وزارة التجارة والصناعة

Ministry of Commerce and Industry

Nº: 780/2020
Date: July 15, 2020

The Minister

Decision of the Minister of Commerce and Industry No. (48) of 2020 Promulgating the AML/CFT Compliance Rules for Auditors, Dealers in Precious Metals or Precious Stones, Trust and Company Service Providers.

The Minister of Commerce and Industry,

After perusal of the Law on Combatting Money Laundering and Terrorism Financing promulgated by Law No. (20) of 2019;

The Law on Combating Terrorism promulgated by Law No. (27) of 2019;

The Emiri Decree No. (12) of 2019 on the Organizational Structure of the Ministry of Commerce and Industry;

The Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing issued by the Council of Ministers' Decision No. (41) of 2019;

The Decision of the Minister of Commerce and Industry No. (95) of 2019 Establishing the Anti-Money Laundering and Terrorism Financing Section under The Companies Affairs Department;

The Adoption of the Draft Decision Promulgating these Rules by the Council of Ministers at its Ordinary Meeting No. (17) of 2020, held on April 22, 2020

Has decided the following:

Article (1)

The AML/CFT Compliance Rules for Auditors, Dealers in Precious Metals or Precious Stones, Trust and Company Service Providers, attached hereto, shall enter into force and effect.

Article (2)

All competent authorities, each within its own competence, shall implement this Decision, which shall come into force on the day following its publication in the Official Gazette.

Ali Ahmad Al Kuwari

Minister of Commerce and Industry

Issued on 24/11/1441 A.H

Corresponding to July 15, 2020 A.D

AML/CFT Compliance Rules for Auditors, Dealers in Precious Metals or Precious Stones, Trust and Company Service Providers

Chapter One

General Provisions

Section One

Definition and Scope of Implementation

Article (1)

In the application of these Rules, any instructions, circulars or guidance issued in implementation thereof, the following words and phrases shall have the meanings assigned thereto, unless otherwise required by the context:

The Law:	The Law on Combatting Money Laundering and Terrorism Financing promulgated by Law No. (20) of 2019.
The Implementing Regulations:	The Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing issued by the Council of Ministers' Decision No. (41) of 2019.
The Ministry:	The Ministry of Commerce and Industry (MOCI).
The Committee:	The National Anti-Money Laundering and Terrorism Financing Committee, stipulated in Article (29) of the Law.
The Unit:	The Financial Information Unit (FIU) established pursuant to Article (31) of the Law.
The Section:	The Anti-Money Laundering and Terrorism Financing Section under the Companies Affairs Department at the Ministry.
The Competent Authority:	Any public authority with specific AML/CFT responsibilities.
The Supervisory Authorities:	Competent authorities responsible for licensing or supervising financial institutions, Designated Non-Financial Businesses and Professions (DNFBPs) and Non-Profit Organizations (NPOs), or for ensuring compliance thereof with the AML/CFT requirements, as stipulated in the Implementing Regulations.

The Predicate Offence:	Any act constituting a misdemeanor or a felony under any Law in force in the State, whether committed inside or outside the State, whenever it generates Funds and constitutes an offence punishable by Law in both countries.
Instrumentalities:	Everything used or intended to be used, in whole or in part, in the commission of any Money Laundering or Terrorism Financing Offence.
Proceeds of Crime:	Any Funds derived or obtained, directly or indirectly, from committing predicate offences, including the income, interest, revenue or other product, whether or not it has been transferred in whole or in part into properties or investment proceeds.
Money Laundering (ML) Offence:	The offence stipulated in Article (2) of the Law.
Terrorism Financing (TF) Offence:	The offence stipulated in Article (3) of the Law.
Funds:	Assets or property of every kind, whether physical or non-physical, tangible or intangible or movable or immovable, including financial assets and economic resources such as oil and other natural resources, and all related rights, of any value, however acquired, and all legal documents or instruments in any form, including electronic or digital copies, evidencing title to, or share in, such assets and any interest, dividends or other income on or value accruing from or generated by such funds or other assets, which can potentially be used to obtain funds, goods or services.
Terrorism Offence:	Any offence provided for in the Law on Combatting Terrorism and any felony provided for in the Penal Code or in any other law, committed with the intent to execute or carry out a Terrorist Act or with a view to advocating or threatening any of the aforementioned.

Terrorist Act:

1. Any act intended to cause death or serious bodily injury to a 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.

2. Any act which constitutes an offence according to any of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), amended by Protocol (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

3. Any act which constitutes an offence under the provisions of other international conventions related to combating terrorism to which the State is a party.

Terrorist:

Any natural person who intentionally commits any of the following acts:

1. Commits or attempts to commit, terrorist acts, by any means whatsoever, directly or indirectly, unlawfully and willfully;
2. Participates as an accomplice in terrorist acts;
3. Organizes or directs others to commit terrorist acts; or
4. Contributes to the commission of terrorist acts by a group of persons acting with a common purpose 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 Entity: Any group of terrorists that commits intentionally any of the following acts:

1. Commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully;
2. Participates as an accomplice in terrorist acts;
3. Organizes or directs others to commit terrorist acts; or
4. Contributes to the commission of terrorist acts by a group of persons acting with a common purpose and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Freeze: Prohibiting the transfer, conversion, disposition, movement, or transport of Funds or equipment or other Instrumentalities, on the basis of, and for the duration of the validity of, a decision of a competent authority, or until an unfreezing order is issued or the Competent Court issues a confiscation order.

In addition to prohibiting the transfer, conversion, disposition, movement, or transport of Funds, within the scope of implementation of Targeted Financial Sanctions, for designated persons or entities on the sanctions list for the duration of the validity of the designation order.

Targeted Financial Sanctions: Asset freezing and prohibitions to prevent Funds or other assets from being made available, directly or indirectly, for the benefit of persons and entities listed in accordance with the Law on Combating Terrorism.

Regulated Entity:

1- Auditors**,** Dealers in Precious Metals or Precious Stones, Trust and Company Service Providers stipulated in Article (1) of the Law, when conducting any of the following activities:

a) Auditors whether sole practitioners, partners or employed professionals within professional firms when they arrange, execute or conduct transactions on behalf of or for their customers in relation to any of the following activities:

- Purchase or sale of real estate.
- Management of the customer's funds, securities or other assets.
- Management of bank accounts, savings accounts or securities accounts.

- Organizing contributions for the establishment, operation or management of companies or other entities.
- Establishment, operation or management of legal persons or legal arrangements, and sale or purchase of business entities.

b) Dealers in Precious Metals or Precious Stones when they participate in cash transactions of a value equal to or exceeding fifty thousand Riyals (QR 50.000).

c) Trust and Company Service Providers (TCSPs) when arranging for or executing transactions for the customers relating the following activities:

- Acting as a formation agent of legal persons.
- Acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
- Providing a registered office, business address or, correspondence or administrative address for a company, a partnership or any other legal person or arrangement.
- Acting as or arranging for another person to act as a trustee of an express trust or performing an equivalent function for another form of legal arrangement.
- Acting as or arranging for another person to act as a nominee shareholder for another person.

2- Any other activity or profession, subject to the supervision of the Ministry, and set forth by virtue of a decision issued by the Council of Ministers upon the proposal of the Committee, in conformity with the provisions of the Law

Customer: Any natural or legal person or legal arrangement, according to the definitions stipulated in the Law, who engages or seeks to engage with the regulated entity in any transaction, on the person's own behalf or as agent for or on behalf of, another person, whether for his own benefit or for the benefit of others.

Occasional Customer: A Customer who does not have a regular relationship with the regulated entity.

