Anti-Money Laundering and Terrorist Financing Section, Supervision and Control Department, Qatar Central Bank.
6. FI should seek the approval of QCB for appointment, removal or resignation of the MLRO and Deputy MLRO.

8.2. Eligibility to be MLRO and Deputy

The Money Laundering Reporting Officer of FI who is designated to oversee ML/FT issues should be:

1. employed at the management level
2. must have sufficient seniority, experience and authority to carry out his responsibilities independently,
3. should report directly to the Board of the FI,
4. ordinarily be a resident in Qatar.

8.3. General Responsibilities of MLRO

The MLRO will be responsible for the following:

1. Oversight on the implementation of FI's AML/CFT policies, procedures, systems and controls, including the risk based approach to ML/FT risks,
2. Ensure that appropriate policies, procedures, systems and controls are developed, established and maintained across the FI to monitor day-to-day operations for compliance with AML/CFT law, regulations, policies, procedures, systems and controls and assess regularly **[at a minimum Yearly]**, review the effectiveness of the same to prevent money laundering and terrorist financing,
3. Able to review all data related to customers transactions in FIS and can obtain such information at the appropriate time so as to determine and analyze data effectively,
4. MLRO should be the key and focal person in implementing the FI's AML/CFT strategies,
5. Supporting and coordinating the Board's focus on managing the FI's money laundering and terrorist financing risks in individual business areas,

6. Ensure that the FI's wider responsibility for preventing money laundering and terrorist financing is addressed centrally,
7. Ensuring the AML/CFT monitoring and accountability within the FI.

8.4. Particular Responsibilities of MLRO & Deputy

The particular responsibilities of MLRO are:

1. Receiving, investigating and assessing the internal suspicious transaction reports of the FI,
2. Making STRs to FIU,
3. Acting as focal or central point of contact between the FI, FIU, the Regulator(s), and State authorities in relation to AML and CFT issues,
4. Ensure prompt response to request for information by FIU, Regulator(s), and State authorities in relation to AML and CFT issues,
5. Receive and act on government, regulatory and international findings about AML/CFT issues,
6. Monitoring appropriateness and effectiveness of the FI's AML/CFT training programme,
7. Reporting to the Board of the FI on AML and CFT issues,
8. Exercising all other functions given to Money Laundering Reporting Officer under AML/CFT Law, regulations or on issues relating to AML/CFT.
9. Ensure to keep Deputy MLRO informed of the significant AML/CFT developments, **(see Item 7.2.8 above)**
10. The MLRO must execute his responsibilities honestly, reasonably and independently, particularly while receiving, investigating and assessing internal STRs and deciding whether to make a STR to FIU.
11. The Deputy MLRO of the FI will function and act as the MLRO during the absence of the MLRO and during the vacancy of MLRO and rules of responsibilities of MLRO applies to Deputy as MLRO.

8.5. Reporting by MLRO to the Board

8.5.1. Reports of MLRO

1. The Board of the FI should on a regular basis decide what general reports should be given to it by the MLRO, periodicity of these reports that may be

given to the Board, in order to discharge its responsibilities under the AML/CFT Law and these regulations.

2. At the minimum, an Annual Report by the MLRO should be given to the Board for each financial year to enable the Board to consider it within a specified time frame as given under **Item 8.5.2.3**. However, this will not limit the reports that may be required by the Board or reports submitted by the MLRO on his own initiative in discharge of his responsibilities.

8.5.2. Annual Report of MLRO

1. The Report should assess the adequacy and effectiveness of the FI's AML/CFT policies, procedures, systems and controls in preventing money laundering and financing of terrorism,
2. The minimum requirements of the Annual Report that should be submitted to the Board of FI for each financial year should include the following details:
    a. The numbers and types of internal STRs made to Money Laundering Reporting Officer,
    b. The number of these STRs that have been passed on to the FIU and the number of STRs that have not been passed on to the FIU, and reasons thereof,
    c. The numbers and types of breaches by the FI of AML/CFT Law, regulations or the FI's policies, procedures, systems and controls,
    d. Areas where the FIs AML/CFT policies, procedures, systems and controls should be improved along with proposals for appropriate improvements,
    e. A summary of the AML/CFT training imparted to FI's officers and employees,
    f. Areas where the AML/CFT training programme should be improved and proposals for appropriate improvements,
    g. Number and types of customers of FIs who are categorized as high risk,
    h. A summary on the progress in implementing AML/CFT action plans, like consideration of the Annual Report by the Board, assessment and review of training, any other issues relating to AML/CFT,
    i. Outcome of any audit reviews that was mandated by the FI in relation to AML/CFT policies, procedures, systems and controls,

j. Outcome of any review or assessment of risks, policies, procedures, systems and control.

8.5.3. Consideration of Annual Report of MLRO by the Board

1. The Board of the FI must consider the Annual Report made by the MLRO in a timely manner,
2. In case the Report had identified deficiencies in FI's compliance to AML/CFT Law, regulations, training programmes, the Board should prepare and/or approve and document an action plan to remedy the deficiencies in a timely manner.
3. The Report submitted by the MLRO should be dealt with by the Board as per Item **8.5.1** above not later than 4 months after the end of the financial year to which the Annual Report relates.

9- Risk Based Approach

9.1. Risk Based Approach – General

1. FIs should develop risk based approach to monitoring as appropriate to their business, their number of clients and types of transactions.
2. The monitoring systems should be configured to identify significant or abnormal transactions or patterns of activity. This system should include:
    a. Limits on number, types or size of transactions undertaken outside the expected norms;
    b. Limits for cash and non-cash transactions
3. FIs should assess the ML/TF risk arising from the:
    a. types of customers it currently has or likely to have,
    b. Different types of products and services rendered by the FI
    c. The technology currently used and the new technology that may be used for better service.
4. FI should assess the potential risks arising from the above items and decide on the strategies to mitigate these risks.

9.2. Assessment Methodology to mitigate ML/FT threats

1. FIs should adopt the threat assessment methodology to mitigate the risks of ML/TF that is suitable to the size, business profile and risk profile of the FI,
2. The FI should be able to demonstrate to QCB that its threat assessment methodology is capable of the following:
    a. Assessing the risk profile of the business relationship with each customer,
    b. Is designed to identify changes in the FIs ML & TF risks, risk posed by new products, new services introduced by the FI and in applying new technologies to FI's services.
    c. From Item **9.2.2(b)** above, the FI should be in position to demonstrate that its general practice of risk management of ML/FT risks matches its threat assessment methodology.

