Regulation on Anti-Money Laundering (AML) And Combating Financing of Terrorism (CFT) for financial institutions (FIs)

Having perused Decree Law No. 33 of 2006 (Qatar Central Bank), and Law No.28 of 2002 on Anti-Money Laundering, together with Law No. 21 of 2003 on amendments to some provisions of Law 28 of 2002 (Anti-Money Laundering Law) and Law No. 3 of 2004 (Combating Terrorism), QCB has decided that all licensed banks in the State of Qatar shall comply with the AML/CFT regulations given hereunder.

These regulations are issued under the provisions of Article 65 read with Article 5(12) of Law 33 of 2006. Any contravention thereof or non-compliance with these regulations shall attract penalties as applicable under Law 33 of 2006.

1. Definitions:

Financial Institutions	Constitutes any bank or a financial services institutions (investment & finance companies and exchange houses) as given under Law 33 of 2006.
Money Laundering (ML):	The process of depositing or dealing with funds obtained from transactions originating from illegitimate or suspicious sources.
Terrorist Financing (TF):	The process of using any funds or other assets in financing terrorist acts or terrorist organizations
Occasional Customer:	An irregular or a customer who deals with the financial institution without having a continuing relationship with the FI.
Beneficial Owner:	Natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted.

	It also includes those persons who exercise ultimate and effective control over a legal person or arrangement.
Shell Bank:	A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management. The existence of a local agent or low level staff does not constitute physical presence.
Batch Transfer:	Transfer comprised of a number of individual wire transfers that are being sent to the same FI, but may or may not be ultimately intended for different persons.
Politically Exposed Persons (PEPs):	Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, political parties' officials and their family members' up to third degree.
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)
Wire transfer:	It means 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.
Reduced due diligence:	It means reducing some Customer Due Diligence (CDD) measures when verifying customer's identity.
Tipping-off	In relation to a business or customer of FI is the unauthorized act of disclosing information that may result in the customer knowing or suspecting that the customer is subject of Suspicious Transactions Report or an investigation relating to ML/FT, which may jeopardize prevention or detection of offences, apprehension or prosecution of offenders, recovery of proceeds of crime or prevention of ML/FT.

2. Scope of Application:

These regulations are applicable to all financial institutions, viz., **Banks, Investment and Finance Companies and Exchange Houses**, licensed and supervised by Qatar Central Bank. FIs must adopt and apply the specific areas of this regulation as appropriately applicable to them.

2.1. **General AML/CFT Responsibilities:**

1. FIs should develop and establish appropriate programme against ML/TF
2. The extent of the programme should be commensurate to the size and nature of business and the potential AML/CFT risks it might face
3. At a minimum, FIs should:
    i. Have internal policies, procedures, systems and controls to prevent ML/TF

ii. Have high screening standards and procedures while appointing officers and staff to manage AML/CFT

iii. Have an on-going training programme

iv. Have an independent audit function to test compliance of AML/CFT policies, procedures, systems and controls in the FIs.

4. Policies , procedures, systems and controls should cover the following:

i. CDD Measures

ii. On-going monitoring

iii. Detection of unusual and suspicious transactions

iv. Reporting requirements

v. Communication of AML/CFT requirements internally to its officers and employees.

5. Any other issues that may be related to AML/CFT and not limited to the extent stated under (1) to (4) above.

2.2. FIs AML/CFT policies, procedures, systems and controls should be risk sensitive and risk based, having regard to the size, complexity and nature of business, together with the risk of ML/FT appropriate to the FIs.

2.3. The regulation on AML/CFT should be adopted by FIs, their branches and financial subsidiaries. In case of any difference in application of AML/CFT requirements between the home country regulator and the host, the stringent requirements should be applied, to the extent authorized by the laws and regulations of the host country. However, if the requirements of the host jurisdiction prevent application of the provisions of this regulation to branches/subsidiaries of FIs, the concerned FI should inform QCB about the same.