Applicant for Business:	Any natural or legal person or legal arrangement seeking the establishment of a business relationship or a one-off transaction with the regulated entity.
Business Relationship:	A regular relationship between a customer and a regulated entity in connection with the services that the customer receives, and a relationship that, when contact is established, is reasonably expected to last for an extended period and to include several transactions.
A One-Off Transaction:	Is a transaction carried out by the regulated entity for the customer otherwise than in the course of a business relationship with the customer.
Customer Due Diligence (CDD):	A series of measures undertaken by the regulated entity, which includes identifying the customer, verifying the customer's identity using original documents, data or information from a reliable and independent source, establishing whether the customer is acting on behalf of another person, verifying that any person purporting to act on behalf of the customer is authorised to act on behalf of the customer and identifying and verifying the identity of that person, understanding the nature of the customer's business or activity pattern, as well as the nature and purpose of the business relationship and identifying the legal form of the Customer, whether the customer is a natural or legal person or legal arrangement.
Financial Institution:	Any person who conducts, as a business, one or more of the financial activities or operations for or on behalf of a customer, as set forth in Article (2) of the Implementing Regulations.
Financial Group:	A group consisting of a parent company or of any other type of legal persons exercising control, and coordinating functions over the rest of the group, for the application of the group supervision, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.
Parent Entity:	A company exercising control and supervision functions over an associate in the following cases: 1. If it owns the majority of the capital of the associate. 2. If it holds a majority of the voting power whether alone or together with other associates through agreements.

Non-Profit Organization (NPO):	Any legal entity or person, legal arrangement or organization, which collects or disburses funds for charitable, religious, cultural, educational, social or fraternal purposes; or for the carrying-out of other types of charitable works for the public benefit.
Express Trust:	A legal relationship that does not establish a legal personality, created by a written deed, whereby a person places funds under the control of a trustee for the benefit of one or more beneficiaries or for a defined purpose.
Beneficiary of a Trust:	A natural or legal person or legal arrangement that benefits of a trust and can ultimately be verified whether immediately or in the future after the expiry of a specific period.
Beneficial Owner:	The natural person(s) who ultimately and effectively owns or controls a customer, through ownership interest or voting rights, or the natural person on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate, or by any other form of representation. It also includes any person who exercises ultimate effective control over a legal person or arrangement, including any person exercising ultimate effective control by any means.
Politically Exposed Persons (PEPs):	Individuals who are or have been entrusted by the State or by a foreign State with prominent public functions, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned companies, members of Parliaments, and important political party officials, and members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organizations. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Family Members of a Politically Exposed Person:	shall include a wife or a husband and any natural person relative by blood or marriage up to the second degree, who are the following: 1- Father/ Mother 2- Father-in-Law/ Mother-in-Law 3- Son/Daughter 4- Stepson/Stepdaughter 5- Grandfather/Grandmother 6- Brother/Sister 7- Brother-in-Law/ Sister-in-Law 8- Grandson/Granddaughter
Close Associates of a Politically Exposed Person:	Shall include any natural person who is a partner in a legal person or legal arrangement, or a beneficial owner of a legal person or arrangement owned or effectively controlled by a Politically Exposed Person, or any person associated with the Politically Exposed Person through a close business or social relationship.
International Organizations:	Entities established under official political arrangements between the member states, which are international treaties legally recognized by the member states, and which are not dealt with as institutional units resident in the States in which they are located.
Risk-Based Approach (RBA):	A series of measures and procedures aiming at identifying, assessing, understanding and mitigating the money laundering and terrorism financing risks.
National Risk Assessment (NRA):	The assessment issued by the Committee, which is responsible for documenting, updating and circulating the results to the competent authorities and supervisory authorities.
Suspicion Report:	The report that the compliance officer at the regulated entity must immediately make to the Unit, upon suspicion or when having reasonable grounds to suspect that a transaction or operation or an attempt to conduct a transaction or operation, irrespective of its value, is linked to or involves proceeds of a predicate offence or relates to terrorism financing.
Suspicious Transaction Report:	The internal report that the employee or officer makes to the compliance officer at the regulated entity, upon suspicion or when having reasonable grounds to suspect that a money laundering offence or terrorism financing offence has been committed.

Compliance Officer: An employee of the regulated entity, who is responsible for managing its compliance with the AML/CFT requirements stipulated in the Law, the Implementing Regulations and these Rules, and who, in particular, prepares and submits Suspicion Reports to the Unit.

Employee: Includes any of the following:

1. A person who is employed or appointed by the regulated entity under a contract of service.
2. A person who is assigned by the regulated entity to perform a service.
3. A person who performs the service under an arrangement between the regulated entity and a third party.

Governing Body: Board of directors or any equivalent governing body at the regulated entity, whatever it is called.

Senior Management: Any natural person or governing body in the Regulated Entity, eligible to make decisions pertaining to the operation and supervision of the regulated entity.

Ongoing Monitoring: Ongoing Monitoring and review applied by the regulated entity to:

1- Transactions conducted under the business relationship with the customer to ensure that the transactions are consistent with the information collected about the customer, the customer's business and risk profile, and, where necessary, the source of the customer's funds and wealth .

2- The existing records of the customer, especially high-risk customers to ensure that documents, data or information obtained through conducting Customer Due Diligence (CDD) are kept up-to-date and relevant.

Outsourcing: Any form of arrangement that involves the regulated entity relying on a third-party service provider for the exercise of a function, or the conduct of a specific activity, that would otherwise be exercised or conducted by the regulated entity. The third-party may include a member of its financial group. Outsourcing does not include:

1- Discrete advisory services, including for example, the provision of legal advice, specialised training, billing, and physical security;

2- Supply arrangements and functions, including, for example, the supply of electricity or water and the provision of cleaning services and catering;
3- The purchase of standardised services, including, for example, market information services and the provision of prices.

Jurisdiction: Any kind of legal jurisdiction, including the following in particular:

1. The State of Qatar referred to by "the State"
2. Any foreign country
3. The Qatar Financial Centre or any similar Jurisdiction

The Financial Action Task Force (FATF): The international body that includes a number of member countries and that sets standards and develops and promotes policies to combat money laundering, terrorism financing and financing of proliferation of weapons of mass destruction, in addition to monitoring the extent of compliance with these policies by countries.

Article (2)

In the implementation of these Rules, if the regulated entity is a natural person exercising his activity in the form of an individual establishment or office, he shall personally undertake the senior management and the compliance officer responsibilities at the establishment or office; and he may appoint one of his employees as a compliance officer.

Section Two

Key AML/CFT Principles

Article (3)

The senior management of the regulated entity must ensure that the entity's policies, procedures, systems and controls, hereinafter referred to as "applicable policies", appropriately and adequately address the requirements of the Law, its Implementing Regulations and these Rules.

Article (4)

The regulated entity must develop and apply a risk-based approach to comply with the requirements of the Law, its Implementing Regulations and these Rules, that is designed to

identify, understand and assess its money laundering and terrorism financing risks in conformity with the size and nature of its business.

Article (5)

The regulated entity must know each of its customers to the extent appropriate for the customer's risk profile.

Article (6)

The regulated entity must have effective measures in place to ensure internal and external reporting whenever money laundering or terrorism financing is known or suspected.

Article (7)

The regulated entity must make and keep records, documents and data, providing documentary evidence of its compliance with the requirements of the Law, its Implementing Regulations and these Rules, and must make them available and submit them without delay to the competent authorities upon request.

Chapter Two

AML / CFT Responsibilities

Section One

Responsibilities of Regulated Entities

Article (8)

The regulated entity must develop a programme against money laundering and terrorism financing, having regard to its ML/TF risks; and the nature, size and complexity of its business.

The programme must include, in particular, the following:

1- Developing, implementing and maintaining adequate internal procedures, systems and controls to prevent money laundering and terrorism financing
2- Appropriate compliance management arrangements, including the appointment of a compliance officer
3- Adequate screening and audit procedures to ensure high standards when employing or appointing officers or employees.
4- Developing and implementing an appropriate ongoing training programme for officers and employees.

5- An independent audit unit for ongoing and adequate assessment, review and testing, to verify the extent of compliance with policies.