9.3. Risk profiling business relationship

1. While risk profiling a business relationship with a customer, FIs should consider the following 4 risk elements:
    a. Customer Risk
    b. Product Risk
    c. Interface or Delivery Channel Risk
    d. Jurisdiction or Geographical area Risk
2. FIs should also assess and identify any other risks that may be relevant to the specific types of business relationship, taking into account the size, complexity and nature of its business in relation to business of its customers.
3. FIs should take into account the 4 risk given under **Item 9.3.1 and 9.3.2 above** in order to arrive at the risk profile of business relationship.
4. FIs should base the intensity of customer due diligence measures and on-going monitoring taking into account the risk profile of the relationship.

10- Customer Risk

10.1. Risk Assessment of customer risks

1. FI should assess and document the risks of money laundering, terrorist financing and other illicit activities posed by different types of customers,

2. The intensity of customer due diligence measures and on-going monitoring required for a particular type of customer should be proportionate to the perceived or potential level of risk posed by the relationship with the customer.

10.2. Policies and procedures to address customer risk

1. FIs should have policies, procedures, systems and controls to address specific risk of money laundering, terrorist financing or other illicit activities posed by different types of customers,
2. FIs should include in its policy and procedures, the methodology adopted to score the customers' profile and risks based on the source of income and wealth,
3. FIs should have enhanced customer due diligence and on-going monitoring if it suspects that a customer is an individual, a charity, non-profit organization that is associated with, or involved in, terrorist acts, terrorist financing or a terrorist organization or when an individual or entity is subject to sanctions or other international initiatives relating to AML/CFT issues.
4. Irrespective of the risk score of the customer, the FI should conduct enhanced due diligence measures and enhanced on-going monitoring to the customers listed at **Item 10.2.3 above.**
5. Any decision to enter into business relationship with non-profit organizations or customers requiring enhanced CDD measures should only be made after seeking the approval of the Board and only after completion of the enhanced CDD measures.

10.3. Measures for politically exposed persons (PEPs)

FIs should adopt the following measures to reduce the risks associated with establishing and maintaining business relationship with PEPs:

1. FIs should establish a PEP client acceptance policy, taking into account the reputational and other risks involved.
2. FI should have clear policies, procedures, systems and controls for establishing business relationships with PEPs,
3. FI should establish and maintain an appropriate risk management system to decide whether a potential or existing customer or the beneficial owner of a potential or existing customer is a PEP. Such measures would entail seeking

relevant information from customers, reference to publicly available information, and having access to, referring to, commercial electronic databases of PEPs, etc.

4. FIs decision to enter into business relationships with PEPs should be taken only after approval of the Board and after enhanced CDD measures have been conducted, and enhanced monitoring and customer due diligence measures should be adopted, wherein the FI should analyze complex financial structures like trusts, foundation or international corporations, and development of a profile of anticipated customer activity which can be used in on-going monitoring.
5. 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 should be continued only with the approval of the Board,
6. FIs should establish a methodology and reasonable measures to establish the sources of wealth and funds of customers and beneficial owners identified as PEP,
7. PEPs should be subject to enhanced on-going monitoring.

10.4. Risk Assessment Process for legal entities, legal arrangements & facilities, Trusts, Clubs and Societies.

1. FIs risk assessment processes and methodology should include recognition of risks posed by legal entities, arrangements and facilities, which may include, companies, partnership, trusts, nominee shareholdings, power of attorney etc.
2. While assessing the risk posed by these legal entities, arrangements or facilities, FI should ensure that the risks posed by beneficial owners, officers, shareholders, trustees, settlers, beneficiaries, managers or any other entities relating to these are reflected in the risk profile of entity or arrangement or facility,
3. FIs while assessing the risks of trusts, should take into account the different ML/FT risks that are posed by trusts having different sizes and activities. This has to be evaluated in the light of the purpose of the trusts (like some trusts may be set up for limited purposes or may have a limited range of activities, while some of the trusts have extensive activities, including financial linkages in other jurisdictions).
4. FIs while assessing the risks of clubs and societies, should take into account the possibilities of ML/FT risks arising from such customer relationship and their different areas of activities.

5. The risk profile should also be able to capture the risks posed by such entities by reduction in transparency or through an increased ability to conceal the risks.

11- Product Risk

11.1. Risk Assessment of product risk

1. The FIs should assess and document the risks of money laundering, terrorist financing and other illicit activities posed by the products it offers or proposes to offer to its customers. Such products may be savings accounts, e-money products, payable through accounts, wire transfers etc.
2. The intensity of customer due diligence measures and on-going monitoring for each type of product should be commensurate with and proportional to the perceived and potential risk that may be posed by each type of product.

11.2. Policies & procedures for product risk

1. FIs should have policies, procedures, systems and controls to address specific risks of ML, TF and other illicit activities posed by different types of products offered by the FI or it proposes to offer to its customers.
2. FIs should have methodology on the basis of which business relationship with customers will be scored based on different types of products it offers or proposes to offer.

11.3. Products with fictitious, false or no names

FIs should not permit any of its products to be used with fictitious, false or when no names or the customer is not identified.

11.4. Correspondent banking relationships

1. FIs (correspondent) prior to establishing correspondent banking relationship with a FI in a foreign jurisdiction (respondent), the correspondent FI should undertake to complete the following:
   a. Gather all information on the respondent to understand the nature of its business (e.g. through a structured questionnaire),
   b. Gather information about the respondent bank's ownership structure and management,

c. Gather information on major business activities of the respondent and its location (i.e for e.g. whether it is located in a FATF compliant jurisdiction) as well as the location of its parent, wherever applicable.
d. Purpose for which the account will be opened.
e. Decide from publicly available information, the respondent's reputation and quality of its regulation and supervision,
f. Assess the respondent FI's AML/CFT policies, procedures, systems and controls and ensure if they are adequate and effective,
g. Obtain the approval of the Board to establish correspondent banking relationship,
h. The correspondent FI should ensure and be satisfied that:
    i. the respondent FI's customers who would have direct access to correspondent FI's accounts, are the customers whose CDD measures are undertaken and verified,
    ii. on-going monitoring being conducted by the respondent FI and
    iii. the respondent FI would be able to provide to correspondent FI documents, data or information on CDD or on-going monitoring, when requested by correspondent FI, within a reasonable time frame.

2. The Correspondent FI should also consider before establishing business relationship the following:
    i. whether the respondent FI has been subject to any investigation, or civil or criminal proceeding relating to ML/FT
    j. The financial position of the respondent FI
    k. Whether the respondent FI is regulated and supervised, by a regulatory or governmental authority equivalent to the authority in home jurisdiction
    l. Whether the jurisdiction in which the respondent FI is operating has an effective AML/CFT regime
3. In case the respondent FI is a subsidiary of another legal entity, the correspondent FI should seek information on the legal entity, its location and domicile, reputation, whether the legal entity is supervised, at least for AML/CFT purposes, by a regulatory body or governmental authority equivalent to the authority in the home jurisdiction, whether the jurisdiction in which the legal entity operates has effective AML/CFT regime, its ownership, control,

management structure, including aspects like ownership, control or management by PEP.