3. Board Responsibility

3.1. The FIs must ensure the following:

1. The Board of Directors of the FIs shall have the overall responsibility for establishing and managing effective AML/CFT system.
2. For FIs having branches and subsidiaries outside the State of Qatar, a group policy should be established in order that its overseas branches and subsidiaries adopt the anti-money laundering strategies, internal controls, procedures and process as per the minimum requirement specified under this regulations or host country regulations. In case the host country regulations are more rigorous, the higher standards must be applied.
3. The Board shall be responsible for appointment of Compliance Officer, with adequate experience in AML/CFT issues. The Compliance Officer must have sufficient seniority, adequate resources, timely access to all information relating to CDD and AML/CFT issues of the FI.
4. Robust MIS is available so that regular, timely and appropriate information is made available to the Board and / or Senior Management relating to AML/CFT risks or issues of the FI.
5. The Compliance Officer shall be the focal point on issues relating to AML/CFT. Compliance Officer shall liaison with the internal and external authorities and also handles reports on suspicious transactions.
6. Ensure that whenever suspicion on AML/CFT arise in the overseas branches, there must be a reporting system in place to report the same as per the requirements of the host country, such reporting should also be made available to QCB and FIU as the case may be, for their information.
7. Decide the extent of MIS and reports required by them in order that the Board or Senior Management discharges their AML/CFT responsibilities.
8. In case of FIs outsourcing any of its functions or activities, the Senior Management should ensure that appropriate assessment is made of any possible AML/CFT risk associated with such functions. The FIs remain responsible for

ensuring AML/CFT compliance. The FI should ensure through service agreements that the requirements of AML/CFT are complied.

9. Ensure that the FIs has policies and procedures in place to impart effective training to its employees manning AML/CFT issues. The training should ensure that the staff understands their legal and regulatory responsibilities, the role in identifying, handling, and managing AML/CFT risks.
10. Ensure to have appropriate internal processes and systems for the purpose of making Suspicious Transactions Reports (STRs).
11. Ensure that appropriate policies and measures are in place in order to assess AML/CFT issues in their day-to-day operations.
12. Consider the Annual report of the Compliance Officer and take appropriate necessary action or remedial measures to rectify deficiencies.

4. The Role of Compliance Officer for AML/CFT issues

The overall responsibility of AML/CFT prevention lies with the Board of Directors and Senior Management. The Compliance Officer for AML/CFT issues shall be responsible for overseeing the AML/CFT risks and following up on the AML/CFT processes, procedures and strategy. The Compliance Officer's appointment shall be in accordance with the QCB Instructions. However, FIs need to ensure that the CO is employed at the Management Level, is sufficiently senior in order to enable him to act independently and report directly to the Audit Committee. The Compliance Officer shall have the following responsibilities within the AML/CFT framework:

1. The Compliance Officer (CO) should ensure to comply with the requirements of AML/CFT under the various Law issued by the State, regulations on AML/CFT issued by QCB
2. The CO will determine the appropriateness of information received relating to transactions that may be deemed to be suspicious, or give rise to any knowledge or suspicion that a customer may be engaged in AML/CFT.

3. Supporting and coordinating with Senior Management's focus on ML/FT risk in all business areas.
4. The CO and the appropriate staff designated to assist the CO should have timely access to customer identification data and other CDD information, transaction records and all related relevant information on AML/CFT.
5. Receive information and reports about unusual and suspicious transactions. The CO will take appropriate steps to validate these reports or information in order to judge if the same needs to be reported to FIU. While making such a judgment, the CO may also verify and consider all other relevant information, review transactions pattern etc. The CO will undertake to report suspicious transactions to FIU. The branches / subsidiaries of FIs should furnish STRs to the CO.
6. The CO will be responsible for maintenance of all documents, records and reports received on matters relating to AML/CFT.
7. The CO will be responsible for coordinating with the Senior Management to manage AML/CFT risk and carry out regular assessments on the adequacy of its systems and controls available to manage these risks.
8. The CO shall prepare periodic reports on all unusual and suspicious transactions. These reports should be made available to the Audit Committee of the Board in case of local bank or to the General Administration in case of branches of foreign banks or appropriate Committee in case of other FIs. Main findings of such reports and information available with the CO should be made available to competent authorities and auditors as and when necessary. Such periodic reports shall be maintained as per the requirements under "Documents and Record Maintenance".
9. The CO should ensure that the FIs, their branches / subsidiaries provide timely, unrestricted access to Senior Management, the CO, regulatory authorities and FIU to documents and information relating to ML/FT issues, except otherwise to the extent prevented under the rules of other jurisdictions.
10. Receiving and acting on government, regulatory and international findings on AML and CFT.