Testing includes, in particular, the regulated entity's AML/CFT programme, screening procedures of employees, record making and keeping and ongoing monitoring of customers.

The regulated entity must ensure that the review and testing stipulated in item (5) above must be conducted at least once every two (2) years by the internal audit unit or by the compliance officer from any other branch of the entity. The review and testing may be also conducted by an external auditor or a person with the required professional competence, qualifications and skills, as well as integrity and independence.

The regulated entity must take the necessary measures to conduct the review and testing set out in item (5) of this Article and must provide the Section with a copy of the records by 31 July 2021 and every 2 years thereafter.

Article (9)

The regulated entity's applicable policies must cover, in particular, the following:

1. Customer Due Diligence measures and ongoing monitoring;
2. Record making and keeping;
3. The detection of suspicious transactions;
4. The Internal and external reporting obligations;
5. The communication of the applicable policies to the regulated entity's officers and employees.

Article (10)

The regulated entity's applicable policies must, in particular:

1- Identify indicators that enable scrutiny of the background and purpose of complex or unusual transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose;
2- Require to apply enhanced CDD measures when ML and TF risks are high;
3- Ensure that there are appropriate systems for risk management and mitigation, particularly when establishing business relationships with PEPs, or in relation to customers whose transactions or operations are carried out in more than one jurisdiction;
4- Require, before any function or activity is outsourced, an assessment to be made and documented of the ML/TF risks associated with outsourcing, , and to be monitored on an ongoing basis;

5- Ensure that officers and employees of the regulated entity are aware of and comply with the requirements of the Law, its Implementing Regulations and these Rules when making suspicious transaction reports; and with the obligation of preventing tipping off customers and the consequences of violating this requirement;
6- Ensure that there are appropriate systems to protect the confidentiality of information related to suspicious transaction reports and suspicion reports;
7- Enable applying simplified CDD measures, including completing verification of the identity of the customer and beneficial owner after the business relationship has been established, where ML/TF risks are low;
8- Ensure that there are appropriate systems and preventive measures to implement targeted financial sanctions under the Law and the Law on Combating Terrorism.

Article (11)

The regulated entity must carry out regular assessments and reviews, at least once every year, of the adequacy of the applicable policies in preventing its ML and TF risks and to ensure its appropriateness in achieving the AML/CFT requirements.

Article (12)

The regulated entity must ensure that its officers and employees, wherever they are, comply with the requirements of the Law, its Implementing Regulations, these Rules and its applicable policies, and must particularly:

1- Require officers and employees to submit suspicious transaction reports to the compliance officer on transactions conducted in, from or to the State.
2- Enable timely, unrestricted access to the senior management, the compliance officer, the Unit and the Section, to documents, data and information that relate, directly or indirectly, to transactions conducted in, from or to the State, wherever they are held, particularly those relating to identifying customers; their sources, and those obtained after conducting CDD and ongoing monitoring or those used for this purpose, as well as all records of such transactions.

In cases where the regulated entity has branches or associates abroad, it must immediately inform the Section in any written form, if a Law of a foreign country prevents the provisions of the previous paragraph from applying.

Article (13)

The regulated entity must apply the AML/CFT programme to all its branches and majority-owned associates in the State or abroad and must include in this programme, in addition to the procedures stipulated in Article (8) of these Rules, the following:

1- Applying policies and procedures related to exchanging information required for the purposes of CDD and ML/ TF risk management.
2- Providing necessary information, at the financial group level, to the compliance officers, audit and AML/CFT officers, concerning customers, accounts and transactions from branches and associates, where necessary for AML/CFT purposes, including information and analysis of unusual or suspicious transactions and activities, suspicion reports and basic information or whatever is useful to submit a suspicious transaction report.
3- Providing the information set out in the previous item to branches and associates, when relevant and appropriate to risk management.
4- Implementing sufficient safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

Article (14)

The regulated entity must ensure that its external branches and majority-owned associates apply AML/CFT measures that are consistent with requirements applied in the State, when the maximum AML/CFT requirements of the host country are less strict than those applied in the State, to the extent that host country laws and regulations permit.

If the host country does not permit the adequate implementation of AML/CFT measures consistent with the State procedures, the regulated entity should apply additional appropriate procedures to manage the ML/TF risks, to external branches and majority-owned associates. The additional procedures particularly include requesting additional information and reports and the regulated entity must immediately inform the Section of the matter in any written form.

If the Section deems that the additional procedures applied by the regulated entity are not sufficient, it must take other supervisory procedures, including imposing additional controls on the regulated entity and, where necessary, requesting suspension of its operations carried out through the branch or associate in the host country.

Section Two

Senior Management Responsibilities

Article (15)

The senior management of a regulated entity must ensure, in particular, that:

1. The regulated entity develops, documents and implements effective AML/CFT policies in accordance with the Law, its Implementing Regulations and these Rules.
2. The regulated entity develops adequate screening procedures to ensure compliance with high standards when appointing or employing officers or employees.

3. The regulated entity designs and implements an ongoing AML/CFT training programme for its officers and employees.
4. Independent review and testing are conducted to ensure compliance with the applicable policies at the regulated entity, including an assessment and review of the policies pursuant to the provisions stipulated in Article (8) of these Rules.
5. Regular and timely information is made available about the management of the regulated entity's ML/TF risks.
6. The regulated entity's ML/TF risk management policies and methodology are appropriately established and documented, including their implementation by the regulated entity.
7. Instructions, circulars or guidance issued by the Ministry and any relevant procedures are taken into account.
8. A compliance officer is appointed and entrusted with the necessary powers and authority, to perform his role in an effective, objective and independent manner.
9. An AML/CFT compliance culture is promoted within the regulated entity.
10. Necessary measures are taken to ensure that ML/TF risks are taken into account in the day-to-day operations of the regulated entity, including, in particular, in relation to the development of new products, the taking on of new customers, or changes in the business profile of the regulated entity.
11. Reasonable measures have been taken to ensure that the reports required to be submitted to the Section are accurate, complete and submitted promptly.

Article (16)

The senior management must, on a regular basis and in a timely manner, take reasonable measures to address deficiencies identified by the compliance officer, in the reports it receives periodically or upon its request, including the adoption of an action plan to remedy the deficiencies, to enable it to discharge its responsibilities in accordance with the AML/CFT requirements of the Law, its Implementing Regulations and these Rules.

Section Three

Compliance Officer and Deputy Compliance Officer

Article (17)

The regulated entity must ensure that it has permanently a Compliance Officer and a Deputy Compliance Officer, whether as part of its governing body or employees.

Article (18)

The compliance officer and deputy compliance officer must:

1- Have sufficient seniority, the necessary knowledge and expertise to perform their functions and act independently, including preparing reports.
2- Be aware of legal and supervisory responsibilities related to their functions in accordance with the Law, its Implementing Regulations and these Rules.
3- Be able to develop appropriate precautionary arrangements in case of their absence.
4- Be resident in the State.

Article (19)

In general, the compliance officer at the regulated entity is responsible, as a minimum, for:

1- Contributing to the development of the regulated entity's policies, overseeing their implementation, assessing their effectiveness and regularly reviewing them.
2- Monitoring the implementation of the national and sectoral AML/CFT strategies.
3- Supporting the senior management and coordinating the ML/TF risk management issues at all the departments of the regulated entity.
4- Contributing to the development of measures that enable to address deficiencies in the AML/CFT area at the regulated entity, in light of the results of national and international studies and researches relating to the AML/CFT issues.
5- Promoting a regulated entity-wide view to be taken of the need for AML/CFT monitoring and accountability.