4. In case the respondent FI is operating in a high risk jurisdiction, the correspondent FI should conduct enhanced on-going monitoring on the transactions conducted under the relationship and review the relationship on an annual basis.
5. Additional measures to be taken by the FIs, prior to opening a correspondent banking relationship, should include a signed agreement that outlines the respective responsibilities and obligations of each institution in relation to money laundering detection and monitoring responsibilities.

11.5. Shell Banks

1. FI should not establish or continue business relations with banks which have no physical presence or "mind and management" in the jurisdiction in which they are licensed and which is unaffiliated with a regulated financial group subject to effective consolidated supervision (Shell banks'),
2. FIs should make a suspicious transaction report to the FIU in the event that FIs are approached by a shell bank or any institution that the FI has reason to suspect that it is a shell bank.
3. FIs should not enter into or continue business relationships with respondent FIs in foreign jurisdiction if they permit their 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. Whenever a correspondent relationship involves maintenance of "payable-through accounts", the FIs should ensure the following :(This specifically applies due to the fact that under the correspondent relationship, a customer of the respondent who is not a customer of the correspondent may have direct access to an account of the customer).
   (i) the respondent FI has performed all normal CDD obligations on those of its customers who have direct access to the accounts of the correspondent FI,
   (ii) conducts on-going monitoring in relation to the customer

(iii) the respondent FI will be able to provide relevant customer identification information upon request to the correspondent FI.

2. When a correspondent FI asks for documents, data or information mentioned under Item 11.6.1 above and the respondent FI fails to comply with the request, the correspondent FI must terminate the customer's access to the accounts of the correspondent FI (s).

11.7. Power of Attorney

When power of attorney authorizes the holder of power of attorney to exercise control over the assets of the guarantor, the following should be ensured by the FI:

a. Before getting involved in or associating with any transaction involving the power of attorney, the FI should conduct customer due diligence measures for the holder of power of attorney and the guarantor
b. The FI should consider the holder and guarantor of power of attorney to be their customers.

11.8. Bearer shares and share warrants to bearer

1. Wherever applicable to FIs, FIs should have adequate AML/CFT customer due diligence policies, procedures, systems and controls for risks related to use of bearer negotiable instruments.
2. Before being involved or associated with a transaction involving conversion of a bearer instrument to registered form, or surrender of coupons for a bearer instrument for payment of dividend, bonus or capital, the FI must apply enhanced customer due diligence measures to the holder of the instrument and / or any beneficial owner. The holder and any beneficial owner should be taken as customers of the FI.

11.9. Wire transfers

This item should be applied to wire transfers exceeding **QR 4000** or equivalent in foreign currencies at the relevant time, whether sent or received by the FIs. This item shall not be applied under the following:

a. When a transaction is carried out using a credit or debit card, when the card number accompanies all transfers flowing from the transactions and the card is not used as a payment system to effect money transfer,

b. When a transfer is from one FI to another FI and the originator and recipient are both FIs acting on their own behalf.

11.9.1 Outgoing Transfers

1. FIs should include all required originator information details with the accompanying electronic transfers of funds that FI's make on behalf of their customers.
2. The FI should apply due diligence measures in terms of information to be obtained from the originator (full originator information) of outgoing transfers, including:-
   A- Name of originator
   B- [285]Account number or reference number in the absence of an account
   C- ID or passport number
   D- Address
   E- Information of the beneficiary (name, address, account number, if any)
   F- Purpose of the transfer
3. The FI should verify all the information in accordance with the procedures and measures stated herein, before making any transfer. In case of batch transfer, the issuing FI (as the case may be) should include the account number or reference number of originator in the absence of any account in his name, provided that:

A- The FI maintains complete information about the originator as provided for at **11.9.1.2** above,

B- The FI is capable of providing the receiving financial institution with required information within three working days from the date of receiving any application in this regard.

C- The FI is capable of responding immediately to any order issued by the competent official authorities requesting access to this information.

4. The FI should ensure that non-routine transfers should not be batched as batching could increase the ML/FT risks in the FI. Such batching obligations do not apply to transfers made by a FI acting as principal, e.g. in case of spot foreign exchange transactions.

[285] In the event where the originator of the transfer does not hold an account at the bank, the banks shall establish a system which gives the originator a distinctive reference number.

11.9.2 Incoming Transfers

1. The FI should draw up effective systems to detect any missing information related to the originator (transfer applicant).
2. The FI should request the party originating the transfer to submit all missing information, and in the event where the originating party fails to do so, the FI should take appropriate actions based on the risk rating assessment, including the refusal of the transfer.
3. The FI should consider these circumstances when evaluating the extent of suspicion about the transaction under reference and refer the same to the Money Laundering Reporting Officer for consideration and judgment whether it is appropriate or not to report it to the FIU.

11.9.3 Obligations of Intermediary FI

1. In the event where the FI performs its role as intermediary FI in the execution of the transfer, (i.e. it is not the issuing or receiving FI) the FI should keep all the information attached to the transfer.
2. If the FI fails to obtain the information attached to the transfer (for technical reasons), it should keep all the other information available, whether they are complete or not.
3. If the intermediary FI receives incomplete information about the originator, it should inform the receiving FI of the missing information upon performance of the transfer.
4. Whenever, any technical limitations prevent the full originator information accompanying the wire transfer from being transmitted with a related domestic wire transfer, a record must be kept for **5 years** by the receiving intermediary FI, of all information received from the originating FI.

11.10. Non-profit Organization

The FI should not offer any financial services to non-profit organizations such as charity, humanitarian, cooperative and vocational associations and societies, unless the following requirements are satisfied:

1. Obtain all Customer Identification data such as the name of the association or society, legal form, address of head office and branches, types of activity, date of establishment, names and nationalities of representatives authorized to

access the account, telephone numbers, purpose of business relationship, sources and uses of funds, approval of competent authority for opening the account at the FI, and any other information required by the competent authority (Ministry of Social Affairs).

2. Verify the presence and legal form of the society or the association through information contained in its official documents.
3. Obtain supporting documents indicating the presence of an authorization issued by the association or the society to the persons authorized to access the account, and necessarily identify the representative in accordance with the customer identification measures provided for in these regulations.

12-Interface or delivery channel risk

12.1. Risk assessment for interface risk

1. FI should assess and document the risk of money laundering, terrorist financing and other illicit activities posed by the mechanisms, electronic banking operations, other operations undertaken electronically etc. through which business relationships are started, conducted and maintained,
2. The intensity of the customer due diligence measures and on-going monitoring in relation to 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. FIs should 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,
2. The policies, procedures, systems and controls should include measures:
    a. To prevent misuse of technological developments in ML, TF schemes,
    b. To manage specific risks associated with non-face-to-face business relationship or transactions.
3. FI should include in its methodology of procedures how the customers will be scored in relation to the interface through which the business relationship is started, conducted and maintained.

