AML/CFT Compliance Guidance for Auditors (Chartered Accountants)

2020

وزارة التجارة والصناعة
Ministry of Commerce and Industry

Table of contents

Introduction

Money laundering (ML) and terrorism financing (TF) are among the serious crimes threatening the stability, reputation and integrity of the financial systems of countries, and also among core scourges facing the international community such as, organized crimes, corruption, trafficking in human beings, terrorism and other emerging crimes.

Money laundering and terrorism financing have devastating economic and social consequences, as they may cause reputational damage to financial markets; State's deprivation from its financial resources that can be allocated for employment, growth and public facilities; unequal distribution of national income, drop in national saving, increase in inflation rates, depreciation of national currency against increased demand of foreign currencies, prejudice to fair competition, negative impact on consumption patterns through the emergence of the excessive and immoderate consumption, increased corruption, and bribery.

In general, ML includes all actions and procedures through which proceeds of a criminal activity are layered to conceal their illicit source. It is also an operation or series of operations aiming at concealing the criminal origin of funds to make them appear as generated from a licit activity and legitimate to be used in the formal or visible economy, or likely to finance an illicit commercial activity. From this perspective, ML operations are ancillary activities to previous criminal activities generating illicit funds.

As for terrorism financing, it comprises all forms of material support to terrorism or those who promote terrorism, plan or participate in terrorist acts.

Initially, money laundering was essentially limited to financial institutions by abusing the financial and banking sectors to conceal and disguise the criminal nature of some funds. However, this phenomenon expanded to include designated non-financial businesses and professions (DNFBPs) (including legal professions such as accountants, lawyers, trust and company service providers) to be used for the same purpose. This prompted the Financial Action Task Force (FATF)[1], in 2003, to extend its Recommendations on combating money laundering and the financing of terrorism, to certain Non-Financial Businesses and Professions, and to set out the submission of the DNFBPs to AML/CFT requirements[2] . This draw up or expansion was not general, but rather limited to some activities conducted by such professions, which involve ML/TF risks.

Risks associated with auditors (chartered accountants) [3], as independent professionals, in the ML/TF field, lie basically in the potential use of this profession to conceal the identity of the beneficial owners, engage in

[1]The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 in the French capital, Paris. The mandate of the FATF is to set standards and to promote policies and measures for combatting money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction, to protect the international financial system.

[2].In fact, certain businesses and professions outside the financial sector are particularly attractive to illicit actors seeking to launder funds or commit other financial crimes, since they can be exploited to help criminals to conceal and/or facilitate the movement of criminal proceeds into the licit financial sector.
Because they are at high risk of abuse, they are subject to special requirements similar to those imposed on financial institutions. These business and professions are known as Designated (selected) Non-Financial Businesses and Professions (DNFBPs).

[3] Within the framework of this Guidance, the term "Auditor" is used following the issuance of Law No. (8) of 2020 on the Regulation of the Auditing Profession repealing the Law No. (30) of 2004 on Regulating the Auditing Profession which uses the term "Chartered Accountant" for the natural or legal person who is registered in the Register of Practicing Chartered Accountants. Since Law No. (8) of 2020 entered into force, the term "Chartered Accountant" has been replaced with the term "Auditor" although both terms refer to the same tasks and same profession. Therefore, pursuant to the AML/CFT Law No. (20) of 2019, the legal AML/CFT obligations of the "Chartered Accountants" also apply to "Auditors".

financial transactions or provide services that may help disguising the proceeds of the criminal activities in order to conceal their illicit source. The following are some services provided by auditors and that may be used in ML and TF:
- Establishing companies or other legal arrangements (such as trusts), as such services may conceal the link between the proceeds of the crimes and the criminals.
- Buying and selling of real estates, as the transfer of the real estate ownership is to cover the illicit funds transfer or the final investment of the proceeds passed through money laundering operations.
- Conducting financial operations on behalf of customers, like cash deposit or withdrawal, foreign currency exchange operations, sale and purchase of shares, sending and receiving international money transfers[4].
- Providing consultation and services with the intention of evading taxes.

In general, due to their high risks, countries have criminalized ML and TF and imposed penalties against the perpetrators, which is the case of the State of Qatar that has criminalized ML and TF and imposed criminal penalties on perpetrators and accomplices pursuant to Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

However, in order to comprehensively address money laundering, a preventive approach, along with a dissuasive or penal approach must be adopted. Financial institutions and Designated non-financial businesses and professions (DNFBPs, including auditors) will have obligations and responsibilities to abide by in order to prevent or detect ML or TF operations, or identify perpetrators. The AML/CFT regime requires the integration of both the preventive and dissuasive approaches.

This guidance aims at introducing legislations relating to combating money laundering and terrorism financing, clarifying and simplifying the AML/CFT obligations of the auditors as per Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, the Council of Ministers' Decision No. (41) of 2019 Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing , Decision of the Minister of Commerce and Industry No. (48) of 2020 promulgating AML/CFT Rules for legal Auditors, Dealers in Precious Metals or Precious Stones and Trusts and Company Service Providers , in order to raise awareness of the risks of money laundering and terrorism financing, and assist auditors in complying with AML/CFT requirements, particularly in relation to the obligation of reporting suspicious transactions reports (STRs), and file high quality STRs to assist the Qatar Financial Information Unit (QFIU) in performing its tasks effectively and efficiently.
The Anti-Money Laundering and Terrorism Financing Section, established pursuant to Decision No. (95) of 2019, under the MOCI Companies Affairs Department, is responsible for monitoring the compliance of the auditors with the AML/CFT requirements set forth in this Guidance, and proposing the administrative and financial sanctions against auditors who violate the provisions of the Law, its Implementing Regulations and any relevant decisions or instructions.

It's worth to note that this AML/CFT guidance is intended by the Ministry of Commerce and Industry to raise the awareness of the auditors of ML/TF risks, highlight their legal obligations and introduce a relevant comprehensive legislative approach. However, this document shall not replace, under any circumstances, any legal texts, laws and regulations applicable in the State and published in the official gazette, which shall be considered the official reference for identifying the legal obligations of the auditors and other DNFBPs subject to AML/CFT requirements.

There is no doubt that auditors' compliance with such requirements shall promote the State's efforts to combat money laundering and terrorism financing and ensure the integrity and safety of the economic and financial activities in the State.

[4] MENAFATF, DNFBPs in Relation to Anti- Money Laundering and the Combating of Terrorism Financing, November 2008. Pages 3--4.

Chapter One

Stages and Methods of Money Laundering

Money laundering encompasses illicit earnings resulting from a wide range of criminal activities (sale of arms, human trafficking, bribery, fraud, extortion, prostitution, deceit, breach of trust, etc.). Laundering the proceeds of these various criminal activities, implies multiple stages and is carried out using various methods.

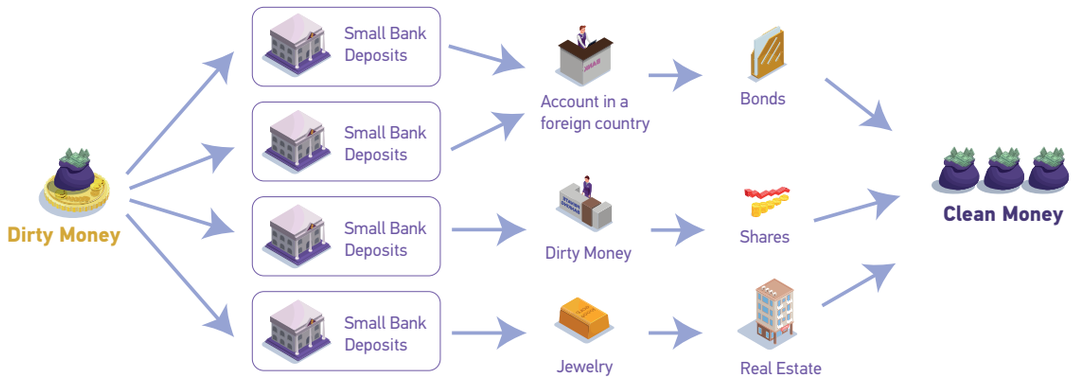
Section One: Money Laundring Stages:

Money laundering consists of three stages as follows:

1. Placement:
at this stage the generated illicit funds are introduced into the financial system, usually through a financial institution, but also through cash purchases of high-value items, such as cars or real estate. This may be achieved through cash deposits in a bank account, large amounts of cash are often structured into smaller and less visible amounts deposited at different times and in different branches of a financial institution(s). It is important to note, however, that not all crimes result in cash proceeds; crimes such as fraud, embezzlement and corruption will frequently result in transfers of proceeds directly into the perpetrator's bank account. Criminal proceeds can also take the form of cryptocurrencies, such as Bitcoins.