Article (20)

The compliance officer at the regulated entity is particularly responsible for:

1- Receiving, investigating and assessing internal suspicious transaction reports.
2- Making suspicion reports and submitting them to the Unit.
3- Notifying the Section of the submission of suspicion reports to the Unit, which may benefit the Section for supervisory and statistical purposes. Notification must not include any information or details about the content of the reports.
4- Acting as central point of contact between the regulated entity, the Unit, the Section and other competent authorities in the State, in relation to AML and CFT issues.
5- Responding immediately to any request for information by the Unit.
6- Responding to any request for information by the Section, necessary to enable it to perform its functions.
7- Keeping the deputy compliance officer informed of any significant AML/CFT developments, whether internal or external.
8- Informing the regulated entity's senior management of any instructions, circulars or guidance issued by the Ministry in the AML/CFT area.

Article (21)

The deputy compliance officer temporarily acts as the compliance officer during absences of the compliance officer and whenever there is a vacancy in his position. When the deputy compliance officer acts as compliance officer, all rules apply in relation to the deputy compliance officer as if he were the compliance officer.

Article (22)

The compliance officer for a regulated entity must act honestly, independently and must be diligent to the extent possible, particularly in the following cases:

1- Upon receiving, investigating and assessing internal suspicious transaction reports.
2- Upon deciding whether to make, and preparing a suspicion report to the Unit

Article (23)

The compliance officer provides the senior management with an annual report on AML/CFT issues, within four months from the end date of each financial or fiscal year of the regulated entity, to enable the senior management to carry out the AML/CFT requirements in accordance with the Law, its Implementing Regulations and these Rules. The annual report must include, as a minimum, the following:

1- The assessment of the adequacy and effectiveness of the regulated entity's applicable policies in preventing money laundering and terrorism financing;
2- The number and types of internal suspicious transaction reports made to the compliance officer;
3- The number of suspicion reports submitted by the compliance officer to the Unit;
4- The reasons why suspicion reports have or have not been prepared or submitted to the Unit in relation to transactions on which the compliance officer received a suspicious transaction reports;
5- The number and types of breaches by the regulated entity of the provisions of the Law, its Implementing Regulations and these Rules, or the regulated entity's applicable policies;
6- Areas where the regulated entity's applicable policies and programmes should be improved, and adequate proposals for avoiding deficiencies in the AML/CFT areas;
7- A summary of the AML/CFT training delivered to the regulated entity's officers and employees, and proposals for making appropriate improvements to the training programmes.

8- A statement of customers of the regulated entity who are categorised as high risk, taking into account the findings of the National Risk Assessment and the business risk assessment stipulated in Article (24) of these Rules;
9- Progress in implementing any AML/CFT action plans;
10- The outcome of any relevant quality assurance or audit reviews in relation to the regulated entity's applicable policies.

Chapter Three

Risk-Based Approach

Section One

General Provisions

Article (24)

A regulated entity must identify, assess and understand the money laundering and terrorism financing risks that it faces (a *business risk assessment*), taking into account the risks identified in the National Risk Assessment and those that may arise from:

1- Risk factors associated with the types of customers that it has and proposes to have, the beneficial owners of the customers and beneficial owners of the transactions carried out by Customers (Customer risk).
2- Risk factors associated with products, services and transactions that it provides and proposes to provide (Product risk).
3- Risk factors associated with technologies that it uses and proposes to use to provide those products, services and transactions (Interface risk).
4- Risk factors associated with jurisdictions with which its customers are or may become associated like the jurisdiction where the customer lives or is incorporated, or where the customer conducts business or has assets (Jurisdiction risk).
5- Risk factors associated with the purpose of establishing business relationships.
6- Risk factors associated with the size of transactions and operations.
7- Risk factors associated with the duration of the relationship with the customer and the frequency of operations.

The regulated entity must identify necessary steps for management and mitigation of such risks.

Article (25)

The regulated entity must document the following:

1- The basis and sources, on which it relied to identify, assess and understand its ML/TF risks, taking into account the National Risk Assessment and any other sources to identify such risks, particularly the sectoral risk assessment conducted by the supervisory authority.
2- The timing of conducting the business risk assessment and the frequency of its updates.
3- The timing of making the report on the business risk assessment available to the Section within the timeframe it specifies.
4- The risk level mitigation procedures taken after the assessment of business risk and their results in terms of mitigation of the risks or failure to mitigate such risks.

In case the regulated entity does not assess any of the risks that it faces or does not demonstrate the basis and sources on which it relied in the assessment, it must explain the reasons for non-compliance with such requirements, if requested by the Section.

Article (26)

The regulated entity must adopt an adequate methodology that addresses its risks, upon implementation of its approach to ML/TF risk mitigation (a threat assessment methodology).

The threat assessment methodology includes, in particular, the following:

1- Identifying the purpose and intended nature of the business relationship with each customer;
2- Assessing the risk profile of the business relationship by scoring the relationship based on:
   a- The types of customers it has or proposes to have and the extent to which the methodology is suitable for the size, nature and complexity of the regulated entity's business.
   b- The Types of new products, services or professional practices, or new delivery channels or means through which it provides or proposes to provide such products, services or professional practices.
   c- The types of jurisdictions with which its customers or third parties are or may become associated.

The regulated entity must demonstrate the appropriateness of its adopted practices with the threat assessment methodology.

The methodology must also be designed to enable the regulated entity to identify and recognize any changes in its ML/TF risks.

The regulated entity must change its methodology, where necessary.

Article (27)

In developing the risk profile of a business relationship with a customer, the regulated entity must identify the risks stipulated in Article (24) of these Rules and any other risks that are relevant to the business relationship, especially in relation to the size, complexity and nature of its business and of its customer's business, which combine to produce the risk profile of the business relationship.

The regulated entity must also take into account the outcome of this risk profile of the business relationship stipulated in the previous paragraph, in deciding the intensity of the CDD and ongoing monitoring to be conducted for the customer.

Section Two

Customer Risks

Article (28)

The regulated entity must identify, assess and document the risks of money laundering and terrorism financing posed by the different types of customers and the different size of their transactions and different activities and it must take adequate measures for management and mitigation of such risks.

The intensity of the CDD and ongoing monitoring conducted for a particular customer must be proportionate to the perceived or potential level of risk posed by the relationship with that customer, especially its duration, and type and frequency of current transactions with that customer.

Article (29)

The regulated entity must, from the outset of its dealings with an applicant for business and on an ongoing basis throughout the entire period of the business relationship, verify whether the applicant for business or the customer is a designated person or entity on the sanctions list stipulated in the Law on Combating Terrorism or is listed by the UN Security Council or the Sanctions Committee. If the person or entity is listed, the regulated entity must:

1- Refrain from establishing or continuing a business relationship with that person or entity;
2- Immediately submit a suspicion report to the Unit.
3- Immediately inform the Section of the matter in any written form.
4- Immediately notify the National Counter Terrorism Committee (NCTC) of the matter in any written form.

Article (30)

If the regulated entity knows or suspects, at any time, that the applicant for business or the customer is associated with or involved in terrorism, money laundering or terrorism financing offences, or is associated or involved with a terrorist or terrorist entity, or is subject to sanctions or measures imposed by regional or international organizations or foreign countries, the regulated entity must:

1- Refrain from establishing or continuing a business relationship with that applicant or customer, unless it obtains approval from the senior management.
2- Apply enhanced CDD measures.
3- Immediately submit a suspicion report to the Unit.
4- Immediately inform the Section of the matter in any written form without disclosing any information or details about the suspicion report.

Article (31)

The regulated entity must establish an appropriate risk management system to determine whether the applicant for business, the customer or the beneficial owner of the applicant for business and the customer is a PEP or a family member or close associate of a PEP. The system must particularly include requesting necessary information from customers, referring to publicly available information and the possibility of having access to databases within the limits specified by the legislation in force.

If the applicant for business, customer or beneficial owner is identified as a PEP or a family member or close associate of a PEP, the regulated entity must adopt the following additional CDD measures:

1- Obtaining senior management approval before establishing or continuing the business relationship for existing customers.
2- Taking reasonable measures to establish the sources of wealth and funds of the customer and beneficial owner of the customer.
3- Applying enhanced ongoing monitoring to the business relationship related to the customer or beneficial owner of the customer.