12.3. Non-face-to-face business relationship and New Technologies

1. Non-face-to-face business relationship or transactions would be:
   A- those types of relationship or transactions concluded over internet, or other means of technological development,
   B- Services or transactions provided or conducted over internet, use of ATMs etc.
   C- Electronic point of sale (POS), using prepaid, re-loadable or account linked cards
2. The policies, procedures, systems and controls for these types of accounts should include seeking additional identification documents, apply supplementary measures to verify documents supplied, developing independent contact etc.
3. FIs should have specific and effective due diligence procedures that can be applied to non-face-to-face customers. In particular, FIs 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. Such measures may include, but not limited specifically to the following:
   D- Telephone contact with the applicant customer on an independently verified home, employment or business number,
   E- With the customer's consent, contact the employer to confirm employment,
   F- Procuring the salary details through official channel, etc.
4. FIs permitting payment processing through on-line services should ensure that monitoring should be the same as its other services and has a risk based methodology to assess AM/FT risks of such services.
5. FIs must refer to the Instructions issued to them by QCB from time to time with regard to Modern Technology and E-Banking Risks, and should ensure to comply with any e-banking regulations issued by QCB.

12.4. Reliance on Third Party

1. Any financial institution should only accept customers introduced to it by other financial institutions or intermediaries who have been subjected itself to FATF equivalent customer due diligence measures.
2. Where a FI delegates or relies on another FI or intermediary, which are third party, any part of the due diligence measures, the ultimate responsibility for meeting the requirements of customer due diligence as per the provisions of

Articles 22 to 33 of Law 4 of 2010 and these regulations remains with the FI concerned and not the third party.

3. Whenever an FI relies on third parties to perform some of the elements of the CDD process, the FI should immediately obtain the necessary information and documentation concerning the aspects of CDD process from the third party and take adequate steps to satisfy themselves that the identification data and other relevant documentations relating to CDD process are as per customer identification measures.
4. FIs should create a direct communication channel with the customer after seeking the documents, data and recommendations from the third party.
5. Where FIs have branches or subsidiaries in foreign jurisdiction, FIs should take into account in which jurisdictions they can rely on third party for introductions, based on the information available whether these countries apply FATF Recommendation adequately.
6. FIs should rely on third parties for introduction after taking a written confirmation from the introducer that all customer due diligence measures required by FATF 40+9 Recommendations have been followed and identity established and verified.
7. Whenever FIs are not satisfied that the introducer is in compliance with the requirements of FATF 40+9 Recommendations, the FI must conduct its own CDD on the introduced business relationship; may not accept any further introductions from the same introducers or even consider discontinuing the reliance on that introducer for CDD purposes.
8. FIs should furnish the details of third party introducers (like for e.g. the details of company, structure of the company, location of the company, business activities undertaken by them etc.) relied upon by them for CDD purposes and notify Qatar Central Bank prior to entering such arrangements.

13- Jurisdiction Risk

13.1. Risk assessment for jurisdiction risk

1. FIs should 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. Such association can be where the

customer lives, or business incorporated or otherwise established in foreign jurisdiction,

2. The intensity of customer due diligence measures and on-going monitoring required for customers in other jurisdiction must be proportionate to the perceived or potential risk posed by the respective jurisdictions.
3. Jurisdictions requiring enhanced due diligence would be those as under:
    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
    e. Jurisdictions with high propensity for corruption.
4. FIs should 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 FIs customers may be associated.
5. Policies and procedures of FIs should include methodology to score the risks associated with different jurisdictions.

13.2. Ensuring effectiveness of AML/CFT Regimes

1. FIs should consider the following 3 factors in order to assess the effectiveness of AML/CFT regimes in other jurisdictions:
    a. Legal framework
    b. Enforcement and supervision
    c. International cooperation
2. When considering the factors listed at **Item 13.2.1 above,** FIs should also consider the findings listed about the jurisdiction and published by international organizations, governments and other bodies, like FATF etc.

13.3. Jurisdictions with impaired international cooperation

1. FIs should guard against customers or introductions by third parties from jurisdictions in which the ability to cooperate internationally is impaired,
2. FIs should subject the business relationships from or to these jurisdictions to enhanced due diligence measures and enhanced on-going monitoring.

13.4. Non-cooperative and sanctioned jurisdictions

FIs should conduct enhanced due diligence measures and enhanced on-going monitoring in relation to transactions or business relationships arising from jurisdictions which have been identified by FATF as non-cooperative country or is subject to international sanctions.

13.5. Jurisdiction with high propensity for corruption

1. FIs should have methodology to assess and document jurisdictions that are vulnerable to high corruption.
2. FIs should conduct enhanced due diligence measures and enhanced on-going monitoring for customers from this jurisdiction.
3. Whenever PEPs from such jurisdictions are accepted as customers of FIs on approval from Board, FIs should take additional and appropriate measures to mitigate additional risks posed by PEPs from such jurisdiction.

14- Know Your Customer (KYC)

14.1. General Principle of KYC

KYC principle requires that every FI to know who its customers are, have necessary identification documents, data and information evidencing identification.

14.2. Customer Acceptance Policy and procedures

1. The FIs should develop clear customer acceptance policy taking into consideration all factors related to the customers, their activities and accounts and any other indicators associated with customer risk. The policy should include detailed description of customer according to their respective degree of risk, the basis on which business relationships with the customers will be scored taking into account their sources of wealth and funds, or as an occasional customer seeking to carry out a one-off transaction.
2. The policy should consider among other things to establish effective systematic internal procedures for establishing and verifying the identity of their customers and source of their wealth and funds.
3. These policies and procedures should be set out in writing and approved by the FI's Board of Directors.

14.3. Customer due diligence (CDD) - basic requirements

1. FIs should not establish any business relationship with a customer, unless the customer, relevant parties to the business relationship, including any beneficial owner, have been identified and verified.
2. FI should not establish anonymous accounts or deal with anonymous customers or establish accounts in fictitious names.
3. Once the relationship has been established, the regular business undertaken by the customer should be assessed at regular intervals against expected pattern of business activity. Any unexpected activity should be examined to decide whether any suspicion arises relating to ML & TF. In order to assess unexpected activities, FI should obtain and maintain information on:
    a. nature of business likely to be undertaken,
    b. pattern of transactions,
    c. purpose and reason for opening the account,
    d. nature and level of activity,
    e. signatories to account etc.
4. Whenever FI has not obtained satisfactory evidence of identity before establishment of business relationship:
    a. FI should not establish the relationship or carry out transaction for or on behalf of such relationship and
    b. Should consider making a STR to FIU.
5. FIs should apply CDD measures when an occasional customer conducts transaction. The threshold limit for a single occasional transaction in a single operation or several linked operations for an amount exceeding QR **55,000** or equivalent in foreign currencies at the relevant time as per the provisions of Article 23 of Law 4 of 2010.
6. FIs should apply CDD in case it has any doubt about the genuineness of the accuracy or adequacy of any customer identification data obtained earlier.
7. FIs should apply CDD in case it suspects the customer of ML or TF.
8. **Identification of beneficial owner:**
    a. For all customers, the FI should determine whether the customer is acting on behalf of another person. FI should take all steps to obtain sufficient identification data to verify the identity of that other person.

b. For customers that are legal persons or legal arrangements, the FI should take steps to:
    i. Understand the ownership and control structure of the customer,
    ii. Determine the natural person(s) who ultimately own or controls the customer.