2. Layering: also referred to as "obscuring":
this second stage of ML starts after the introduction of the illicit funds into the channels of the legitimate financial system, whereas money launderers separate the illicit funds to be laundered from their source. This is done by the sophisticated layering of the financial transactions in order to make it legitimate, and make the source of such illicit funds difficult to trace ; and that by transferring funds or securities from one bank to another, or to any form of bearer negotiable instruments (BNIs) such as cheques, banker's drafts and money orders, or to other accounts in different jurisdictions, or to banks in countries with strict rules protecting banking secrecy, known as "financial havens", or by layering the transferred amount through fictitious goods or services.

3. Integration:
at this final stage of ML, the illicit funds are converted into apparently legitimate business earnings or proceeds by being integrated into the economy or the banking sector. For example, settling fictitious invoices, buying over priced front companies, concluding successive sales and false loans, etc.



Section Two: Money laundering Methods

The methods and Mechanisms of Money laundering are diverse and multiple. The following are the most significant ML methods:

- Structuring or smurfing: cash amounts are structured and broken up into smaller amounts and deposited in financial institutions to be layered below the applicable designated threshold of reporting. This method requires the use of "mules" who are often trusted by, or close associates of, the launderer.

- Purchase of assets in cash: launderers aim at purchasing high value assets in cash, such as cars, yachts, gold, or jewelry. Afterwards, launderers use or sell these assets but often register them in the names of close associates to avoid raising doubts.

- Smuggling of significant cash amounts: significant amounts of cash are smuggled across borders to another State and deposited in an offshore bank having strict rules in terms of bank secrecy, and without an effective AML/CFT regime.

- Cash-intensive businesses: money launderers usually engage in cash revenue-producing activities and businesses. The accounts of such activities and businesses are then used to deposit funds generated from a criminal activity. These businesses operate openly and thus generate cash proceeds from legitimate activities (conducted secondarily), in addition to illicit cash. In such cases, these businesses usually pretend that all cash received is legitimate profits from their apparent activities (cash-intensive activities), and these activities are mostly related to the services sector given the difficulty in discovering the differences between revenues and costs, such as restaurants, bars, casinos, parking, etc.

- Trade-based money laundering: it is the process of disguising the proceeds of crime and moving (or manipulating) value through the use of trade transactions in an attempt to legitimize their illicit origins[5]. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail. For example, artworks can be used for money laundering purposes, given that their price is related to many subjective factors as well as the absolute confidentiality of the persons involved in this sector in terms of not disclosing the identity of the buyer and seller.

- Alteration of value: the launderer purchases a property from a person willing to become an accomplice, by stating in the Contract of Sale a value for the property less than its actual price. For example, the launderer purchases a property that worth QR 1 million, but in the Contract of Sale the value is stated QR 500, 000 only. After a short period of time, the property is sold at its actual price (i.e. QR 1 million), and the launderer obtain false justification of the source of the funds at about QR 500,000.

- Money laundering through life insurance contracts: the launderer enters into a life insurance contract at high premiums, then cancel or renounces the contract and receives a part of the amount agreed upon; to receive later on a justification for the funds obtained illicitly.

The above methods reflect the general money laundering patterns. However, some other methods involve DNFBPs (specifically legal professions and accountants) in terms of planning and implementing ML schemes. The FATF considers that professionals, practitioners and experts may largely contribute to the enhancement of the capacities of perpetrators by planning complex and advanced ML schemes to conceal, collect, move or use illicit sources of wealth[6]; including but not limited to:

- Establishing shell trusts: trusts may be used to conceal or obscure the beneficial owners of funds, by separating the legal ownership from the beneficial ownership (or the effective control) of the assets.

- Self-borrowing schemes: whereas launderers lend themselves their own laundered proceeds. The launderer hands over the illicit funds to an accomplice, who lends back the launderer an amount equal to the amount previously received from him. This transaction is then documented in a loan contract (in good and due form) to legitimize the funds of the launderers.

- Establishing shell companies: which are incorporated companies (legal entity), but have no independent operations, significant assets, ongoing business activities, or employees. Shell companies are often established with several forms of ownership structures, with the participation of partners from several countries.

- Designing and conception of schemes: aimed at concealing the beneficial owner of a legal person, in order to allow the separation between the natural person (money launderer) and the funds derived from a criminal offense.

- Establishing and managing front companies: A front company is a fully functioning company with the characteristics of a legitimate business. Front companies often operate in service-oriented businesses such as restaurants, clubs and salons, as such businesses are cash-intensive. Front companies are used in money laundering by integrating and mixing the criminal proceeds with the proceeds of legitimate activities of the said companies.

- Concealing the beneficial owner of natural persons: which allows separation between the natural person (launderer) and funds generated from criminal activities, such as designing a complex ownership and control structure of overlapping layers of partners of legal persons, to conceal and separate between the beneficial owners and assets, multiple beneficiaries of one account, and use of legal persons such as directors or board members.

- Serving as nominee directors for some companies: while deliberately not disclosing the nominator or actual and real director.

- Providing assistance and consultation in fraudulent schemes: aiming at changing the legal form or name of some contracts with the intent to deceive; or at using false or forged invoices for tax evasion purposes.

[5]. Financial action task force, Trade based money laundering, 2006.

[6]. FATF, Professional money laundering, July 2018.

Chapter Two:

Criminalization of Money Laundering and Terrorism Financing

Article (2) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing clearly and explicitly criminalizes ML, as follows:

Whoever intentionally commits any of the following acts shall be deemed to have committed money laundering offence:

1. Conversion or transfer of funds, knowing that they are proceeds of a crime or an act of participation in the said crime; with a view to concealing or disguising the illicit source of funds or assisting any person involved in the commission of the crime to evade the legal consequences of his actions.
2. Concealment or disguise of the true nature, source, location, disposition, movement, ownership or the rights of funds, knowing that they are the proceeds of a crime.
3. Acquisition, possession or use of funds, knowing, at the time of receipt thereof, that they are proceeds of a crime.
4. Participation in, association with or conspiracy to commit, attempt, or aid, abet, facilitate, counsel in, cooperate in, or contribute to the commission of any of the acts stipulated in this Article.

The Money Laundering crime shall be considered as an independent crime from the predicate offence. When proving that funds are the proceeds of crime, it shall not be necessary that a person be convicted of a predicate offence.
The punishment of the persons committing the predicate offence shall not prevent their punishment for the money laundering crime.

Based on the above Article, the general characteristics of the ML crime can be described as follows:

1. Money laundering crime is an ancillary offence or a crime of consequence: Money laundering crime is perpetrated after the commission of a principal offence, which generates proceeds. This principal offence is referred to as the predicat offence[7].

2. Material elements of the ML crime include concealment and disguise: concealment refers to any act, which prevents detecting the true illicit source of funds by any means whatsoever, while disguise refers to any act by which a false sophisticated source is elaborated and tailored providing apparently veil of legitimacy over the funds generated by a criminal activity.

3. Any funds or proceeds may be laundered and consequently the underlying conduct is criminalized: any funds or assets (whether corporeal or incorporeal, tangible or intangible, movable or immovable), including the revenue, income, or interest derived or obtained, directly or indirectly, from committing a predicate offence may be an underlying money laundering crime.

4. The Money laundering crimes often entail providing false justification for the source of funds or have a false justification as their goal: the perpetrator intentionally and willfully provides false justification for the source of illicit funds. In an attempt to legitimize their illicit origin, many false justification variations may be employed such as fictitious invoices, counterfeit certificates, fictitious loan agreements, making false statements on bank documents, establishing shell companies, etc. As such, money laundering is an intent crime. However, in practice, the knowledge and intent required to prove money laundering or terrorism financing offences, may be inferred from objective factual circumstances.[8]

5. The ML crime is an ancillary crime or a crime of consequence because it requires proof of a predicate offence that was previously committed and resulted in criminal proceeds, which would be subject of the ML crime. The prosecuting authority shall prove the predicate offence.

6. Money laundering is an independent crime of the predicate offence: although the Money laundering crime is preceded by a predicate offence, it should be considered as an independent crime of the predicate offence. A perpetrator may be prosecuted for committing a ML crime, even if he was not prosecuted for the predicate offence, irrespective of any related obstacles that prevent the prosecution of the predicate offence [9], for example in circumstances when the perpetrator is not identified or unknown, or by reason of statute of limitations, or when the crime is committed outside the State. This should not preclude proceedings.

7. The ML offender may be (a) either the perpetrator of the predicate offence: in this case he proceeds by his own with concealing the true criminal source of funds; (b) or any other person who assists (the perpetrator of the predicate offence) in disguising the criminal source of funds, for the purpose of integrating the proceeds of crime into the formal economy.