Article (32)

In assessing the risks posed by the customers, the regulated entity must take into account all legal forms such as legal persons or legal arrangements and legal or agreement means that pose any reduction in transparency and concealment of the identity of the applicant or customer such as a powers of attorney and acting shareholders.

If the power of attorney authorises the holder to exercise control over assets of the grantor, the holder and the grantor are both considered to be customers of the regulated entity and must be subject to CDD measures by the regulated entity before engaging in a transaction involving this power of attorney.

Section Three

Product and Service Risks

Article (33)

The regulated entity must identify, assess and document ML and TF risks that may arise from the development of new products, services or business practices before their launch or use.

The regulated entity must adopt appropriate measures to manage and mitigate such risks.

The level of applied CDD and ongoing monitoring measures for each type of product, service and practice must be proportionate to their perceived or potential level of risk.

Section Four

Interface Risks

Article (34)

The regulated entity must identify, assess and document ML and TF risks that may arise from the development of delivery channels or new means to provide services, products or operations, or that may arise from the use of new or developing technologies for new or pre-existing products, before the launch or use of such technologies.

The regulated entity must adopt appropriate measures to manage and mitigate such risks.

The level of applied CDD and ongoing monitoring measures for each type of delivery channel or new means for providing services, products or operations must be proportionate to the perceived or potential relevant level of risk.

Article (35)

In terms of interface risks, the regulated entity must adopt appropriate measures, particularly the following:

1- Preventing the misuse of advanced technologies in money laundering and terrorism financing regimes; and
2- Managing any specific risks associated with non-face-to-face business relationships or transactions.

Article (36)

The management of risks related to non-face-to-face business relationships or transactions particularly includes the following:

1- Requiring additional identification documentation for non-face-to-face customers.

2- Establishing independent and secure contact with non-face-to-face customers.
3- Requiring first payments by or for non-face-to-face customers to be made through accounts in the customers' names with financial institutions subject to similar CDD measures.

Article (37)

Non-face-to-face business relationships or transactions include, in particular, the following:

1- Business relationships concluded over the Internet or through the post.
2- Services and transactions provided or conducted over the Internet, using ATMs, telephone or fax.
3- Electronic point of sale transactions using prepaid, reloadable or account-linked value cards.

Article (38)

The regulated entity may identify and verify the identity of the customer through electronic verification of the identification documentation from a reliable and independent source and, must in this case establish and maintain a register that clearly shows the basis of the electronic verification.

Article (39)

The regulated entity may rely on third parties to implement CDD measures for permanent or occasional customers, including identifying the customer and beneficial owner and understanding the nature of their business. The ultimate responsibility for implementing such measures and applying ongoing monitoring remains with the regulated entity.

When relying on a third party financial institution or DNFBP, the regulated entity must conduct CDD measures and must before establishing the business relationship:

1- Immediately obtain necessary information from the third party concerning the CDD measures, including customer identification.
2- Ensure that the third party will provide, without delay, copies of the customer identification documentation and other documents related to such measures upon request, which the regulated entity would obtain if it had conducted the CDD measures itself.
3- Verify that the third party is subject to regulation or supervision and complying with CDD measures and record-keeping, in accordance with the Law, the Implementing Regulations and these Rules.

4- Take into account information available on the ML and TF risk level in countries where the third party is located, especially information issued by international and regional organizations and foreign countries.
5- Verify that the third party provides it with all information about the customer, which is obtained from the CDD measures conducted, and that the regulated entity would obtain if it had conducted the CDD measures itself.

Article (40)

The provisions of the previous Article shall apply when the regulated entity relies on a third party that is part of the same financial group.

The requirements referred to in the previous Article shall be deemed achieved in the following cases:

1- When the financial group applies CDD and record-keeping measures and AML/CFT programmes in accordance with the Law, the Implementing Regulations and these Rules.
2- When supervision is carried out by the competent authorities in the State or host country to verify the implementation of such measures and programmes by the financial group.
3- When high risks related to countries are sufficiently mitigated through the financial group's AML/CFT policies.

Article (41)

The regulated entity shall not be obligated to obtain any of the original documents obtained by the third party in applying CDD measures according to the two previous Articles.

Article (42)

If the regulated entity outsources its functions or activities to an external third party, it must ensure compliance by the third party with the following through a Service Agreement:

1- Requiring officers and employees, wherever they are, to comply with the Law, the Implementing Regulations, these Rules and the regulated entity's applicable policies.
2- Requiring officers and employees to submit suspicious transaction reports to the entity's compliance officer concerning transactions carried out in or through the State, or transactions sent to the State and in which the regulated entity or the third party, acting on its behalf, is a party.
3- Providing timely, unrestricted access by the senior management, the compliance officer, the Unit and the Section, to documents, data and information relating directly or indirectly to transactions conducted by the regulated entity or the third party,

acting on its behalf, and carried out in, through or to the State, wherever they are held, particularly those relating to the customer identification, their sources and those obtained while conducting CDD and ongoing monitoring or used for this purpose, as well as all records of transactions.

In cases where the regulated entity has foreign branches or associates, the third party must immediately notify the entity to notify the Section any written form, in the event where the law in a foreign country prevents the application of the provisions of the previous paragraph.

Section Five

Jurisdiction Risks

Article (43)

The regulated entity must identify, assess and document ML and TF risks posed by the different types of jurisdictions with which customers and third parties are, or may become, associated.

The regulated entity must adopt appropriate measures to manage and mitigate such risks.

The intensity of the CDD measures and ongoing monitoring conducted by the regulated entity must be proportionate to the perceived or potential level of risk posed by the jurisdiction.

In terms of jurisdiction risk, the regulated entity must, particularly, apply the following:

1- Enhanced CDD measures commensurate with the level of risk posed by the business relationships and operations with customers or third parties from countries against which FATF calls for such action, and that are published by the Committee on its website.
2- Any other measures, including countermeasures proportionate to the level of risk, which are specified in the circulars issued by the Section, based on FATF's data, or measures decided by the Committee independently.
3- Any other measures that are proportionate to the level of risk related to business relationships and operations with customers or third parties from countries subject to international sanctions, or countries that have ineffective AML/CFT regime or deficiencies in the area of international cooperation, or that are more vulnerable to corruption, while taking into account publications issued by international and regional organizations and foreign countries.
4- Applying any other measures to mitigate additional risks posed by PEPs associated with jurisdictions that are more vulnerable to corruption.

Chapter Four

Know Your Customer and Relevant Measures

Section One

General Provisions

Article (44)

The regulated entity must know its permanent and occasional customers, and must have the necessary documents, data and information to validate their identity (customer identification documentation), from a reliable and independent source.

The regulated entity must not establish a business relationship with a customer unless:

1- The permanent or occasional customer has been identified, whether in case of a natural or legal person or legal arrangement.
2- The beneficial owner has been identified and reasonable measures have been taken to verify his identity to satisfy itself that it knows the beneficial owner.
3- The purpose and intended nature of the business relationship or transaction have been adequately clarified.
4- Any person acting on behalf of the customer has been identified and his identity has been verified, validating that person according to rules applied in this regard.
5- The nature of the activity of the customer has been identified, for legal persons and arrangements, as well as the ownership and control structure and the beneficial owner.

Once the relationship has been established, the regulated entity must assess the transactions conducted with the customer at regular intervals against the expected pattern of activity of the customer. Any unexpected activity can then be detected to determine whether there is a suspicion of money laundering or terrorism financing.

If the regulated entity did not obtain evidence of identity for the customer, or the person acting on behalf of the customer or the beneficial owner, or clearly notices fictitious or insufficient data related to their identities, it must not establish or continue the business relationship or carry out a transaction and must, where necessary, consider making a suspicion report to the Unit.

The regulated entity must also not maintain unknown accounts or accounts with fictitious names.

Article (45)

The regulated entity shall rely on the customer identification documentation in developing the risk profile of the customer, and determining the intensity of the CDD measures and ongoing monitoring that it must conduct for the customer.