14.4. General requirements on extent of CDD

1. FIs should decide the extent of CDD measures 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. FIs should be in a position to demonstrate to QCB that the extent of CDD measures is appropriate and proportional to the risks of ML/TF.

14.5. General requirements for on-going monitoring

1. FIs should conduct on-going monitoring for each of their customers.
2. FIs should pay special attention to all complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. FIs should examine the background and purpose of such transactions and record their finding. Such of these records should be maintained as per the requirements of record keeping given under **Item 21** (Documents, Record Keeping and Retention).
3. FIs should have policies, procedures, systems and controls for conducting on-going monitoring. Systems and controls should include:
    a. Flagging of transactions for further examination. Such examinations may be performed by a senior independent officer of the FI and appropriate follow-up action should be taken on the findings of such examination. In case of knowledge or suspicion of ML or TF raised by such examination, a report by the senior officer should be made to the Money Laundering Reporting Officer.
    b. The system for on-going monitoring should have the ability to review transaction on real time basis, i.e. as they take place.
    c. The on-going monitoring may be by reference to particular type of transaction or related to 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. FIs may not limit the approaches as given here. FIs may use stringent on-going monitoring processes.

4. Monitoring of one-off linked transactions:
    1- FI should have systems and controls which have ability to identify one-off transaction linked to same person.
    2- When FIs knows, suspects or has reasonable grounds to know that a series of linked one-off transactions are for the purposes of ML/TF, the FI should make a report to Money Laundering Reporting Officer.

14.6. FIs unable to complete CDD procedure for customer

When a FI is unable to complete the CDD procedure for a customer, it must:

a. immediately terminate any relationship with the customer and
b. consider whether it should make a suspicious transactions report to FIU.

14.7. Timing of customer due diligence

1. An FI should implement the customer due diligence measures outlined in Section 6 of Law 4 of 2010 and this regulation.
2. FI should undertake to implement the provisions of Article 23 of Law 4 of 2010 and also when:
    a. Establishing 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 change in the way the account with the FI is operated or material changes in the manner of conducting business relationship
    e. The documentation standards change substantially
    f. The FI has doubts about the veracity or adequacy of previously obtained customer due diligence information and documents
    g. CDD must be conducted on an existing customer when items (b) to (f) above are encountered.
    h. Carrying out one-off or occasional transactions above **QR 55,000**
    i. Carrying out wire-transfers above the prescribed threshold limit
    j. There is a suspicion of money laundering or terrorist financing.

14.8. Circumstances when CDD may be completed at a later stage

Verification of identity for CDD purposes can be completed at a later stage as per the provisions of Article 25 of Law 4 of 2010, where:

a. This is necessary in order not to interrupt the normal conduct of business
b. There is little risk of money laundering or terrorist financing and these risks are effectively managed.
c. The CDD process under Article 25 is completed as soon as practicable after contact is first established with the customer.

15- Customer Identification Documentation

15.1. General requirements of Customer Identification Documentation

1. FIs should ensure that the customer identification documentation should relate to customer as a physical person and the nature of customer's economic activity.
2. FIs should make and keep a record of all customer identification documentation that is obtained during the customer due diligence measures and on-going monitoring of a customer's business relationship.
3. FIs must make and keep record of how and when each of the steps of CDD measures for a customer was satisfactorily completed. This should be applied in relation to a customer irrespective of the nature and risk profile of the customer.
4. In order that the FIs mitigate the risks associated with ML/TF by using the business relationship and co-mingle proceeds of criminal activity with legitimate economic activity in order to disguise the origin of these funds, FIs must address them by:
    a. Identifying sources of customer's income and wealth and establish that such sources are not from criminal activity, the FI will be in a position to establish risks arising from customer and jurisdiction.
    b. Identify the purpose and intended nature of business relationship, by establishing that FIs can monitor the transactions on a real time basis and ensure that they correspond to the transactions intended under the business relationship. When the assessment identifies variances between the actual transactions conducted under the business relationship and the stated purpose and intended nature then the FIs should ensure and satisfy itself that they are not intended for ML/FT purposes.

c. When an FI is not satisfied about the variation in the intended transactions, FI should consider making a STR to FIU.

15.2. Customer Identification Documentation

The FIs should maintain the following documents as minimum requirements for the following types of customers:

1. Individuals

Customer identification data should include customer's full name, permanent address, telephone number, profession, work address and location, nationality, ID number for Qataris and residents (passport number for non-residents), date and place of birth, name and address of sponsor, purpose of business relationship, names and nationalities of representatives authorized to access the account.

2. Legal Entities

Customer identification data should include legal entity's name (company/institution), CR data, type of activity, date and place of establishment, capital, names and nationalities of authorized signatories, telephone numbers, address, purpose of business relationship, expected size of business, name and address of individual institution's owner (in case of individual institution), names and addresses of joint partners in case of joint ventures, names and address of shareholders whose shares exceed 10% of the capital of joint stock companies.

3. Holding Companies

In case of legal entities having multi-layered ownership and control structure, FIs must obtain the ownership and control structure at each level and document the same, apart from the verification requirements applicable to legal entities.

4. Unincorporated partnership

When a legal entity is an unincorporated partnership or association, the identity of all partners / directors must be obtained and verified.

5. Partnership

In case the entity is a partnership with formal partnership agreement, FIs must obtain the mandate from the partnership on:

(i) Authorizing establishing relationship with the FI

(ii) Empowering persons on behalf of the partnership

(iii) Authority to operate accounts.

6. Trusts, Clubs and Society

All requisite customer identification documents should be obtained by the FIs.

16- Enhanced CDD and on-going monitoring

General requirements for enhanced CDD & on-going monitoring

1. FIs should conduct enhanced CDD measures and enhanced on-going monitoring in cases where it is required under the provisions of Law or regulations, or when there is a perception of high risk of money laundering or terrorist financing.
2. Generally, enhanced CDD should be applied for the following categories:
    a. Non-face-to-face business and new technologies
    b. Politically Exposed Persons
    c. Correspondent banking relationships
    d. Bearer shares and share warrants to bearers
    e. Charities, clubs and societies
    f. Jurisdiction risks (mainly impaired international cooperation, non-cooperative and sanctioned jurisdictions and jurisdictions with high propensity for corruption),
3. FIs should, in addition, apply enhanced CDD on:
    a. **Non-resident customers** - The following measures should be observed while applying the identification procedures:
        i. Identify the purpose of the business relationship
        ii. Verify the validity of the entry visa initially while initiating business relationship.
        iii. Obtain a copy of the Passport

iv. Obtain a copy of the memorandum of association in case of legal entity, certified by the competent authorities in the country of origin or the embassy of country of origin in the State of Qatar

v. Obtain a copy of the CR or registration documents certified by the competent authorities in the country of origin or the embassy of the country of origin in the State of Qatar

b. Politically exposed Persons

c. **On customers belonging to countries that do not apply FATF Recommendations appropriately**. Risks will be greater when the customer belongs to a country that is subject to sanctions imposed by the UN or a country that does not apply sufficient legislations in terms of combating money laundering and terrorist financing or which is known to be affected by criminal activities, such as drug trafficking. Under such cases, apply enhanced CDD on customers coming from those countries and constantly and accurately monitor their accounts. FIs must assess and document risks of ML/FT from different jurisdictions with which their customers are associated. The intensity of CDD should be commensurate and proportionate to the perceived or potential risk from the jurisdiction.

d. FIs should also pay special attention to any dealings with the entities or persons who are domiciled in countries which are identified by FATF as being 'non-cooperative". Whenever, transactions with such parties are carried out which have no economic or visible lawful purposes apparently, the background and purpose of such transactions should be re-examined and finding documented by the FI and in case of reasons to believe that the transactions are related to ML/TF, this information should be submitted to the FIU.

e. **Third Party reliance for CDD**

f. **Interface or delivery channel risks**

g. **Private banking services -** Drawing appropriate policies and analyzing the product risks, taking into consideration the nature of those services. Factors may include:

i. Determine the purpose of the private banking service application.

ii. Development of the business relationship between the bank and the customer to whom the service is offered.

17-Simplified Customer Due Diligence

17.1. General Requirements for simplified CDD

1. Article 31 of Law 4 of 2010 allows simplification of CDD requirements. However, this will not limit FIs from enhancing the CDD measures if there is a suspicion of ML/TF.
2. FIs may apply simplified CDD measures on the following customers only:
    a. Ministries, Government authorities, and semi-government companies in the GCC countries.
    b. Financial institutions that is based or incorporated or otherwise established in Qatar, or those based, or incorporated or otherwise established in other jurisdictions that impose requirements similar to those of AML/CFT Law and these regulations, consistent with the FATF 40+9 Recommendations, and is supervised for compliance with those requirements.
    c. Companies listed in the securities' markets across the GCC and those which apply disclosure standards equivalent to those required by the QFMA/Qatar Exchange.
    d. In the event where a one-off or occasional transaction is undertaken, where the amount of transaction(s) or related transaction(s) does not exceed QR **55,000** or equivalent in foreign currency, it may be sufficient to obtain the name and contact details of the customer.
    e. FIs wishing to apply simplified CDD measures on the above customers must retain documentary evidence supporting their categorization of the customer.
    f. Simplified CDD should not be applied where FI knows, suspects, or has reason to suspect, that the customer is engaged in ML/TF or that the transaction is carried out behalf of another person engaged in activities of ML and TF.
    g. Simplified CDD should not be applied by FI if it knows, suspects, or has reason to suspect, that the transaction are linked and intended to exceed the threshold specified under **Item 17.1.2(d) above.**

18- Reporting

18.1. General Reporting Requirements

Any unusual or inconsistent transaction by a customer's known legitimate business and risk profile, by itself does not make it a suspicious transaction. In this regard a FI has to consider the following:

1- Whether the transaction has no apparent or visible economic or lawful purpose,
2- Whether the transaction has no reasonable explanation,
3- Whether the size and pattern of transaction is not similar to the earlier pattern or size of same or similar customers,
4- Whether the customer has failed to furnish adequate explanation or information on the transaction,
5- Whether the transaction is made from a newly established business relationship or is a one-off transaction,
6- Whether the transaction involves use of off-shore accounts, companies etc that are not supported by the economic needs of the customer,
7- Whether the transaction involves unnecessary routing of funds through third parties
8- The list of possibilities is only indicative and FIs may consider any other relevant issue to assess if the transaction is in the nature of unusual or inconsistent.

18.2. Internal Reporting requirements

1. FIs should have clear and effective policies, procedures, systems and controls for internal reporting of the known or suspected instances of ML & TF,
2. These policies, procedures, systems and controls for internal reporting should enable the FI to comply with the AML/CFT Law, regulations and also enable prompt making of internal suspicious transactions report to the Money Laundering Reporting Officer.
3. The FI should ensure that all officers and employees have direct access to the FI's Money Laundering Reporting Officer and also that the reporting hierarchy between the officers and employees are short.

4. All officers and employees of the FI are obligated to report when they have reasonable grounds to suspect that funds channeled through the FI are proceeds of criminal conduct or related to TF or linked, related to or are to be used for terrorism or terrorist act or by a terrorist organization.
5. The officers and employees of FI should promptly make an internal STR to the Money Laundering Reporting Officer. On making such an internal STR to Money Laundering Reporting Officer, the officer or employee should promptly report all subsequent transactions details of the customer until required by the Money Laundering Reporting Officer.
6. Such internal STRs to Money Laundering Reporting Officer should be irrespective of amount of transaction.

18.3. Obligation of Money Laundering Reporting Officer on receipt of internal reports

On receipt of the internal reports from the officers or employees of FI, Money Laundering Reporting Officer should:

a. properly and appropriately document the report
b. furnish a written acknowledgment to the officer or employee, together with a reminder of the provisions relating to tipping off
c. consider the internal report in the light of all other relevant information available with the FI and decide whether the transaction is suspicious and furnish a notice to the officer or employee of the decision of the Money Laundering Reporting Officer.

18.4. External Reporting requirements

1. FIs should have clear and effective policies, procedures, systems and controls for reporting all known or suspected instances of ML or TF to FIU.
2. These policies and procedures of FI should be able to comply with AML/CFT Law, regulations in relation making of STRs to FIU promptly and speedily and also to cooperate effectively with the FIU and law enforcement agencies in relation to STRs made to FIU.

18.5. Obligation of FIs to report to FIU

1. FIs are statutorily obligated under the provisions of Law 4 of 2010 to submit a report to FIU,
2. When FIs are aware, suspects or has reasonable grounds to know or suspect that funds are proceeds of criminal conduct, or related to TF or linked or related to, or are to be used for, terrorism, terrorist acts or by terrorist organization, FIs are obligated to make a report to FIU.
3. The FI should immediately make a STR to FIU and ensure that any future or proposed transaction relating to the report does not proceed without consultation with FIU.
4. The STR to FIU should be made by the Money Laundering Reporting Officer, or Deputy Money Laundering Reporting Officer of FI (**Refer to Item 7.2.8 and 8.4 above)**.
5. FIs should make STRs to FIU as given under **Item 18.5.2 above,** irrespective of the fact that an internal STR has been made under the requirements of **18.2 above** to the Money Laundering Reporting Officer, or irrespective of the amount of transaction.

18.6. Matters to be included in the Report

The report to be made to FIU should include:

a. Facts or circumstances on which the FI's knowledge or suspicion is based, and
b. the grounds for FI's knowledge or suspicion.

18.7. Obligation on part of FIs not to destroy records relating to customer under investigation

1. When FI makes a STR to FIU in relation to a customer, such customer is bound to be under investigation and surveillance of law enforcement agencies in relation to AML/CFT.
2. Under such circumstances where FI has made a report to FIU and the customer is under investigation, the FI should not destroy any records relating to the customer or business relationship without consulting FIU.

18.8. Restricting or terminating business relationship of customer under investigation

As a commercial practice, the FI may restrict or terminate the business relationship with a customer after the FI has made a STR to FIU. However, before restricting or terminating the business relationship, the FI should:

a. Consult FIU in the matter, and
b. Such action should not inadvertently result in tipping-off the customer.

18.9. Records to be maintained by Money Laundering Reporting Officer

The Money Laundering Reporting Officer should make and maintain records relating to:

a. Details of each of the internal STRs received
b. Details relating to Obligations of Money Laundering Reporting Officer under **18.3.**
c. Details of each STR made to FIU.

19- Tipping off

19.1. FIs to ensure no tipping off occurs

1. Tipping off is prohibited under the provisions of Article 39 of Law (4) of 2010
2. FIs should ensure that its officers and employees are aware of and sensitive to the issues surrounding and consequences of tipping off.
3. FIs should have policies, procedures, systems and controls to prevent tipping off.
4. In case FI believes or has reasonable grounds to believe that a customer may be tipped off by conducting CDD measures or on-going monitoring, the FI should make a STR to FIU instead of conducting CDD measures or monitoring.
5. When a FI makes a STR to FIU based on **Item 19.1.4 above,** the Money Laundering Reporting Officer should make and maintain record to the effect to demonstrate the grounds for belief that conducting CDD measures or on-going monitoring would have tipped off the customer.

19.2. Internal measures to safeguard information relating to STRs

1. FIs should take all reasonable measures to ensure safeguarding information relating to internal STRs

2. In particular, FIs should ensure that information relating to internal STRs are not disclosed to any person, other than members of Board of FI, without the consent and permission of the Money Laundering Reporting Officer.
3. The Money Laundering Reporting Officer should not accord permission or consent to disclosure of information relating to internal STR to any person, unless Money Laundering Reporting Officer is satisfied that such disclosure would not constitute tipping off.
4. Whenever the Money Laundering Reporting Officer consents to disclose the information relating to internal STR, Money Laundering Reporting Officer should make and maintain a record.

20- Screening and training requirements

20.1. Specific requirements for screening procedures

1. FIs should ensure to comply with the provisions of Article 35 (1) of Law 4 of 2010 on screening and Article 35 (2) on training.
2. For the purpose of screening, individuals may be classified as under:
    a. Higher-impact individual – such individuals are those who have a role in preventing ML/TF under the FIs AML/CFT programme, [For the purpose of clarification, these category of individuals will be Senior Official, Money Laundering Reporting Officer or Deputy, any individual who may perform the controlled functions, (i.e. official carrying out a regulated activity of the FI)], in the FI, and
    b. Other individuals
3. FIs screening procedures for appointment or employment of officers and employees should ensure that, the officers and employees in the higher impact category, should have appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently. In the case of other individuals who do not fall under the higher impact category, FI should ensure and be satisfied about individual's integrity.
4. The screening procedure at a minimum, prior to appointment or employment, should ensure to:
    a. Obtain and confirm references about the individual
    b. Confirm the employment history and qualifications

c. Seek information or details about any criminal convictions, regulatory action if any, and verify the same.
d. Take appropriate and reasonable steps to confirm accuracy, completeness of the information obtained by the FI for screening purposes.

20.2. AML/CFT Training programme

1- FIs should identify, design, deliver and maintain an appropriate and adequate on-going training programme on AML/CFT for its officers and employees.
2- The training programme should envisage that the officers and employees of FI understand:
   a. the legal and regulatory responsibilities and obligations under AML/CFT Law and regulations
   b. their role in preventing ML and TF and the liability devolving on officers and employees and FI due to their involvement in ML or TF and failure to comply with AML/CFT Law and regulations.
   c. the FI's management of ML & TF risks, role of Money Laundering Reporting Officer, importance of CDD measures and on-going monitoring, typologies of ML & TF, threats of ML & TF, methods and trends, vulnerabilities of the products offered, recognition of suspicious transactions, processes and procedure of making internal STRs, etc.
3- While considering the training needs FIs should consider issues like, existing experience, skills and abilities, functions and roles intended, business size and risk profile of FI, outcome of earlier training and needs envisaged, etc.

20.3. Maintaining and reviewing training

1. FI's AML/CFT training should be on-going to ensure that the officers and employees maintain the AML/CFT knowledge, skills and abilities and keep these up-to-date and in line with the new developments, including latest AML/CFT techniques, methods and trends.
2. FI should carry out review of training needs at regular intervals in order to ensure that the objectives envisaged above are met.
3. The Board of FI should consider the outcome of each such review. Whenever the review identifies deficiencies in AML/CFT training requirements, the FI should

prepare and approve an action plan to remedy the identified deficiencies in a timely manner.

21-Documents, Record Keeping and Retention

1. FIs must keep and maintain all documents and records related to the following at least for a minimum period of mentioned below:
   A- Financial Institution should maintain all necessary records on transactions, both domestic and international, for a period of fifteen years following the completion of the transaction. This is regardless of whether the account or business relationship is ongoing or has been terminated.
   B- Regarding the accounts opened for natural persons or legal entities or other banks and financial institutions, documents and records related to those accounts should be kept for a period of fifteen years at least starting from the date of closing the account.
   C- Regarding 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 should be kept for a period of fifteen years at least from the date of executing the transaction.
   D- Regarding unusual and suspicious transactions, records should be kept for a period of fifteen 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 wire transfer as given at **Item 11.9.4.3** should be retained for 5 years.
   F- Training records should be retained for a period of 5 years.
   G- Retrieval of records – The records and regulations relating to AML/CFT should be able to be retrieved without undue delay.

2. FI should update these data periodically and ensure that the judicial authorities and competent authorities entrusted with the enforcement of AML/CFT Law have timely access to these documents and records, as and when necessary.