8. Sanctions imposed for committing a money laundering crime : any person who commits any of the money laundering crimes, shall be sentenced to imprisonment for a term not exceeding ten (10) years, and a fine not less than (QR 2.000.000) two millions Qatari Riyals and not more than (QR 5.000.000) five millions Qatari Riyals, or twice the value of the money laundered, whichever is greater. [10]

[7]. Article (1) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing defines the "Predicate Offence" as 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 is an offence punishable by law in both countries
[8]. Article (5) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.
[9]. Article (2) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.
[10]. Article (78) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

Article (3) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing clearly and explicitly criminalizes terrorism financing, as follows:

Whoever intentionally, by any means, directly or indirectly, with an unlawful intention provides or collects funds to be used, or while knowing that they are to be used, in whole or in part, in any of the following, shall be deemed to have committed a terrorist financing offence:

1. To carry out a terrorist act(s);
2. By an individual terrorist or by a terrorist organization, even in the absence of a link to a specific terrorist act or acts;
3. To finance the travel of individuals to a State other than their State of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;
4. To organize or direct others to commit or attempt to commit any of the acts stipulated in this Article.
5. To participate; collude; aid, abet, facilitate, counsel in, cooperate in, conspire to commit or attempt to commit any of the acts stipulated in this Article.

The terrorism financing offence extends to any funds, whether from a legitimate or illegitimate source, regardless of whether the funds were actually used to commit or attempt to commit a terrorist act, or are linked to a specific terrorist act.

The terrorism financing offence shall be deemed to have been committed, irrespective of whether the person charged with committing the offence is present in the same country or where the terrorist or terrorist organization is located or where the terrorist act was committed , or would be committed or in any other State.

The terrorism financing offence shall be considered a predicate offence of money laundering.

Accordingly, the following can be noted:

1. Criminalizing terrorism financing is a basic requirement for combating terrorism: prosecuting and imposing criminal sanctions on terrorism financiers and confiscating terrorists' funds, are effective and successful means to mitigate the resources and capabilities of terrorist groups.

2. Whoever intentionally, by any means, directly or indirectly, with an unlawful intention provides or collects funds to be used, or while knowing that they are to be used, in whole or in part, in any of the following, shall be deemed to have committed a terrorist financing offence:

a. To carry out a terrorist act(s).
b. By an individual terrorist.
c. By a terrorist organization.

3. Terrorism financing also includes financing the travel of individuals to a State other than their States of residence or nationality for the purpose of perpetrating, planning, preparing, or participating in terrorist acts, providing or receiving terrorist training.

4. TF offences should extend to any funds or other assets **whether from a legitimate or illegitimate source.**

The terrorism financing offence extends to any funds, that are 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.

5. The terrorism financing offence shall be deemed to have been committed irrespective whether the funds or other assets were actually used to carry out or attempt a terrorist act, or are linked to a specific terrorist act.

6. TF offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organization(s) is located or the terrorist act(s) occurred/will occur : the location of the person alleged to have committed the TF offence, shall not impact the fact that the offence is committed or not.

7. Any person who commits any of the terrorism financing crimes shall be sentenced to imprisonment for a term not exceeding twenty (20) years, and a fine not less than (QR 5.000.000) five millions Qatari Riyals and not more than (QR 10.000.000) ten millions Qatari Riyals, or twice the value of the financing provided, whichever is greater.[11]

8. the Legal Person is punished for a ML/TF crime. Article (77) of the Law No.(20) of 2019 on Combating Money Laundering and Terrorism Financing stipulates that: « a legal person, on whose behalf or for whose benefit any of the crimes stipulated in this Law has been committed by any natural person, acting either individually or as part of an entity of the legal person, or serves in a leading position therein, or represents the legal person, or is authorized to take decisions or exercise control on behalf of the legal person, and acts in such capacity, should be sentenced to a fine not less than (QR 4.000.000) four million Qatari Riyals and not more than (QR 8.000.000) eight million Qatari Riyals, or threefold the maximum fine applied to such offence, whichever is greater. The above should not prevent the punishment of the natural person, perpetrator of the crime, with the corresponding penalty prescribed by this Law. The Court may order that the legal person be prohibited, either permanently or temporarily, from directly or indirectly carrying on certain business activities, or be subjected to judicial supervision, or to close permanently or temporarily the premises used for perpetrating the offence, or to dissolve and liquidate his business. The Court may also order that the judgment issued against the legal person in relation thereto, be published in two daily newspapers at the legal person's own expense».

[11]. Article (79) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

Chapter Three

Preventive Measures for Money Laundering and Terrorism Financing: AML/CFT Legal Obligations for Auditors

Auditors fall within the category of DNFBPs according to Article (1) of the Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

In general, auditors provide the following services:

1- Review and audit financial accounts and give advice according to the accounting and auditing standards approved in the State.
2- Prepare reports on financial statements, balance sheets, annual and periodic accounts of their customers.
3- Provide expertise, advice and studies in financial, economic and taxation fields.
4- Liquidation activities.
5- Any other tasks assigned to them under the applicable laws in the State[1].

[1]. Article (21) of Law No. (8) of 2020 on the Regulation of the Auditing Profession.

1. What are the auditors' activities that are subject to AML/CFT compliance requirements?

As per Law No. (20) of 2019 on Combating Money Laundering and Terrorism financing, auditors shall be subject to the obligations stipulated in the Law 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: As the transfer of the real estate ownership is used to cover the illicit funds transfer (layering phase of ML indicated below) or the final investment of the proceeds passed through laundering operations (integration phase).
- Management of the customer's funds, securities or other assets.
- Management of bank accounts, saving accounts or securities accounts: such as execution of financial transactions on behalf of customers, like cash deposit or withdrawal, foreign currency exchange operations, sale and purchase of shares, or sending and receiving international money transfers.
- 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: whereas the establishment of companies or other complex legal arrangements (like trusts) may conceal the link between the proceeds of the crimes and the criminals.

The following, are guidelines and recommendations for auditors on how to comply with the above-mentioned provisions:

- If the auditors conduct any of these activities (qualifying activities), they must have an AML/CFT programme at all times.
- If the auditors are performing qualifying activities for the customer, they must carry out CDD and all relevant AML/CFT obligations. They don't have to conduct CDD if they don't do any qualifying activities for the customer.
- The auditors should have operational controls to ensure their compliance with CDD requirements when the customer's nature of work changes.
- The auditors must comply with recordkeeping requirements for all the above-mentioned qualifying activities.

2. To whom shall the Guidance apply?

This Guidance shall apply to auditors whether as sole practitioners, partners or employed professionals within professional firms, who are included in one of the following registers:
- the Register of Physical auditors.
- the Register of accounting Offices and Companies.
The provisions of this Guidance shall apply to:
- All branches and majority-owned subsidiaries of auditors' firms and offices in the State of Qatar.
-All branches and majority-owned subsidiaries of auditors' firms and offices headquartered in the State of Qatar.

Auditors may practice their profession as sole practitioners (natural person)[12], or under a joint liability company established for this purpose, in participation with Qatari or non-Qatari auditors, and shall be registered in the Register of Accounting Offices and Companies[13]. The branches of non-Qatari accounting firms may practice the profession in Qatar upon registration in the Register of Accounting Offices and Companies, and subject to complying with the obligations stipulated in Article (11) of Law No. (8) of 2020 on the Regulation of the Auditing Profession.
Auditors, whether as sole practitioners (natural persons) or under joint liability companies or branches of companies and non-Qatari accounting offices, shall comply with the obligations provided for in Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, which will be mentioned respectively.

Obligation 1: Development of an AML/CFT Programme:

Principle: Auditors shall develop an AML/CFT programme[14], considering AML/CFT risks; size, complexity and nature of the businesses. The design and implementation of such compliance programme is a prerequisite to ensure compliance with the provisions of the AML/CFT Law and meeting all the obligations related to the verification of the customers' identity, record- keeping and reporting.

Components of the Programme:

Auditors shall develop an AML/CFT programme that includes internal policies, procedures, systems and controls aiming at preventing ML and TF. The programme shall include the following:
- Appropriate compliance management arrangements[15], including the appointment of a compliance officer at the office level.
- Adequate screening procedures to ensure high standards of efficiency and integrity when appointing or employing officers and employees.
- Appropriate ongoing training programme for officers and employees.

[12]. Articles (1), (2), (3), and (4) of Law No. (8) of 2020 on the Regulation of the Auditing Profession.
[13]. Article (7) of Law No. (8) of 2020 on the Regulation of the Auditing Profession.
[14]. Generally, the term programme refers to sets of applicable instructions and rules designed to implement a certain task. A programme is a series of instructions or topics that are closely related to a certain field, that is arranged and organized in advance according to a particular structure in which precise rules are followed.
[15]. Arrangements refer to measures and procedures taken and implemented in special cases.