11. The CO on an annual basis must submit a report to the Audit Committee. The annual report must consist of details relating to the operation, effectiveness of AML/CFT systems in the bank, the number and types of internal suspicious transaction reports, the number of such STRs submitted to FIU, reasons for not referring some of the STRs to FIU, suggestions and recommendations for improving AML/CFT systems, with areas where deficiencies have been noticed, recommendations of the Audit Committee of Board or similar Committees and internal or external auditors on the adequacy of systems and controls.
12. The CO must discharge his functions honestly, reasonably, independently while investigating and assessing internal suspicious transaction reports and deciding whether to make, and making STRs to FIU.

5. Risk Based Monitoring

5.1. FIs shall lay down systems and procedures for management of AML/CFT risk on a risk based basis, which shall include classification of customers and business relationship. These risk classification may made under 3 categories, high risk, medium risk and low risk. These risk categories should be revised atleast on an annual basis or on occurrence of any development that may require revising the risk category of customers or business relationships.

5.2. When profiling the risks, FIs should take into account the risks such as customer risk, product risk, transactions risk, and country risk. FIs must identify any other risks relevant to business relationships. By combining all the above, FIs should be in a position to arrive at a risk profile of the business relationship. FIs should be able to demonstrate to QCB and other competent authorities that it has system and methodology to assess the above risks, and the day-to-day operations follows this methodology on a consistent basis, i.e. its practice matches methodology.

5.3. The risk assessment process must include recognizing the risks posed by natural persons, legal entities, or products etc. Similarly, it must also include profiling of risk posed by beneficial owner, officers, shareholders, trustees, settlers, managers and other relevant persons and entities. Such profiling should assess the potential lack of transparency or ability to conceal by the entity.

6. Customer Due Diligence (CDD)

6.1. Customer Acceptance Policy (CAP)

The FIs should develop clear customer acceptance policies 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 income and wealth.

6.2. General Rules of applying CDD

6.2.1. FI must apply CDD measures:

(i) when establishing a business relationship,

(ii) when carrying out occasional transactions in single operation or several linked operations, beyond the threshold fixed in the regulations,

(iii) when there is a suspicion of AML/CFT without regard to any limits or when there are doubts about the genuineness or adequacy of the previously obtained customer identification data.

6.2.2. The following should be complied with by the FIs:

1. Should not establish anonymous accounts or deal with anonymous customers or establish accounts in fictitious names.
2. Identify the customer and verify customer's identity based on documents, data and other information.

3. FI should also identify wherever applicable, beneficial owner. FI must establish, verify and validate the identity of the customer or any other person who may be acting or proposing to be acting on behalf of another natural person or legal entity.
4. Should apply CDD measures in terms of customers or beneficial owners in the following cases:
    a. Establishing on-going business relationship with new customers and the nature of their business they may conduct
    b. Carrying out occasional transaction in a single operation or several linked operations for an amount exceeding QR 75,000 or equivalent in foreign currencies.
    c. In case the FI has any doubt about the genuineness of the accuracy or adequacy of any customer identification data obtained earlier, or
    d. In case the FI has suspicion on any transactions relating it to AML/CFT.
5. In order that the CDD is complied with, the FI should obtain information on the nature of business that the customer is expected to undertake, the pattern of transactions, including the purpose and reason for opening the account, business relationships, nature and level of activity, signatories to the account etc.
6. The FI is not authorized to initiate any business relationship or execute any transaction before obtaining satisfactory evidence of identity and other CDD measures stipulated in this regulation.
7. The bank or other entities of the FI (where ever applicable) may open an account or establish business relationship by delaying the CDD process, provided there are adequate safeguards to ensure that AML/CFT risks are mitigated and controlled.
8. In any event where the FI initiates business relationship without being able to satisfy all aspects of CDD measures, the said relationship should be terminated and the FI must consider making a report to FIU immediately in accordance with the "Reporting Procedure".
9. The FI should periodically and within a maximum period of 5 years update the data on the customer identification, taking into account the level of risk of the