The regulated entity must make and keep a comprehensive record of all the customer identification documentation, including CDD and ongoing monitoring measures applied to obtain such documentation, irrespective of the nature and risk profile of the customer.

The regulated entity must take into account that the risks of money laundering and the financing of terrorism associated with the customer's economic activity may arise from the fact that either:

1- the funds that are going to be put through a business relationship derive from a criminal activity and the business relationship will be used to channel these funds; or
2- the proceeds of the predicate offence will be mixed with the proceeds of legitimate economic activity to disguise their origin.

The regulated entity must manage and mitigate these risks, by adopting reasonable measures to identify the sources of the customer's wealth and funds and identify the nature and intended purpose of the business relationship.

Article (46)

When conducting CDD measures for an applicant for business or a customer, the regulated entity must obtain and document information on the sources of wealth and funds, having regard to the risk profile of the applicant for business or the customer.

If it appears to the entity that money laundering and terrorism financing risks are high, it must obtain and document information on the sources of funds or wealth.

The information stipulated in this Article forms part of the regulated entity's customer identification documentation.

Article (47)

The regulated entity must obtain information about the purpose and intended nature of the business relationship, which would enable it to identify differences between the transactions conducted and the usual pattern of the customer's activity and to ensure that money laundering or terrorism financing has not taken place.

The regulated entity must document information stipulated in the previous paragraph, which shall form part of the customer identification documentation.

Article (48)

The regulated entity must identify the applicant for business or the customer in case of a natural person by collecting the following information as a minimum:

1- The person's full name, as written in official documentation by sighting:
(a) An official government-issued document that has the person's name and a photograph; such as a valid Qatari ID card, a valid passport or a valid driving licence with a photograph.
(b) A document from a reliable, independent source that bears the person's name and a photograph.
2- The address of residence or the local address.
3- The date and place of birth and the nationality, or nationalities if he holds more than one.

Article (49)

The regulated entity must identify the applicant for business or customer in case of a legal person by collecting the following information as a minimum:

1- The name and legal form of the person.
2- The certificate of incorporation.
3- The powers and regulations that regulate the legal person.
4- The names of relevant persons holding senior management positions.
5- The address of the registered office; and
6- if different, the principal place of business.

Article (50)

The regulated entity must understand the ownership and control structure of the legal person and verify the identity of the beneficial owners, in accordance with the Law, the Implementing Regulations and these Rules.

If the legal person has a multi-layered ownership or control structure, the regulated entity must:

1- obtain an understanding of the legal person's ownership and control at each level of the structure;
2- obtain information confirming the existence of the legal person and his management at each level; and
3- document and maintain its findings about the legal person's ownership and control at each level of the structure.

Article (51)

If the customer, or owner of the controlling interest, is a corporation listed in a stock exchange that has disclosure requirements that enable the beneficial owner's identity to be verified in a fully transparent way, or an associate in which it owns a controlling interest, the regulated entity need not identify, nor verify the identity of, the shareholders or beneficial owners in those corporations and may instead satisfy the customer identification requirements by obtaining information from a public register, the customer or other reliable sources.

Article (52)

The regulated entity must identify the applicant for business or customer in case of NPOs by collecting the following information as a minimum:

1- The full name of the NPO.
2- The certificate of incorporation and intended purpose.
3- The articles of association of the NPO.
4- The jurisdiction in which the NPO was established.
5- The names of the persons holding the functions of the members of the Board of Directors of the NPO.
6- The principal place of business of the NPO.

The regulated entity must verify the identity of officers of the NPO who are authorized to establish a relationship with the entity or to adopt procedures in the management of the relationship on behalf of the NPO.

Article (53)

The regulated entity must identify the applicant for business or customer in case of a legal arrangement by collecting the following information as a minimum:

1- The legal arrangement's full name.
2- The nature and intended purpose of the legal arrangement.
3- The Jurisdiction where the arrangement was established.
4- The identities of the settlor, trustee and, if possible, the protector and the beneficiaries or class of beneficiaries; and
5- If possible, the principal place of business of the arrangement.

The regulated entity must understand the ownership and control structure of the legal arrangement and verify the identity of beneficial owners, in accordance with the Law, the Implementing Regulations and these Rules.

Article (54)

The regulated entity must identify the applicant for business or customer in case of a governmental body, a public institution or a firm wholly owned by the State or other public bodies and institutions or in which they own a controlling ownership interest, by collecting the following information as a minimum:

1- The full name of the applicant for business or customer.
2- The legal status and articles of association that regulate the applicant or the customer.
3- The main address.
4- The names of the natural persons authorized to work with the regulated entity on behalf of the applicant or customer and the relevant legal basis.

Article (55)

For customers who are legal persons, the regulated entity must identify and take reasonable measures to verify the identity of the beneficial owner using relevant information or data from a reliable source, as follows:

1- Identifying the natural person (s) who ultimately has an effective controlling ownership interest not less than 20% of a legal person or voting rights and taking reasonable measures to verify the identity of such persons.
2- If no individual can be identified as the beneficial owner of the legal person, or there is a doubt that a natural person who owns controlling interest is the beneficial owner under the previous item, or where no natural person exerts control through ownership interests, the regulated entity must identify the natural person (s) exercising de facto or legal control in the legal person and arrangement through any means, whether directly or indirectly, over the executives, the general assembly, or the operations of the legal person, or any other control instruments.
3- In case no natural person is identified under the provisions of the two previous items, the regulated entity must identify and verify the identity of the relevant natural person who holds a senior management position in the legal person.

If the regulated entity does not obtain satisfactory evidence of identity of at least one natural person under this Article, it must not accept a customer, carry out a transaction or continue a business relationship, and must terminate the business relationship for existing customers and file a suspicion report with the Unit.

For customers that are trusts, the regulated entity must identify and take reasonable measures to verify the identity of the beneficial owner by identifying the settlor**,** the trustee and the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising, directly or indirectly, ultimate effective control over the trust.

For other types of legal arrangements, the regulated entity must identify the natural persons in similar positions.

Moreover, the regulated entity must take the necessary procedures to determine whether a customer is acting as a trustee of a trust or holds an equivalent or similar position in other types of legal arrangements.

Section Two

CDD and Ongoing Monitoring

Article (56)

The regulated entity must determine, from the outset of its dealings with the customer, whether the customer is seeking to establish a business relationship with it, or is an occasional customer seeking to carry out a one-off transaction.

The regulated entity must apply CDD measures when:

1- establishing a business relationship with the customer;
2- conducting a one-off transaction for the customer with a value equal to or exceeding (QR 50.000) fifty thousand Qatari Riyals or several operations involving smaller amounts totalling to that amount, and the regulated entity must establish adequate measures to reveal such operations;
3- suspecting of money laundering or terrorism financing operation, irrespective of the amount of that operation; and
4- having doubts about the veracity or adequacy of data previously obtained.

Article (57)

If the regulated entity acquires the ongoing business, transactions or operations of another entity, it may not conduct CDD for transactions, operations or customers acquired if:

1- It obtains records of all transactions, operations, and customers acquired; and
2- It ensures that the other entity has taken all CDD measures for transactions, operations and customers acquired by the regulated entity in accordance with the AML/CFT Law, its Implementing Regulations and these Rules or the law of another jurisdiction that has an effective AML/CFT regime.

Article (58)

If it appears to the regulated entity that the other entity does not have records of transactions, operations and customers or that it has not taken CDD measures for acquired transactions or operations as stipulated in the previous Article, or if it was not possible to

establish whether these procedures have been taken, the regulated entity must develop and document an action plan that ensures that CDD is conducted for all customers with incomplete records or for acquired transactions or operations as soon as possible.