- Independent audit and review function to test compliance with AML/CFT policies, procedures, systems and controls.
- Appropriate and ongoing review and assessment of policies.

In practice, the auditor shall develop a guidance on procedures, systems, and internal controls aiming at combatting money laundering and terrorism financing, provided that it should be disseminated to the relevant employees in order to understand and apply the related requirements.

1. Appointing a Compliance Officer:

The compliance officer is responsible for overseeing and managing the regulated entity's compliance with the AML/CFT requirements stipulated in the AML/CFT Law, its Implementing Regulations and the MOCI's AML/CFT Rules for Auditors (Chartered Accountants), Dealers in Precious Metals or Precious Stones, Trusts and Company Service Providers. The compliance officer shall particularly prepare and submit STRs to the QFIU; and shall be responsible for the effective implementation of the AML/CFT Programme (ensuring that appropriate policies, procedures, systems and controls are established and developed on a regular basis, risk assessments, audit and review is conducted to ensure the effectiveness of this Programme).
Practically, if the auditor, is a natural person exercising his activity in an individual establishment or office, he should personally undertake the responsibilities of the senior management and the compliance officer, within his establishment or office, and may designate one of his qualified employees as a compliance officer. If the auditor is exercising his duties under a joint liability company, branch of a company or a non-Qatari accounting office, the management of the company should appoint a compliance officer to manage the company's compliance with AML/CFT requirements, and submit STRs to the QFIU (Artical 2 of the AML/CFT rules).
The name and full data of the compliance officer must be reported to AML/CFT Section and to the Qatar Financial Information Unit (QFIU). The compliance officer is mainly responsible for preparing and submitting STRs to the QFIU, and informing the Section thereof.
Upon his appointment, the compliance officer shall, be granted the necessary powers to perform his duties independently, while maintaining the confidentiality of the information received and the procedures taken. The compliance officer may, while performing his duties, have access to the necessary records and data. The compliance officer should be able to communicate, directly and periodically, with the Board members or the auditor (natural person)[16] , being the natural person, to raise any issue related to the compliance with AML/CFT requirements.
The compliance officer should be acquainted with the structure and functions of the office, and aware of the AML/CFT risks and vulnerabilities facing the sector, and of the methods and patterns of these threats, and should understand the legal obligations of the profession under the relevant legislation and implementing regulations.

2. Establishment of policies, procedures and internal controls to ensure compliance:

The auditor, as a DNFBP, shall develop and implement written policies, programmes and controls to ensure compliance with AML/CFT requirements. Such controls must be:
- in a written form and made available to the concerned entities.
- updated to keep pace with the latest applicable legislations and non-compliance cases reported, and

[16]. Of course, the Compliance Officer's contact with the auditor (chartered accountant, natural person) is possible only when there is dissociation between the two persons, i.e. the auditor (chartered accountant, natural person) chooses another person who performs the function of compliance officer in his office.

outcomes of the independent review and testing.
- approved by the senior management.
Generally, policies, procedures, and controls include all the obligations of the auditors and cases in which a particular procedure or measure is to be taken; in addition to the information that must be disclosed, documented, or taken into account; the measures taken and implemented to ensure compliance, the compliance timeframe, disclosure or reporting obligations and relevant methods.

3- Development of an ongoing training programme:

The auditor must develop an appropriate training programme for officers and employees, to be fully aware of their obligations by virtue of the AML/CFT Law and its Implementing Regulations, and of the responsibilities that may be incurred in case of involvement in ML and TF or non-compliance with such obligations, and of the threats, patterns and trends of ML and TF, and of how to detect suspicious transactions and take relevant actions.
The training programme should also ensure that the auditor, officers and employees are well acquainted with the procedures, controls and policies adopted by the office to manage and mitigate ML and TF, in addition to the role of the compliance officer and the importance of applying CDD measures and ongoing monitoring.
The auditor shall decide on the best training method, taking into account the size of the office. Several methods can be adopted such as, face-to-face training, e-learning, self-learning, or a combination of more than one method. The auditor, however, should document the training programme, for example by keeping record of the training attendance. It would be advisable if the training programmes are supported by a test (simplified test) to ensure staff's understanding of the relevant content.
Moreover, the programme shall take into account the different needs of officers and employees, their expertise, qualifications, capacities, tasks, the level of supervision they are subject to (the extent of their independence while performing their functions), and the size of business and the ML/TF risks.
The auditor shall update the training programme to ensure its compliance with the amended applicable legislations and relevant implementing regulations, as well as the applicable international standards and the emerging typologies of ML.

4- Adequate screening procedures to ensure high standards of integrity when appointing employees

The auditor shall develop adequate screening procedures to ensure high standards of efficiency and integrity when appointing or employing officers and employees, as stipulated in the MOCI AML/CFT Rules. Enhanced screening procedures must be adopted in particular for individuals entrusted with a prominent role or position at the office of the auditor. In order to comply with this requirement, the auditor should, before appointing officers or employees, obtain information and references about the individual, his employment background and qualifications, and confirm whether any criminal convictions, or disciplinary sanctions are taken against such individual.

5- Independent audit and review function to test AML/CFT programme:

The auditor should carry out periodic assessment to ensure the effectiveness of the components of the AML/CFT programme: policies and procedures, ongoing training programme and risk assessment. This review aims at evaluating and documenting deficiencies and shortcomings of the AML/CFT programme for future remedial actions.
The review can be conducted by an independent and competent internal or external auditor, qualified

to conduct the assessment. If the auditor is internal, he shall be sufficiently independent from the sections in charge of the office's operations, and not directly involved in the implementation of the activities related to the compliance programme, and have a direct line of communication to the auditor (the natural person), the Board or the Chief Executive.
The methods carried out to test the effectiveness of the AML/CFT programme varies depending on the scale of activity of the auditor's office or company, complexity of operations conducted, and nature of customers. The review must be conducted at least once every two (2) years, and reported to the AML/CFT Section by 31st of July 2021, and every two years thereafter.

Obligation II: Risk identification and assessment for mitigation and management

The auditor shall identify, understand, assess, and mitigate ML and TF risks. Since ML and TF risks are not the same in every case, a risk identification and assessment-based approach should be adopted in order to focus on high-risks (specifically CDD measures) in order to ensure effectiveness.
Types of the risks that should be taken into consideration:
the auditor shall, when identifying risks within his office, consider the risks identified in the National Risk Assessment, in addition to the following factors:
Risk factors related to customers, beneficial owners of customers, and the beneficiaries of customers' transactions. For example, the risks related to a customer are initially higher if the customer is a Politically Exposed Person (PEPs), or resident in a high-risk country or was not subject to the identity verification process (i.e. non-face to face transactions). However, the risks may be lower if the customer is a company listed on the stock exchange and subject to disclosure requirements under the Law or the financial market rules that ensure adequate transparency of beneficial ownership,

or if the customer is an administrative authority or public institution, or resident in low-risk countries.

A customer's nature of business may be a significant risk indicator. Customers whose businesses are related to arms sales, tobacco products, precious metals, jewelries and antiquities, and the protected creatures or products such as ivory may be higher risk. DNFBPs are also higher risk, as are any businesses that involve a high volume of cash transactions.

Further clarification shall be made in this regard in relation to **Politically Exposed Persons (PEPs).** PEPs are individuals who are or have been entrusted with prominent public functions by the State or a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, parliament members, important political party officials, members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organisations. This definition does not cover middle ranking or more junior individuals in the foregoing categories.

Family members of a PEP shall include the spouse and any natural person relative by blood, or marriage up to the second degree[17]. Close associates of a PEP 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.

PEPs represent increased ML/TF risks given their prominent public functions in the State, foreign country or international organization, they might be exposed to, involved in, or misuse their power and influence for the personal gain, have access to, or misappropriate public funds. Such PEPs may often use their families or close associates to conceal funds or assets that have been misappropriated as a result of abuse of their official position, which increases their ML/TF risks.

Due to high risks that the PEPs represent, the auditor shall:

1. Establish appropriate risk management policies and procedures to determine whether the customer or the beneficial owner is a PEP, a family member or a close associate.
2. Conduct additional CDD measures as follows:

2.1 Obtain senior management approval before establishing or continuing a business relationship for existing customers;

2.2 Take reasonable measures to establish the source of wealth and funds of the customers and beneficial owners of PEPs, their family members or close associates.

2.3 Conduct enhanced CDD measures and ongoing monitoring on business relationships with PEPs, to ensure the continued implementation of CDD measures, risk assessment and appropriate supervision.