customer. While reviewing periodically, bank should ensure to maintain accurate and up-to-date documentation with reference to CDD. The maximum period mentioned above for updating customer identification data may be reduced taking into account the level of risk of the customer. This time frame will not be limiting the FI from updating if (i) the FIs documentation standards change substantially (ii) there are material changes in the way an account is operated or (iii) if there are material changes in any other aspect of business relationship with the customer. In case of any doubt regarding the accuracy of data or information or the customer, the customer should be requested to identify the beneficial owner and provide the bank with updated data on the latter along with supporting documents.

7. Customer Identification Measures

The FIs should maintain the following documents as minimum requirements:-

7.1. Natural Person

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.

7.2. Legal Entities

1. 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.

2. **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.

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

4. **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.

5. **Trusts, Clubs & Society** – All required identification details must be obtained by the FI.

6. **Products**

FIs must assess and document the risks in ML/FT and other illicit activities posed by different products promoted by them. FIs must accordingly have customer due diligence relative to the intensity of particular type of product proportionate to the potential level of risk of the product.

FIs should have policies, procedures, systems and controls to address specific risks of ML/FT for all products it offers.

7.3. CDD for the existing customers

FIs, if at any time becomes aware of the fact that it lacks sufficient information or documentation relating to CDD requirements, or has a concern about the accuracy of the available information or documentation, they may obtain appropriate documentation and verify the customer's identity immediately.

8. Customer Identity Verification

8.1. Natural Person

Verify all data mentioned under item 7.1, above through obtaining and keeping a copy of the official documents signed and dated by the competent officer certifying them as true copy. Verify the permanent address through receiving, for instance the latest electricity or telephone invoice. For self-employed people, the bank should obtain a copy of their professional license, and obtain supporting documents for legal representatives of persons not competent, such as minors.

8.2. Legal Entity

Verify all data mentioned under item 7.2, above through obtaining and keeping a certified copy of their respective CR, memorandum of association, articles of association, ID of the owners and joint partners, shareholders who own more than 10% of the shareholding company capital, in addition to supporting documents of representatives authorized to access the account, such as official or banking power of attorney and their personal IDs.

8.3. Correspondent financial institutions

8.3.1. Prior to establishing any business relationship with correspondent banks / financial institutions, FIs must establish and verify the identity of correspondent banks / financial institutions. Identification measures would include due diligence on:

(a) ownership and management structure

(b) major business activities and customer base

(c) locations of the correspondent banks / financial institutions and its branches

(d) the intended purpose of establishing correspondent banking / relationships with the FIs.

- Verify that the correspondent bank / FI are subject to effective supervision by supervisory authority.
- Whether the FI has been subject or is subject to any investigation in relation to ML/FT transactions or any supervisory penalties in this regard.
- The FI should apply the following procedures before initiating any business relation with any correspondent financial institution:
    - A- Obtain the approval of the senior management before establishing the relationship.
    - B- Assess the correspondent bank's / FIs AML/CFT control and assess if they are adequate and effective.
    - C- Determine the respective AML / CFT responsibilities of the bank / FI and the correspondent bank / financial institution (s). Document the respective AML/CFT responsibilities of each institution.
    - D- FIs should have systems in place to guard against establishing any business relationship with business partners who may permit their accounts to be used by Shell Banks.
- In case the respondent FI is a subsidiary of another entity, the following additional procedures have to be applied and established by the FIs:
    - (i) entity's domicile and location
    - (ii) reputation of the entity
    - (iii) whether regulated and supervised at least for AML/CFT by regulatory or governmental authority or any body or agency equivalent to regulatory authority
    - (iv) whether the jurisdiction where it operates has effective AML/CFT regime