Article (59)

The regulated entity must conduct CDD measures before establishing a business relationship with the customer or before conducting a one-off transaction. However, the CDD may be conducted during the business relationship, in cases determined by the Section, provided that:

1- The identify is verified as soon as practicable;
2- this is necessary in order not to interrupt the normal conduct of business; and
3- there is little risk of money laundering or terrorism financing and any risks are effectively managed.

Article (60)

If the regulated entity establishes a business relationship or a one-off transaction with the customer under the previous Article but cannot complete CDD for the customer, the regulated entity must terminate the business relationship or one-off transaction, must not carry out a transaction for the customer and, where necessary, must make a suspicion report to the Unit.

Article (61)

The regulated entity must take into account the relative importance and risks related to its current customers when applying CDD measures and must take such measures for current business relationships at appropriate intervals, taking into consideration whether these measures have already been taken, when they were taken and the sufficiency of data obtained.

The regulated entity must also apply CDD to current customers if there is a material change in the nature of the customer or his ownership or in any aspect of the business relationship with the customer or if it lacks important information about the customer.

Article (62)

The regulated entity must decide, consistently with these Rules and according to a risk based approach, the extent of CDD measures for a customer, taking into account the risk factors stipulated in Article (24) of these Rules, and must be able to demonstrate that the extent of the measures is in line with the risks of money laundering and terrorism financing.

Article (63)

The regulated entity must conduct ongoing monitoring for all its customers and must, as far as possible and in a reasonable matter, examine the background and purpose of all complex or unusual transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose, like significant transactions or transactions that exceed limits set by the Section under instructions, or transactions that fall outside the regular pattern of a customer's activity. The regulated entity must also examine as far as possible the background and purpose of the mentioned transactions and must make and maintain a record of their findings.

Article (64)

The policies taken by the regulated entity in accordance with the previous Article must as a minimum:

1- flag transactions for further examination;
2- provide for the prompt further examination of these transactions;
3- provide for appropriate action to be taken on the findings of the further examination; and
4- If there is knowledge or suspicion of money laundering or terrorism financing raised by the findings, provide for a report to be made promptly to the regulated entity's compliance officer.

Article (65)

The monitoring mechanisms provided for in the policies stipulated in the previous Article particularly include the following:

1- Reviewing transactions as they take place or are about to take place.
2- Reviewing transactions after they have taken place.
3- Identifying particular types of transactions or the customers risk profiles.
4- Determining a set of approaches, such as comparing the transactions and operations of the customer, or the customers risk profiles, with those of customers in a similar peer group.

Article (66)

The regulated entity must have systems and controls to identify one-off transactions that are linked to the same person.

If the regulated entity knows or suspects, or has reasonable grounds to know or suspect, that a series of linked one-off transactions involves money laundering or terrorism financing, the regulated entity must make a suspicion report to the Unit and inform the Section of the matter in any written form, without disclosing any details or information about the report.

Section Three

Enhanced CDD

Article (67)

The regulated entity must apply enhanced CDD commensurately with the level of risk and ongoing monitoring in the following cases:

1- Business relationships and operations with customers or third parties from countries against which FATF calls for the adoption of such measures.
2- If the assessment of the business relationship reveals high money laundering or terrorism financing risks.
3- Other cases decided by the Committee or the Section.

Article (68)

Where ML or TF risks are high, the regulated entity must apply enhanced CDD, commensurately with the risks identified, and it must, in particular, increase the degree of monitoring for the business relationship, in order to identify unusual or suspicious operations or activities. Enhanced CDD measures must particularly include the following:

1- Obtaining additional information related to the customer, such as, profession, volume of assets and information available through public databases and open sources.
2- Updating on a regular basis the identification data of the customer and the beneficial owner.
3- Obtaining additional information on the intended purpose and nature of the business relationship.
4- Obtaining information on the sources of the customer's wealth and funds.
5- Obtaining information on the reasons for the expected transactions or the transactions that have been carried out.
6- Obtaining senior management approval before establishing or continuing a business relationship.

7- Conducting enhanced monitoring of the business relationship, by increasing the intensity and intervals of monitoring applied, and selecting patterns of transactions that require further examination and verification.
8- Making the first of any required payment through an account in the customer's name in a bank subject to similar CDD standards.

Section Four

Simplified CDD

Article (69)

The regulated entity may conduct simplified CDD measures that are commensurate with low risk factors resulting from the National Risk Assessment and its assessment of its risks, provided that there is no suspicion of money laundering or terrorism financing or distinct cases in which risks are high. The measures include:

1- Verifying the identity of the customer or beneficial owner after the business relationship has been established.
2- Reducing the intensity, extent and frequency of updates of customer identification.
3- Reducing the extent of ongoing CDD and scrutiny of operations based on a reasonable threshold.
4- Not collecting information, or not carrying out measures, to determine the purpose and intended nature of the business relationship, and instead inferring that purpose and nature from the transactions carried out under that relationship.

Simplified measures may only be related to accepting customers or ongoing monitoring.

The Section shall specify in Circulars the mechanisms for implementation of this Article.

Article (70)

The regulated entity may conduct simplified CDD if the customer or owner of the controlling interest is a corporation listed in a stock exchange that has disclosure requirements that enable the beneficial owner's identity to be verified in a fully transparent way, or an associate in which it owns a controlling interest.

Chapter Five

Reporting and Tipping-Off

Section One

General Provisions

Article (71)

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

Article (72)

The regulated entity must consider the following matters in particular in deciding whether an unusual transaction or a transaction that is inconsistent with a customer's known legitimate business or the size of his transactions is a suspicious transaction:

1- Whether the transaction has an apparent economic or lawful purpose;
2- Whether the transaction has a reasonable explanation or whether the customer has failed to give an adequate explanation for the transaction or to fully provide information about it;
3- Whether the transaction involves the use of a newly established business relationship or is for a one-off transaction;
4- Whether the transaction involves the use of offshore accounts, companies or structures that are not supported by the customer's economic needs;
5- Whether the transaction involves the unnecessary routing of funds through third parties.

Section Two

Internal Reporting

Article (73)

The applicable polices must ensure immediate submission of internal reports to the compliance officer when suspecting or having reasonable grounds to suspect that a ML or TF offence has been committed, and must enable any officer or employee to contact the compliance officer while respecting confidentiality and while reducing administrative communication channels as much as possible.

Article (74)

If an officer or employee at the regulated entity, in the course of office or employment, knows, suspects, or has reasonable grounds to suspect, that funds are related to or involve the proceeds of a predicate offence or are related to terrorism financing, the officer or employee must promptly make a written or oral suspicious transaction report to the regulated entity's compliance officer.

The officer or employee must prepare the internal report, regardless of the following:

1- the amount of any transaction or operation;
2- whether or not any transaction relating to the funds involves tax matters;
3- Whether or not no transaction or attempt to begin a transaction has been, or will be, conducted.
4- Whether the regulated entity has terminated any relationship with the customer;
5- Whether any attempted money laundering or terrorism financing activity in relation to the funds has failed.

When submitting a suspicious transaction report to the compliance officer, the officer or the employee must promptly give the compliance officer details of every subsequent transaction of the applicant or customer involved in such report, whether or not of the same nature as the transaction that gave rise to the internal report, until the compliance officer tells the officer or employee not to do so.

Article (75)

If the compliance officer of a regulated entity receives a suspicious transaction report, the compliance officer must promptly do the following:

1- Properly document the report if received orally, when the regulated entity's applicable policies allow a report to be made orally;
2- Give the officer or the employee making the report a written acknowledgment for the report, together with a reminder about the provisions related to tipping-off;
3- Consider the report and decide whether the transaction is suspicious without delay.

Section Three

External Reporting

Article (76)

The applicable policies at the regulated entity must include the following:

1- Notifying the Unit immediately by the compliance officer of suspicion reports relating to transactions or operations or attempted transactions or operations, when

suspecting or having reasonable grounds to suspect that they relate to or involve proceeds of a predicate offence or relate to terrorism financing.