Risks factors associated with jurisdictions and geographical areas initially, these risks are likely

[17]. This definition includes Father/ Mother, Husband/Wife, Father-in-Law/ Mother-in Law, Son/Daughter, Stepson/Stepdaughter, Grandfather/Grandmother, Brother/Sister, Brother-in Law/ Sister –in- Law, Grandson/Granddaughter.

to be higher if the transaction is related to a jurisdiction identified by credible and reliable source documents (for example: FATF Mutual Evaluation Reports, available at http://www.fatfgafi.org/publications/mutualevaluations/?hf=10&b=0&s=desc(fatf_releasedate)) as having ineffective AML/CFT regimes or high level of corruption and other criminal activities . On the other hand, the risks may be lower if the transaction is related to jurisdictions which have effective AML/CFT regime, or identified by credible and reliable sources as jurisdictions with low propensity for corruption and other criminal activities, or identified by reputable bodies and organizations in the mutual evaluation process and published relevant reports as compliant and effectively implementing FATF recommendations.

* Auditors should be aware, however, that financial crimes take place even in lower-risk jurisdictions, and that customers can be very high risk even if they are residents (or nationals) of a country with a low crime rate and a strong AML/CFT regime.

Risk factors associated with products and services provided by the auditor: certain products and services that auditors may provide are more vulnerable to abuse by illicit actors. In particular, if the auditor deals in cash (accepting cash as payment, or handling cash on behalf of a customer), the risks are higher than if the auditor is conducting transactions through a financial institution. Auditors should have explicit policies when dealing in cash.

Other products that are higher risks are those that ensure the customer's confidentiality and anonymity, whether in regards to the auditor or to financial institutions or other DNFBPs, products that do not

require the physical presence of the parties, products that involve anonymous or loosely-related third parties, and new products and new business practices, especially those based on new technologies.

When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels risk, the auditor should take into account risk variables relating to those risk categories. These variables, either singly or in combination, may increase or decrease the potential risk posed, thus impacting the appropriate level of CDD measures. The variables include, but not limited to :

- The purpose of an account or relationship.
- The level of assets to be deposited by a customer or the size of transactions undertaken.
- The regularity or duration of the business relationship.

Examples of variables that may increase risks:

a) Unexplained urgency of assistance required from the auditor.

b) Unusual sophistication of client, including complexity of structure or control environment.

c) Unusual sophistication of transaction/scheme.

d) The irregularity or duration of the client relationship. One-off engagements involving limited client contact throughout the relationship may present higher risk.

Examples of variables that may decrease risks:

a) Involvement of adequately regulated financial institutions or other DNFBP professionals.

b) Role or oversight of a regulator / supervisor or multiple regulators/supervisors.

c) The regularity or duration of the client relationship. Long-standing relationships involving frequent client contact and easy flow of information throughout the relationship may present less risk.

d) Private companies that are transparent and well-known in the public domain.

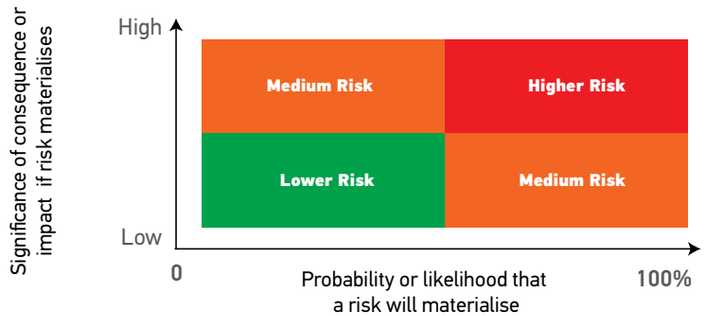
The risk-based approach shall not be applied only at the absolute discretion of the auditor and does not exempt the auditor from their obligations.

The auditor should rather be able to demonstrate the basis and means adopted to identify the risks subject to the National Risk Assessment and other relevant sources, as well as the means and timelines of the assessment of business risks. The auditor should also be able to prove that the low risk approach is based on an appropriate methodology where the CDD measures are proportionate to the risks identified.

The auditor shall carry out the following:

- Document the risk assessment processes.
- Update risk assessment processes.
- Provide appropriate mechanisms to make risk assessment information available to AML/CFT Section.

Example of a Risk Analysis Matrix [18]



[18]. Reference: FATF National Money Laundering and Terrorist Financing Risk Assessment, February 2013, page 27.

Obligation III: Applying Customer Due Diligence measures: identifying customers and beneficial owners:

1. The scope of applying CDD measures by auditors (covered activities):

The auditor practicing his profession, whether as sole practitioner (natural person), or under a joint liability company or branch of companies and non-Qatari accounting offices, when preparing for, or carrying out, transactions for his customers concerning the following activities :

a) Purchase or sale of real estate.

b) Management of the customer's funds, securities or other assets.

c) Management of bank accounts, saving accounts or securities accounts.

d) Organizing contributions for the establishment, operation or management of companies or other entities.

e) Establishment, operation or management of legal persons or legal arrangements, and sale or purchase of business entities.

The auditors are prohibited from keeping anonymous accounts or accounts in obviously Fictitious names.

2. The auditor should conduct CDD when :

- Establishing business relationships.
- Carrying out occasional transactions with a value equal to or exceeding fifty thousand Qatari Riyals (QR 50,000), whether as a one-off transaction or in several operations that appear to be linked.
- There is a suspicion of ML/TF, regardless of the amount of transaction.
- Having doubts about the veracity or adequacy of previously obtained customer identification data.

3. Can CDD measures be delayed?

The auditor must apply CDD measures when on-boarding a new customer, as it is not allowed to establish any business or transaction before completing CDD measures.

In some exceptional circumstances, CDD measures may be conducted after the establishment of the

business relationship, provided that:
- This is essential for not interrupting the normal conduct of business.
- The ML/TF risks are minimal.
- Measures are adopted to effectively manage risks related to the customer's possible benefit of the business relationship before verifying his identity, such as limiting the number, type and/or amount of the transactions that can be performed; monitoring large or complex transactions being carried out outside of expected norms for that type of relationship.
- CDD measures are completed as soon as possible after the initial contact with the customer.

If the auditor conduct CDD measures after the establishment of the business relationship, he must document each instance and be prepared to demonstrate AML/CFT Section that delayed CDD was appropriate and justified in that context.

4.The content of the customer due diligence (CDD)

The auditor should identify and verify the identity of the customer using reliable, independent source documents, data or information, and shall at minimum obtain the following information:

a) For customers that are natural persons: obtaining the complete name of the person as registered in the official documents (full identity and photo), residence address or domestic address, date and place of birth, and nationality.

For example: name, date of birth, and nationality of the customer can be verified with a valid passport or identification card with a clear photo. The customer's place of residence can be verified with a leasing contract, Kahrama bill or a letter from the employer.

b) For customers that are legal persons or legal arrangements: obtaining name, legal form, proof of incorporation, powers and resolutions that regulate the legal person or arrangement, a list of directors; and, the names of the relevant persons holding a senior management position in the legal person or arrangement (such as senior managing directors or trustee of a trust), the address of the registered office and, if different, a principal place of business,

c) For customers acting on behalf of another person: the auditor shall identify that the customer is authorized to act on behalf of such person and must verify his identity using reliable, independent source documents, data or information.

For customers that are legal persons or legal arrangements: the auditor shall understand the customer's ownership and control structure, and verify the identity of the beneficial owners.

The beneficial owner(s) of customers that are legal persons shall be identified 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. In case no beneficial owner is identified, or there is a doubt as whether the natural person with controlling ownership interest (s) is the beneficial owner under the previous item (1) or where no natural person exerts control through ownership interests, the auditor 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 supervision and control instruments.
3. In case no natural person is identified under (1) and (2) above, the auditor shall identify and verify the identity of the relevant natural person who holds the position of senior managing official in the legal person.

In cases where the auditor is unable to identify at least one natural person who meets the above requirements, he shall not accept or establish a business relationship with the customer, or perform a transaction or continue the relationship, and shall terminate such relationship for existing customers and file a suspicious transactions report with the Unit.

Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements, which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

For customers that are trusts, the auditor must take reasonable measures to identify and verify the identity of the beneficial owners 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 auditor shall identify the natural persons in equivalent or similar positions; and shall 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.

For all customers, the auditor shall understand the nature of the customer's business or activity pattern, understand the purpose and intended nature of the business relationship, and obtain the relevant necessary information, where applicable.

5. Can auditors rely on third parties to conduct CDD?

Auditors may rely on third parties such as financial institutions and DNFBPs to conduct CDD measures to identify the customer, the beneficial owner and understand the nature of the business. However , they remain the ultimate responsible for the proper conduct of CDD measures.

Auditors, when relying on third-party to perform the CDD measures as set out in the AML/CFT Law and it's implementing regulation, shall:

1. immediately obtain from the third-party necessary information in relation to the CDD measures and identification of the Customer.
2. Ensure that the third party will provide without delay and upon request a copy of every document relating to the customer and other documents in relation to such measures that auditors would need if it were conducting CDD itself for the customer.
3. Verify that the third party is regulated and supervised and complies with the CDD measures requirements and maintains the records in conformity with this Law and the Implementing Regulations.
4. Auditors must have regard to any relevant findings published by international and regional organizations and foreign jurisdictions, as well as available information on the level of risks related to ML and TF in jurisdictions where the third party operates or is located, before deciding to rely on said third party.
5. Ensure that it has received from the third party all information about the customer obtained from the CDD conducted by the third party introducer for the customer that it would need if it had conducted the CDD itself.

6. What should Auditors do when they cannot complete CDD because the client refuses to provide the information or when they discover that the customers' data are fictitious or incomplete?

1- Auditors should not establish or continue the business relationship with the customer or carry out the transaction for the customer.

2- Auditors should strongly consider filing an STR with the QFIU in relation to the customer, especially if the customer refuses to provide information, backs out of the process halfway through, or provides fictitious information.

7. Applying CDD measures commensurate with ML risks

The auditor shall apply CDD measures on a risk-based analysis according to the following two levels:

ML high risks → Implementing Enhanced Due Diligence (EDD)

Where the ML/TF risks are higher, the auditor shall perform enhanced due diligence measures commensurate with the risks identified, and shall increase the intensity of monitoring the business relationship to identify unusual or suspicious activities or transactions.

1. When is enhanced CDD required?

1. For business relationships and transactions with customers from certain countries:

• Countries identified by NAMLC as high-risk countries; and circulars about the vulnerabilities of their AML/CFT regimes are issued and published on NAMLC's website.

• Countries subject to a FATF enhanced due diligence requirement. Information about these countries will be published on NAMLC's website[19].

2. When ML/TF risks are high, especially in the following cases:

• Complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

• Purchase and sale transactions or transactions involving the power of attorney through non-resident customers in the State.

3. For other cases that are identified by NAMLC and the AML/CFT Section as high ML/TF risks for auditors.

II. Enhanced CDD to be conducted by Auditors:

The goal of Enhanced CDD is to learn more about the customer or transaction in order to minimize the chance that the customer or transaction is involved in ML/TF. Therefore, EDD should be tailored to fit the risk of the specific customer or transaction. Auditors should generally carry out the following enhanced measures, but may add others as appropriate:

1- Increase the frequency and intensity of the business relationship monitoring;

2- Obtain additional information about the customer including profession, volume of assets and information available through public databases and open sources;

3- Update on an ongoing basis the identification data of the customer and the beneficial owner by undertaken reviews of existing records particularly for high-risk categories of customers;

4- Obtain additional information on the purpose and intended nature of the business relationship;

5- Obtain additional information on the customer's source of wealth and funds;

6- Obtain information on the purpose of the intended transactions or the conducted transactions;

7- Obtain senior management approval before establishing or continuing a business relationship;

8- Take enhanced measures to monitor the business relationship by furthering the intensity and degree of supervision, and identifying patterns of transactions that require additional scrutiny and review;

9- Make the first payment through an account in the customer's name in a bank that is subject to similar CDD measures.

ML Low risks → Implementing Simplified CDD

The auditor may conduct reduced or simplified CDD measures for customers who poses lower level of risk.

I. When can auditors conduct simplified CDD?

Auditors may conduct simplified CDD when all the following conditions are met:

1- If the risk factors of the customer or transaction identified in the National Risk Assessment are low;

[19]. See Circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers about High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring , attached to this guidance.

2- If the risk factors of the customer or transaction identified in the self- assessment are low.
3- There is no suspicion of ML/TF.
4- There are no higher-risk factors, such as a link to a higher-risk jurisdiction, present.
Auditors may also conduct simplified CDD if the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company.

II. What are the simplified CDD measures that auditors can conduct?

Simplified CDD can consist of taking one or all of the following actions:
1- Verifying the identity of the customer and beneficial owner after the establishment of the business relationship.
2- Reducing the frequency of the customer's identification updates.
3- Reducing the intensity of ongoing monitoring and scrutiny of transactions based on a reasonable threshold
4- Limiting the collection of information, or the conduct of specific measures, to determine the purpose and intended nature of the business relationship, and inferring instead the purpose and nature from the type of transactions carried out or from the business relationship established.
In any case where an auditor carries out simplified CDD, he must document the risk assessment and be prepared to demonstrate to the AML/CFT section at MOCI that the risk was appropriate and justified in this context.

8. Ongoing monitoring: extended CDD measures.

The auditor shall conduct ongoing monitoring for each customer; and shall pay special attention to all complex, unusual, large transactions, or unusual patterns of transactions, that have no apparent economic or clear legal purpose, like transactions exceeding the designated threshold or transactions not in line with the customer's type of business or occupation. The Auditor shall also examine, to the extent possible, the background and purpose of the mentioned transactions, and make a record of his findings.

The ongoing monitoring requires taking the following types of measures:
- Monitor the transactions conducted under the business relationship between the auditor and the customer to ensure that the transactions are consistent with his knowledge of the customer, his business and risk profile, and, where necessary, the source of his wealth and income.
- Review the records held by the auditor to ensure that the documents, data and information collected using CDD and ongoing monitoring for the customer are kept up-to-date and relevant

Obligation IV : Reporting Suspicious Transactions to QFIU

1. General Principle:

The auditor, shall report to the Qatar Financial Information Unit (QFIU) suspicious transactions in the form approved by the QFIU, and following the instructions and guidance issued by the QFIU, when suspecting or having reasonable grounds to suspect that funds are the proceeds of a predicate offence, or are related or linked to terrorism financing, irrespective of the following:
- The amount of the transaction.
- The transaction was not conducted.
- The nature of the predicate offence.
- The attempted money laundering or terrorism financing has failed.

Auditors must notify the Anti- Money Laundering and Terrorism Financing section at MOCI that an STR has been filed with the QFIU.
The obligation of reporting Suspicious Transactions to QFIU, constitutes a special dispensation of auditor's confidentiality obligation which imposes to this professional to maintain confidentiality of information he may receive in the practice of his profession.

2. Reporting Confidentiality and Tipping-off

The auditor should be prohibited from disclosing to any unauthorized person the fact that a suspicious transaction report or related information is being filed with the QFIU. Failure to comply with this requirement shall result in imposing the penalities stipulated in Article (84) of the AML/CFT Law[20].

The auditor, the natural person, the director of the company in public practice and all the employees shall be prohibited from disclosing to the person subject of the STR or to third parties whether or not a suspicious transaction report, or any other relevant information, has been filed with the QFIU.

This prohibition shall be considered justified and reasonable, since customer's knowledge or suspicion that he is, or may be, the subject of an STR may compromise the actions, procedures, and investigations carried out by the competent authorities in the State for the prevention or detection of ML crimes, the arrest or prosecution of offenders, or the recovery of the proceeds of crime.

In all cases, the auditor must be mindful when dealing or communicating with the customer after reporting a suspicious transaction to QFIU; inquiries may be made as long as they fall within the conduct of business relationship and within the regular CDD that must be applied by the auditor. For example, the auditor may ask the customer about a tax declaration not attached with a requested invoice.

Tipping off shall not prevent the auditor from sharing information with foreign branches and majority-owned associates[21] to the extent that this is necessary to maintain a unified AML/CFT program. Where the auditor seeks to dissuade the customer from engaging in illegal activity, this does not amount to tipping-off.

If the auditor reasonably believes that performing the CDD process will tip-off the customer, he may choose not to pursue that process, and should file an STR with the QFIU. The auditor shall take all reasonable measures to ensure that information relating to suspicious transaction reports are kept confidential.

3. Identification of the suspicious transactions: practical instructions to auditors.

A transaction that is unusual or inconsistent with the customer's known legitimate business and risk profile does not make it by itself suspicious. The basic principles are honesty, integrity, and good faith unless proven otherwise.

The auditor must consider the following circumstances when assessing whether an unusual or inconsistent transaction is suspicious:

- When the transaction has no apparent economic or lawful purpose, such as when the customer accepts to sell at a lower cost or to conduct an activity without any expected income or profit.
- When the transaction has no reasonable explanation;
- When the size or pattern of the transaction is inconsistent with any earlier size or pattern of transactions for the same customers;
- When the customer has failed to give an adequate explanation for the transaction or to fully provide information about it;
- When the transaction involves the use of a newly established business relationship or is a one-off transaction;
- When the transaction involves the use of offshore accounts, companies or structures that are not supported by the customer's economic needs;
- When the transaction involves unnecessary routing of funds through third parties.

Examples cited by the Financial Working Group to assist auditors in identifying unusual or suspicious transactions:

The following examples include, but not limited to, the indicators that may trigger the auditor to suspect that the customer is involved in a ML crime.