(v) the ownership, control and management structure

8.4. Shell Banks

A shell Bank must not be established or operated from the State of Qatar. FIs should not enter into, establish or continue any operations with Shell Banks. Further, FIs should also not have any correspondent banking relationship or respondent relationship with Shell Banks. FIs should satisfy that the respondent banks or any financial institution with which they have relationship in any foreign country do not permit their accounts to be used by Shell Banks.

8.5. Payable-through Accounts

8.5.1 Whenever a correspondent relationship involves maintenance of "payable-through accounts", the FIs should ensure that:

(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.

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.

8.5.2. When a correspondent FI asks for documents, data or information mentioned under 8.5.1 above and the respondent fails to comply with the request, the correspondent FI must terminate the customer's access to the accounts of the correspondent FI (s).

8.6. Power of Attorney

In case the power of attorney authorizes the holder of the power of attorney to exercise control over the assets of the guarantor, the following should be ensured by the FIs:

(i) Before becoming involved in or getting associated with any transaction involving the power of attorney, the FI must conduct CDD measures for the holder of the power of attorney and the grantor of the power of attorney

(ii) The FI should consider the holder and grantor of the power of attorney to be their customers.

8.7. Non Profit Organizations

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

(a) 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 bank, and any other information required by the competent authority (Ministry of Social Affairs).

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

(c) 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 herein.

9. Reduced Due Diligence (RDD)

9.1. The FIs must apply reduced CDD measures on the following customers:

A- Ministries, Government authorities, and semi-government companies in the GCC countries.

B- Financial institutions licensed within GCC countries.

C- Companies listed in the securities' markets across the GCC and those which apply disclosure standards equivalent to those required by the QFMA/DSM.

9.2. In the event where the amount of transaction(s) or related transaction(s) do not exceed (QR 75000), it may be sufficient to obtain the name and contact details of the customer.

9.3. FI wishing to apply RDD measures must keep evidence on the customer classification, in accordance with item 7 above.

9.4. RDD must not be applied on correspondent banks/ financial institutions specified in item 8.3 above.

9.5. RDD measures must not be applied in the event of any suspicion raised about the involvement of the customer or its representative in ML/TF transactions.

10. Enhanced Due Diligence (EDD) applied on high-risk customers:

FIs should apply and perform EDD measures on high-risk customers, business relationship or transactions of:

10.1 Non-resident customers

The following measures should be observed while applying the identification procedures:

A- Identify the purpose of the business relationship

B- Verify the validity of the entry visa initially while initiating business relationship.

C- Obtain a copy of the ID

D- 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

E- 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

10.2 Politically Exposed Persons (PEPs)

The FIs must have the following measures to establish and maintain business relationship with PEPs:

A. FIs are required to put in place appropriate risk management systems to determine whether a potential customer, a customer or beneficial owner is politically exposed person. This will in addition to the CDD measures listed above.

B. Obtain the approval of the senior management for establishing business relationship with a PEP.

C. Obtain information identifying PEPs through details submitted directly by them or through reference to publicly available information or through commercial database relating to PEPs.

D. While applying EDD on PEPs, FIs should take appropriate measures to establish the source of wealth and the sources of funds of the customer and the beneficial owners identified by PEPs.

E. In the event where any of the current customers becomes PEP, this person should be classified under this category and the approval of senior management should be obtained in terms of maintaining the business relationship with this person.

F. The bank should constantly and extensively monitor its relationship with these customers , provided that CDD measures applied on them include:-

1. The customer's file to include the following:-
    - Procedures taken to identify the wealth and source of funds

- Nature of future relationship to be used in ongoing monitoring.
- Evidence on the approval of the senior management to maintain the business relationship.
- Supporting documents on the customer's income, source of funds, job position, address and verification of such information by referring to reliable and neutral sources.