2- Postponing the implementation of transactions included in the report for a period not exceeding forty-eight (48) hours upon request of the Unit, in accordance with Article (35) of the Law.
3- Effective cooperation with the Unit and law enforcement authorities in terms of suspicion reports submitted by the regulated entity.

Article (77)

If the compliance officer or his deputy at the regulated entity, in the course of office or employment, knows, suspects, or has reasonable grounds to suspect, that funds are related to or involve the proceeds of a predicate offence or are related to terrorism financing, a suspicion report on the matter must be immediately submitted to the Unit.

The compliance officer or his deputy must submit a suspicion report to the Unit regardless of the following:

1- Whether or not an internal suspicious transaction report has been made;
2- The amount of the transaction or operation relating to the funds;
3- Whether or not any transaction relating to the funds involves tax matters;
4- Whether or not a transaction or attempt to conduct a transaction has been, or will be, conducted;
5- Whether or not the regulated entity has terminated any relationship with the customer; and
6- Whether or not any attempted money laundering or terrorism financing activity in relation to the funds has failed.

The suspicion report shall be made based on the form prepared by the Unit for this purpose.

Moreover, the regulated entity shall inform the Section of the submission of the suspicion report to the Unit in any written form, without disclosing any information or details about the report.

Article (78)

The regulated entity may, after making a suspicion report to the Unit, restrict or terminate, in the normal course of activity, its business relationship with the customer subject of the said report, provided that it does not result in tipping-off or warning the customer.

If the regulated entity restricts or terminates a business relationship with a customer, it must tell the Section in any written form, about the restriction or termination.

Section Four

Reporting Records

Article (79)

The compliance officer of the regulated entity must make and keep records:

1- showing the details of each internal suspicious transaction report the compliance officer receives;
2- showing compliance with the provisions of Article (75) of these Rules; and
3- showing the details of each suspicion report made to the Unit.

Article (80)

The regulated entity must not destroy any records relating to the applicant for business or customer after the legally specified period for maintaining the records ends without consulting with the Unit, in the following cases:

1- If the regulated entity makes a suspicion report to the Unit in relation to an applicant for business or a customer; or
2- If the regulated entity knows that an applicant for business or customer is under investigation by a law enforcement agency in relation to money laundering or terrorism financing.

Section Five

Tipping-Off and Confidentiality

Article (81)

The regulated entity must not disclose information to any unauthorized person relating to the submission or non-submission of a suspicion report to the Unit or any other relevant information that may result in:

1- a customer knowing or suspecting that he is or may be the subject of:
    a. a suspicion report; or
    b. an investigation relating to money laundering or terrorism financing; and
2- may prejudice the prevention or detection of ML and TF offences, the apprehension or prosecution of offenders or the recovery of proceeds of crime.

If the regulated entity believes, on reasonable grounds, that an applicant for business or a customer may be tipped off by conducting CDD or ongoing monitoring, the regulated entity must make a suspicion report to the Unit instead of conducting the measures or monitoring.

The procedures and controls established by the regulated entity must protect the confidentiality of information relating to the suspicion reports.

Article (82)

The principle of tipping-off in the previous Article shall not prevent the regulated entity from sharing information with foreign branches and majority-owned associates.

The act of auditors in advising a customer against engaging in an illegal act does not constitute tipping-off, as stipulated in the previous Article.

Chapter Six

Screening and AML/CFT Training Programme Requirements

Section One

Screening Procedures

Article (83)

The regulated entity must have adequate screening procedures to ensure that officers and employees who are appointed or employed have the required competence and integrity.

The screening procedures that the regulated entity must take before appointing or employing officers or employees, must include, as a minimum:

1- Identification data of the individual and relevant supporting documents;
2- Information about the individual's employment history and qualifications;
3- Details of any regulatory action taken in relation to the individual; and
4- Details of any criminal convictions of the individual.

Section Two

AML/CFT Training Programme

Article (84)

The regulated entity must design an appropriate ongoing AML/CFT training programme for its officers and employees, which must ensure that the officers and employees are aware, and have an appropriate understanding, of the following:

1- Their legal and supervisory responsibilities and obligations, particularly those under the AML/CFT Law, its Implementing Regulations and these Rules.
2- Their role in preventing money laundering and terrorism financing and the liability that they, and the regulated entity may incur for involvement in money laundering or terrorism financing; and failure to comply with the AML/CFT Law, its Implementing Regulations and these Rules.
3- How the applicable regulations are managing and mitigating money laundering and terrorism financing risks, the role of the compliance officer and the importance of CDD and ongoing monitoring.

4- Money laundering and terrorism financing risks, techniques, trends, patterns and indicators, the vulnerabilities of the products and services offered by the regulated entity and the means for providing them, as well as how to access and assess information to reveal, where necessary, suspicious transactions.
5- The regulated entity's internal processes for making internal suspicious transaction reports.

Article (85)

In making a decision about the appropriate training for its officers and employees, the regulated entity must consider the following:

1- Their differing needs, experience, skills and abilities.
2- Their differing functions, roles and levels in the entity.
3- The degree of supervision over, or independence exercised by, them.
4- The availability of information that is needed for them to decide whether a transaction is suspicious.
5- The size of the regulated entity's business and the risk of money laundering and terrorism financing.
6- The outcome of reviews of their training needs.

Article (86)

The regulated entity's permanent AML/CFT training programme must ensure that its officers and employees have the necessary AML/CFT knowledge, skills and abilities and are kept up to date with new AML/CFT developments, including the latest money laundering and terrorism financing techniques, trends, patterns and indicators.

The regulated entity must, at regular and appropriate intervals, carry out reviews of the AML/CFT training needs of its officers and employees and must ensure that the needs are met effectively. If a review identifies deficiencies in the entity's AML/CFT training, it must prepare an action plan to remedy the deficiencies.

Chapter Seven

Record-Keeping

Section One

General Record-Keeping Obligations

Article (87)

The regulated entity must make the records necessary to demonstrate how:

1- the key AML/CFT principles in these Rules have been complied with;
2- the regulated entity's senior management has complied with responsibilities under the AML/CFT Law, its Implementing Regulations and these Rules;
3- the regulated entity's risk-based approach has been designed and implemented;
4- each of the regulated entity's risks have been mitigated;
5- CDD and ongoing monitoring were conducted for each customer; and
6- CDD and ongoing monitoring were enhanced where required by the AML/CFT Law, its Implementing Regulations or these Rules.

Examples of records that must be kept:

a- documents and data obtained while performing CDD
b- account files
c- business correspondence of the customer
d- results of analysis of suspicious transaction reports

The operations records should be sufficient to permit reconstruction and reorganization of individual operations so as to conduct data analysis and provide, if necessary, evidence for prosecution of criminal activity.

The regulated entity must make and keep records of the AML/CFT training provided for its officers and employees, including, as a minimum the dates the training was provided, the nature of the training and the names of the individuals to whom the training was provided.

Section Two

How Long Records Must Be Kept

Article (88)

All records, documents and data of all local and international transactions and operations must be kept by the regulated entity for at least ten (10) years after the date on which the transaction or operation ends.

It must also keep all records, documents and data it has obtained or collected through CDD measures, as well as account files, business correspondence and the results of any analysis

carried out, for at least ten (10) years after the date on which the business relationship ends or after the occasional transaction or operation is completed.

Article (89)

The regulated entity must ensure that all records stipulated in the previous Article can be retrieved without delay for competent authorities and must develop adequate systems that would enable it to quickly respond to requests by said authorities.

Article (90)

The regulated entity must make and keep records relating to business relationships with all customers and all transactions carried out with or for the customer, enabling it to:

1- Assess its compliance with the AML/CFT Law, its Implementing Regulations, these Rules and the applicable policies.
2- Reconstruct and reorganize transactions.
3- Comply with any request by the Unit, Supervisory Authorities, competent authorities, law enforcement authorities or judicial authorities.
4- Indicate the nature of any documents and evidence obtained and submit them to the competent authorities.

****