- Customer's disinterest in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business, persisting in pursuing his activities.
- High volume of foreign transfers from/to the customer's accounts or the increase of the revenues and cash amounts he obtains in a sudden manner, that is not commensurate with his usual incomes, without any justification.
- Customer's receipt of cash money or high value cheques, which do not suit the volume of his work or the nature of his activity, particularly if they come from certain people who are not clearly or justifiably connected to the customer.
- Unjustified amounts or deposits in the customer's accounts whose origin or cause is difficult to identify.
- Disproportionate amounts, frequency and nature of transactions carried out by the customer that are not commensurate with the nature of his business, profession or known and declared activity, particularly if these transactions are carried out with suspicious countries that are not connected to his apparent business domain.
- Repeated large-amount cash transactions including foreign exchange transactions or cross-border fund movement when such types of transactions are not commensurate with the usual commercial activity of the customer[23].

4. Scope of STRs reporting obligations

The obligation of the auditor to report suspicious transactions is not absolute, but has some exceptions. In fact, the auditor is exempted from such obligation when acting in the course of ascertaining the legal position of his customer. This exemption covers financial, economic and taxation consultancy services, unless the consultancy services provided by the auditor are intended to assist the customer in engaging in ML activities, or the auditor is aware that the customer requested such consultancy services for ML purposes.

5. Shall the auditor stop dealing with the customer once the suspicious transaction is reported to the QFIU?

The AML/CFT Law or its Implementing Regulations do not require the auditor to terminate the business relationship with the customer upon reporting a suspicious transaction to the QFIU. However,

[20]. Article (84) of the AML/CFT. Law stipulates that: « Any person who commits the offence of disclosing information that may reveal that a suspicious transaction report has been submitted to the Unit, or has not been submitted, shall be sentenced to imprisonment for a term not exceeding three (3) years and a fine not more than (QR 500.000) five hundred thousand Qatari Riyals, or one of these two penalties ».

[21]. Article (22) of the AML/CFT Law.

[23]. Source: MENAFATF, DNFBPs in relation to AML/CFT, November 2008, P. 13.

the auditor shall, in performing his duties and functions, be straightforward and honest, and assist in respecting the Law. As such, by respecting the professional and ethical norms, the auditor is mostly supposed to terminate the business relationship with the customer, particularly since filing a suspicious transaction report with the QFIU is an indicator of the loss of confidence between the auditor and the customer[24]. However, it is important to highlight the following:

1. The auditor must ensure that he does not tip-off the customer that an STR was filed. Meanwhile, terminating the business relationship simultaneously with filing the suspicious report, may raise the doubts of the customer, particularly if the investigations are being conducted to consider the facts of the STR.
2. The STR does not constitute grounds for the termination of the auditor's job as per the Commercial Companies Law.

To conclude, the auditor shall, based on his professional ethics, decide whether to maintain the business relationship with the customer, when filing an STR. The auditor shall, when deciding to terminate the business relationship with the customer, take the necessary precautions to not inadvertently tip-off the customer that he is subject to a suspicious report or ongoing financial investigations, in order to ensure the efficiency of such investigations.

[24]. Article (24) of Law No. (8) of 2020 on the Regulation of the Auditing Profession stipulates that «The Auditor shall comply with the code of ethics, conduct, and traditions of the Profession, and with accounting and auditing standards approved in the State.» Article (26) of the same Law also prohibits the following: « An Auditor may not engage in the following activities:
1- Trading.
2- Exercising the Profession or advertising the same in any way that is contrary to laws and regulations in effect, or against generally accepted rules of professional conduct and code of ethics...

Obligation V: Record Keeping:

Consistent with his respective obligations, pursuant to the AML/CFT Law, the auditor shall keep records, documents and evidences supporting his compliance with such obligations.
In practice, the auditor shall keep records as evidence of his compliance with the AML/CFT Law and its Implementing Regulations, specifically adopting and implementing the risk-based approach to mitigate risks, conduct CDD measures and ongoing monitoring.
Such records, include but not limited to:

- Documents and data obtained through CDD measures.
- Account files.
- Business correspondence with the customer.
- Results of the STRs analysis undertaken.

Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. As such, record-keeping enables detecting money launderers and terrorism financiers and provides a material evidence that can be traced by competent authorities in order to prosecute and track illicit actors.
The auditor should be required to maintain all necessary records on transactions, both domestic and international, for at least (10) ten years following completion of the transaction. The auditor should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least (10) ten years following the termination of the business relationship or after the date of the occasional transaction.

Auditors must retain records beyond the end of the ten-year period mentioned above:
1-If they have filed with the QFIU a suspicious transaction report relating to the applicant for business or customer.
2-If they know that the applicant for business or customer is under investigation by law enforcement or judicial authorities for issues related to money laundering or terrorism financing.
Auditors should ensure that all CDD records, data and documents on transactions and operations are available without delay to the competent authorities upon request.
Auditors should also establish proper systems to ensure prompt response to the requests of the competent authorities.

Chapter four

Sanctions and penalities imposed on auditors for breach of AML/CFT obligations

In the event of a breach to the AML/CFT obligations, auditors will be subject to the sanctions and penalties provided for in the law regulating the combating of money laundering and terrorism financing.

Section 1: Penalities

Article (82) of Law No. (20) on Combating Money Laundering and Terrorism Financing stipulates that directors, board members, owners, authorized representatives or any other employees of financial institutions and DNFBPs shall be sentenced to imprisonment for a term not exceeding two (2) years or a fine not less than (QR 5.000.000) five million Qatari Riyals and not more than (QR 10.000.000) ten million Qatari Riyals, or one of these two penalties, when contravening, whether wilfully or as the result of gross negligence, the provisions stipulated in the following Articles of the same law:

(9) : keeping anonymous accounts or accounts in obviously fictitious names.
(10): failure to undertake Customer Due Diligence measures in cases determined by the Law.
(11): failure to undertake measures to identify customers, whether permanent or occasional / initiate or maintain a business relationship or carry out any transaction when they are unable to comply with these measures or when they discover that the customers' data obtained is obviously fictitious or inadequate.
(13): failure to apply EDD measures in cases determined by the Law.
(14): failure to keep data and information related to the CDD processes up-to-date and relevant on an ongoing basis.
(15): failure to perform CDD measures proportionate to the level of risks involving the customers, their businesses and their transactions.
(16): failure to put in place appropriate risk management systems to determine whether a customer or beneficial owner of a customer is a Politically Exposed Person (PEP), a family member of a PEP, or a close associate of a PEP/ Failure to take additional relevant measure if the above is determined.
(20): failure to maintain records / failure to make all information available to authorities upon request.
(21): failure to promptly report to the QFIU any information concerning any transaction or operation, including attempted transactions and operations, regardless of the value thereof, when there is a suspicion or reasonable grounds to suspect that such transactions and operations are associated with, or involve proceeds of a predicate offence or may be used in terrorism financing.

Section two: Financial and Administrative sanctions

Article (44) of Law No. (20) on Combating Money Laundering and Terrorism Financing stipulates that without prejudice to a more severe penalty stipulated in any other law, and in case it is evidenced that any DNFBP, or any of the directors, board members, executives or management thereof, has violated the provisions of this Law, its Implementing Regulations and any decisions or guidance related to AML/CTF, The AML/CFT section may impose one or more. of the following measures:

1. Sending written warnings.
2. Ordering regular reports on the measures taken.
3. Ordering compliance with specific instructions.
4. Imposing a financial penalty of no less than (QR 25.000) twenty-five thousand Qatari Riyals, and no more than (QR 100.000) one hundred thousand Qatari Riyals per violation per day, on the DNFBP after being notified.
5. Imposing a financial penalty of no more than (QR 100.000.000) one hundred million Qatari Riyals on the violating DNFBP.
6. Imposing a financial penalty of no more than (QR1.000.000) one million Qatari Riyals on any of the directors, board members, executives or management.
7. Restricting the powers of the directors, board members, executives, or management, in addition to appointing a special administrative supervisor, or subjecting the DNFBP to direct control.
8. Prohibiting the perpetrator from working in the relevant sectors, either temporarily or permanently.
9. Suspending, dismissing or replacing directors, board members, executives, management, trustees of trusts, or trustees, either temporarily or permanently.
10. Imposing suspension of the license, restricting any other type of permit, and prohibiting the continuation of work, the profession or the activity, or barring the name from the relevant registry.
11. Revoking and withdrawing licenses and registrations.

The decisions referred to may be appealed in accordance with the controls, procedures and timelines Set forth in article 64 and 65 of the implementing regulations of low No.(20) of 2019.

Legal References

1- Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing.
2- Law No. (1) of 2020 on the Unified Economic Register.
3- Council of Ministers' Decision No. [41] of 2019 Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing
4- Council of Ministers' Decision No. [12] of 2020 Promulgating the Implementing Regulations of Law No. (1) of 2020 on the Unified Economic Register.
5- Decision of the Minister of Commerce and Industry No. (95) of 2019 on establishing the Anti-Money Laundering and Terrorism Financing Section under the Companies Affairs Department.
6- Decision of the Minister of Commerce and Industry No. (48) of 2020 promulgating AML/CFT Rules for legal Auditors, Dealers in Precious Metals or Precious Stones and Trusts and Company Service Providers.

Useful Links

1- The Financial Action Task Force
https://www.fatf-gafi.org/

2. Middle East and North Africa Financial Action Task Force on Combating money laundering and financing of terrorism (MENAFATF)
http://www.menafatf.org/

3- National Anti-Money Laundering and Terrorism Financing Committee
http://www.namlc.gov.qa/

4- Qatar Financial Information Unit
http://www.qfiu.gov.qa/?page_id=564&lang=ar

5- Ministry of Commerce and Industry :Anti-Money Laundering and Terrorism Financing Section under Companies Affairs Department.

https: https://www.moci.gov.qa/مكافحة-غسل-الاموال-و-تمويل-ارهاب/
mail address: control.aml@moci.gov.qa
Address: 2 floor Ministry of Commerce and Industry Lusail City, Qatar

وزارة التجارة والصناعة

Ministry of Commerce and Industry

Companies Affairs Department إدارة شؤون الشركات

Circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers about High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring

Gentlemen / Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers,

Pursuant to the requirements of Article (13) of Law No. (20) of 2019 issuing the Anti-Money Laundering and Terrorist Financing Law,

And Articles (22), (23) and (60) of the executive regulations of the Anti-Money Laundering and Terrorist Financing Law issued by Cabinet Resolution No. (41) of 2019,

And Article (2) of the Decision of Minister of Commerce and Industry No. (95) of 2019 establishing the Anti-Money Laundering and Terrorist Financing Section in the Companies Affairs Department,

The Anti-Money Laundering and Terrorist Financing Division issues the following circular:

The Financial Action Task Force (FATF) identifies, three times per year and in a public statement, jurisdictions whose regimes have strategic deficiencies in terms of combating money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction, in which it calls upon countries to adopt certain measures against them. In accordance with its latest meeting in February 2020, FATF issued a statement regarding the list of those jurisdictions and the measures and procedures that must be adopted.

In light of such event, the National Anti-Money Laundering and Terrorism Financing Committee (NAMLC) published on its website (www.namlc.gov.qa) the link to FATF's statement and issued letter No. 1417/2020 dated 13/04/2020 in which it called upon supervisory authorities to require their supervised entities to adopt due diligence measures when dealing with the jurisdictions concerned, implement procedures and instructions relevant to combating money laundering and terrorism financing and related to dealing with high-risk jurisdictions and other jurisdictions under monitoring, based on FATF's requirements

وزارة التجارة والصناعة

Ministry of Commerce and Industry

Companies Affairs Department إدارة شؤون الشركات

indicated above and Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its Implementing Regulations.

Jurisdictions whose regimes have strategic deficiencies in combating money laundering and terrorism financing are distributed as follows:

a- **High-risk jurisdictions subject to a call for action by FATF:**

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction. For all countries identified as high-risk, the FATF calls on all members to apply enhanced due diligence (EDD), and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction risks emanating from the country. This list currently includes:

I. **Democratic People's Republic of Korea (DPRK):**

FATF reaffirms in its latest statement its call on its members to advise their financial institutions and designated non-financial businesses and professions (DNFBPs) to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. FATF further calls on its members to continue applying **EDD and counter-measures** and to implement **targeted financial sanctions** in accordance with applicable United Nations Security Council Resolutions.

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

1. **Implementing EDD** that is proportionate to the level of risk for business relationships and operations carried out with customers, including financial institutions and DNFBPs from DPRK[1], as follows[2]:
   - Examining, as much as possible and in a reasonable manner, the background and purpose of all complex or unusual operations and all unusual patterns of operations that have no apparent legal or economic purpose.
   - Increasing the level of monitoring for the business relationship to identify unusual or suspicious activities or operations.
   - Obtaining additional information on the nature of the expected business relationship.
   - Obtaining senior management approval to establish or continue the business relationship.
2. **Implementing counter-measures** for business relationships and operations carried out with customers, including financial institutions and DNFBPs from DPRK, as follows[3]:
   - Submitting immediate reports to the AML/CFT Section at the Companies Affairs Department at MOCI on business relationships and operations carried out with that jurisdiction or persons located in it.
3. **Implementing targeted financial sanctions** related to combating terrorism and terrorism financing and preventing proliferation of weapons of mass destruction against DPRK according to the provisions of Law No. (27) of 2019 on Combating Terrorism and Decision No. (1) of 2020 of the Public Prosecutor Regulating the Implementation Mechanisms of the Targeted Financial Sanctions related to Combatting the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction pursuant to the Law on Combating Money Laundering

[1] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (22) of its Implementing Regulations.
[2] Article (25) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.
[3] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (23) of its Implementing Regulations.

وزارة التجارة والصناعة
Ministry of Commerce and Industry
Companies Affairs Department إدارة شؤون الشركات

and Terrorism Financing and the Law on Combating Terrorism and the United Nations Security Council Resolutions, in addition to Decision No. (59) of 2020 of the Public Prosecutor issuing the Guidelines to the Effective Implementation of the Targeted Financial Sanctions Regime in the State of Qatar.

II. Iran:

FATF decided to **re-impose counter-measures against Iran** and called upon its members to apply them. This step followed Iran's failure to comply with implementing the action plan related to addressing deficiencies in countering money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in its regime within the period specified. The most significant deficiencies relate to Iran's failure to ratify the United Nations Convention against Transnational Organized Crime (Palermo Convention) and the Terrorist Financing Convention.

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

1. **Implementing EDD** that is proportionate to the level of risk for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran[4], as follows[5]:
   - Examining, as much as possible and in a reasonable manner, the background and purpose of all complex or unusual operations and all unusual patterns of operations that have no apparent legal or economic purpose.
   - Increasing the level of monitoring for the business relationship to identify unusual or suspicious activities or operations.
   - Obtaining additional information on the nature of the expected business relationship.

[4] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (22) of its Implementing Regulations.
[5] Article (25) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.

- Obtaining senior management approval to establish or continue the business relationship.

2. **Implementing counter-measures** for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran, as follows[6]:
   - Implementation of the following EDD for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran:
     - Obtaining additional information on the customer, including the profession, size of assets and information available through public databases and open sources, and updating customer and beneficial owner identification data regularly.
     - Obtaining additional information on the nature of the expected business relationship.
     - Obtaining information on the source of the customer's wealth or funds.
     - Obtaining information on the reasons for the expected operations or operations conducted.
     - Applying enhanced monitoring for the business relationship by increasing the extent and period of supervision and selecting patterns of operations that need additional scrutiny and review.
     - Making the first payment through an account in the customer's name in one of the banks subject to similar due diligence standards.
   - Submitting immediate reports to the AML/CFT Section at the Companies Affairs Department at MOCI on business relationships and operations carried out with that jurisdiction or persons located in it.

Auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must periodically view updates of the list of high-risk jurisdictions subject to a call for action by FATF via the following link:

[6] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (23) of its Implementing Regulations.

وزارة التجارة والصناعة
Ministry of Commerce and Industry
Companies Affairs Department إدارة شؤون الشركات

http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

b- Jurisdictions under increased monitoring:

Jurisdictions under increased monitoring are jurisdictions whose regimes have strategic deficiencies in countering money laundering, terrorist financing and financing of proliferation but that have highly complied with FATF's action plan. These jurisdictions are subject to monitoring by FATF until the fulfilment of the action plan within a specific timeframe. FATF does not call upon its members to apply EDD against these jurisdictions; on the other hand, **it urges them, upon analysis of risks related to such jurisdictions, to take into account information published on the link indicated below.**

The list of these jurisdictions under monitoring currently includes: **Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen and Zimbabwe.**

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

1. Periodically viewing updates of the list of jurisdictions under increased monitoring to take into account, upon analysis of risks, information published on the following link regarding business relationships and operations carried out with customers, including financial institutions and DNFBPs from such jurisdictions[7]:

http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html

[7] Article (24) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.

وزارة التجارة والصناعة

Ministry of Commerce and Industry

Companies Affairs Department

إدارة شؤون الشركات

Furthermore, in its latest meeting, FATF excluded the Republic of Trinidad and Tobago from the list of jurisdictions under increased monitoring due to its success in implementing the action plan related to addressing deficiencies in countering money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in its regime.

For view and implementation

Salem bin Salim Al Mannai

Director of the Companies Affairs Department