22- Internal and External Auditing

1. The internal auditing function should review the effectiveness of the procedures and control systems applied in respect of AML/CFT on an annual basis, by the FIs for their branches and subsidiaries inside and outside Qatar. All appropriate actions should be taken to fill any gap or update and develop the said procedures and systems to ensure their effectiveness and adequacy.
2. The external auditor should, among other functions, ensure that the FIs applies these regulations and verify the adequacy of the policies and procedures applied by the FIs in this regard. It should also include the results of such review in the management letter and inform QCB immediately of any major violation of these regulations.

23- Sanctions

Sanctions relating to AML/CFT shall be applied as per the provisions of Law (4) of 2010.

24- Approved Forms to be used

QCB would approve the forms that are required to be completed for the purposes of AML/CFT Law or these regulations.

25- Regulations effective from

The present regulations will come into force as on the date of issue and all other regulations on AML/CFT for financial institutions are cancelled.

APPENDIX

A. Miscellaneous issues for guidance

1. Processes of Money Laundering

There are three stages of Money Laundering as under:

(a) **Placement** – involves introduction of illegally obtained funds into the financial system, usually through FIs. This is achieved through cash deposits, purchase of financial instruments for cash, currency exchange, purchase of security or

insurance contracts, check cashing services, cash purchases or smuggling of cash between countries.

(b) **Layering** - usually 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 transfers to other banks, purchase and sale of investments, financial instruments, insurance contracts, phony or bogus investments or trade schemes etc.

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

2. Money laundering through cash transactions

1. Large cash deposits not in line with the customer's type of business or occupation.
2. Numerous cash deposits of small amounts, which is known as structuring or smurfing, in order to avoid detection.
3. Cash deposits followed by a transfer (wire transfer, bank check etc.)
4. Structured cash payments for outstanding credit card balances, with relatively large sums as payments.
5. Depositing cash through multiple deposit coupons, in such a manner that each deposit operation is performed separately in small amounts so not to draw attention of authorities, but when calculated together the total deposits would reflect a huge amount.
6. Constant deposit operations through cheques, transfers or marketable instruments.
7. Attempts to replace smaller denomination currency notes with higher denomination currency notes.
8. Branches showing cash transactions that exceed the usual limits, in relation to their usual positions' statistics.
9. 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 would be usually undertaken as under:

1. 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.
2. Cash settlement between external payments (payment orders, transfers) and the customer's balances on the same or previous day.
3. Deposit of cheques in large amounts by third parties endorsed in favor of the customer.
4. Large cash withdrawals from an account that was previously inactive, or from an account which was fed with unusual large amounts from outside.
5. Multiple deposits by a large number of individuals into one account, without any clear explanations or clarifications.

4. Money Laundering through financial transaction associated with investment activities

It would as follows:

1. Loan/deposit transactions with subsidiaries or affiliates of FIs located or operating in areas known to be affected by ML/drug trafficking etc.
2. Applications submitted by customers for purchase or sell investments or services (whether foreign currencies or financial instruments) with obscure source of funds, or sources that do not correspond with their apparent activity.
3. Large cash settlements for purchase or sale operations of securities.

5. Money laundering through cross-border activities:

It may be represented in the following forms:

1. Customer introduced to the bank by an external financial institution located in a country known to be affected by criminal drugs production and trafficking.
2. Customers paying /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 drugs production or trafficking or in relation to the prohibited terrorist organizations, or countries offering opportunities for tax evasion.
3. Incoming or outgoing transfer operations executed by a customer without using any of his accounts at any bank.

4. Constant and regular withdrawal/deposit of cheques issued in foreign currencies or travel cheques into the account of the customer.

B. Typologies

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. FIs should update the new typologies applicable to their area of business. Such information is available from FATF and MENA FATF web-sites.

Some of the examples are as under:

1. Alternative remittances channels (hawala, hundi etc) – are informal mechanisms based on 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.
2. 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.
3. Currency exchanges / cash conversion – through usage of travelers check or extensive usage of exchange house.
4. Cash couriers / currency smuggling – concealed movement of currency across border.
5. Purchase of valuable assets – criminal proceeds are invested in high value good like real estate, shares, gold etc.
6. Use of wire transfers
7. Trade based ML – involving invoice manipulations and using trade financing routes and commodities.
8. Mingling – by combining proceeds of crime with legitimate business monies.
9. Use of shell companies – used to obscure the identity of persons controlling funds.

C. Guidance by International Bodies

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

****

Second: FATF Statement on AML and CFT

The FATF statements are issued regularly on countries that are considered risk on the world financial system and the list of the countries that have achieved progress in rectifying the strategic deficiencies in anti-money laundering and terrorism financing. All banks should review these assessments and measure risks of dealing with these counties. In additions to circular no. (67/2008), (84/2008), (77/2009), (81/2010), (30/2012) which are relevant to this issue.

List can be viewed on the internet: www.fatf-gafi.org.

New relevant circulars issued on The UN web-site:

112/2012 - 109/2012 - 107/2012 - 106/2012 - 5/2013 - 7/2013 - 8/2013 - 13/2013- 14/2013 - 18/2013 - 25/2013 - 21/2013 - 23/2013 - 27/2013 - 31/2013 - 32/2013 - 33/2013 - 34/2013 - 35/2013 - 37/2013 - 39/2013 - 49/21013 - 54/2013 - 51/2013.

(AML) and (CFT)

Third:[286]Financial Information (FIU) Unit's Guidance and STR Forms

A. In view of the FIU's letter ref. (و م م/ ن م ح/286/2010) dated 25/4/2010 concerning issuing its guidance and reporting on the suspicious transactions in money laundering and terrorism financing.

Pursuant to article (19) of law no. 4 of the year 2010 on AML and CFT, attached hereto guidance and form of STR reported to the FIU in the annexes mentioned below. All banks must comply with these guidance and forms as from 20/5/2010.

- Guidance, annex no. (150)
- STR form, annex no. (151)

B. [287]Updating Data of Money laundering reporting officer and his deputy

All banks should fill in annex no. (154) and provide QCB within maximum deadline one week from 24/8/2011. Kindly notify QCB with any new details in this regard.

[286] Refer to circular no. (46/2010) dated 20/5/2010.
[287] Refer to circular no. (65/2011) dated 24/8/2011.

(AML) and (CFT)

Fourth: [288]National Anti money laundering and Terrorism Financing Committee Guidance on Mechanism to revise matching of names, persons, and entities with Security Council Sanctions Lists

In accordance with Article no. (50) of law no. (4) of the year 2010 on Anti money laundering and terrorism Financing, we attach herein the National Anti money laundering and Terrorism Financing Committee's Guidance on Mechanism to revise matching of names, persons, and entities with security Council Sanctions Lists. Please comply with this Guidance as from 29/4/2012.

[288] Refer to circular no. (35/2012) dated 29/4/2012.