2. Ongoing monitoring by the compliance officer.

10.3. Bearer shares and share warrants to bearer

10.3.1. Where ever applicable to FIs, the bearer instruments would mean a bearer share or a share warrant to bearer. FIs should have adequate AML/CFT CDD policies, procedures, systems and controls for risks related to bearer instruments. FIs before being involved or associated with a transaction involving the conversion of a bearer instrument to registered form, or the surrender of coupons for a bearer instrument for payment of dividend, bonus or capital, the FI must apply enhanced CDD measures to the holder of the instrument and / or any beneficial owner.

10.4. Persons belonging to countries that do not apply the FATF recommendations appropriately:

10.4.1. 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.

10.4.2. 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.

10.4.3. The following jurisdictions, as examples, would require enhanced CDD measures:

(i) Jurisdiction with impaired international cooperation

(ii) Jurisdiction listed as non-cooperative by FATF

(iii) Jurisdiction subject to international sanctions, and

(iv) Jurisdiction with high propensity for corruption.

10.5. Due diligence through Third Party

In case a 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 given under Item 6 above (CDD) of this Instructions.

FIs should create a direct communication channel with the customer after seeking the documents, data and recommendations from the third party. However, compliance with the requirements and ultimate responsibility for customer identification and verification will remain with the FI relying on the third party.

10.6. Use of New Technologies

This includes electronic banking operations / operations undertaken by FIs electronically and prepaid cards. Sufficient policies and procedures should be applied to prevent their use in ML/TF. EDD measures should be applied, including authentication of documents submitted by the customer upon establishment of the business relationship.

Banks must refer to the Instructions on Modern Technology & E-Banking Risks, Circular No.106/2008 of 11/9/2008.

FIs are required to have policies, procedures, systems and controls to prevent any misuse of modern technologies or future technological developments for AML/CFT activities. Since use of new technologies for financial transactions are in practice at FIs, they should also have policies and procedures to address specific risks associated with non-face-to-face business relationships or transactions, where ever applicable to FIs. These policies and procedures should be applied while establishing customer relationships and also during on-going due diligence. FIs should also have in place specific and effective due diligence procedures that can be applied to non-face-to-face customers.

Additional controls are required in respect of non-face-to-face customers, like ensuring that customer's identity is established by additional documents, applying supplementary measures to verify the documents supplied, requiring eligible introducers to certify the identification documents etc.

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 ML/FT risks of such services.

10.7. Private Banking Services

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

A- Determine the purpose of the private banking service application.

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

11. Monitoring of Transactions

1- FIs should establish appropriate control systems that fit the size and nature of its business in order to disclose any large and unusual transactions or unusual patterns of transactions, provided that this includes the ceiling, type and size of the transaction executed beyond the expected behavior. Ceilings should be defined for both cash and non-cash transactions. An auditing system should be equally established in order to test the efficiency of the applied procedures.

2- Control systems should be able to identify the following:

   a. Transactions with unclear purpose or unjustified economic conditions.
   b. Significant or large transactions inconsistent with the normal behavior of the customer.
   c. Unusual patterns of activities.

3- The FI (according to its size) should observe the need to automatically monitor the transactions, as part of the monitoring systems to spot unusual transactions. Further, the information obtained from the originator remains with the transfer or the related message through the payment chain.

4- The FI should verify the unusual transactions spotted by the monitoring systems in addition to examining the background and purpose of those transactions.

5- The FI should observe the changing circumstances in the customer's activities, particularly the unusual and non-repetitive types of transactions.

6- The FI should take into consideration that the transaction risks are higher when the size, pattern or frequency of the transaction is not in conformity with the customer's activity.

12. Wire Transfers (for domestic and cross-border transfers)

This item should be applied on wire transfers exceeding QR 5000 or equivalent in foreign currencies, whether sent or received by the FIs. This item shall not be applied under the following: