AML/CFT Compliance Guidance for Trust and Company Service Providers

2022

وزارة التجارة والصناعة
Ministry of Commerce and Industry

Table of contents

Introduction

1.1 General Framework of the Guidance :

Traditionally and historically, commercial companies, particularly those based on limited liability of partners and trusts represent the legal structures that allow for engagement in economic activities and realization of legitimate of legitimate investments. However, experience has proven that there may be deviation from the initial and legitimate goals of the commercial companies and trusts, thereby converting these legal structures to tools used by criminals to facilitate money laundering and other criminal activities such as corruption, tax evasion, theft, etc[1] .

The controls, policies and procedures, which are established by financial institutions to prevent and detect money laundering and terrorism financing, have contributed to the reluctance of criminals and money launderers to using traditional financial channels (the banking system) and resorting to the companies and trusts as innovative tools to disguise and conceal the criminal source of their funds. New types of commercial companies have, therefore, emerged which are not intended to engage in legal economic activities by a group of individuals (partners) wishing to place their contributions, efforts and funds within a joint venture, but aims to enable criminals and money launderers to disguise and conceal their proceeds of crime before it enters the traditional financial system. Some examples of such companies include:

1. **Shell companies –** incorporated company (legal entity) with no independent operations, significant assets, ongoing business activities, or employees . It may also be established with various forms of ownership structure and participation of partners from different countries.

2. **Front companies –** fully functioning company with the characteristics of a legitimate business, serving to disguise and obscure illicit activity. Front companies can be exploited in money laundering through the integration of criminal proceeds with the legitimate income obtained from the activities carried out by the above companies. Then theses funds can be deposited into the company's bank account and used by the beneficial owner or they may pay fictitious expenses in order to transfer the money to the true beneficial owner.

   The need has emerged for criminals and money launderers to seek out the services of professionals to benefit from their expertise, knowledge, professional status (particularly confidentiality privilege which is recognized to some legal professions) and good reputation, in setting up and implementing money laundering schemes through the misuse of trusts and company services. The professionals have varying degrees of involvement in helping with the setting up and implementation of money laundering schemes and the concealment of criminal proceeds: they may be engaged deliberately in these schemes or without their knowledge or intent. These concerns have led to the extension of AML/CFT regimes' scope to include, in addition to financial institutions, some professionals who can be exploited in the setting up and

1. FATF, the misuse of corporate vehicles including trust and company service providers, October 2006, p. 1-2.
2. A shell company is an incorporated company with no independent operations, significant assets, ongoing business activities, or employees, Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019, p9

implementation of money laundering schemes through the abuse of trusts and companies, such as accountants, lawyers and TCSPs. In 2003, the FATF Forty recommendations were amended to include Designated Non-Financial Businesses and Professions (DNFBPs) such as lawyers, accountants, notaries and TCSPs.

Such concerns have been amplified, especially under the considerable ease and flexibility with which companies and trusts can be created and dissolved in some countries or jurisdictions. Additionally, several reference studies issued by the relevant international organizations[3] highlighted that trust and company service providers, which participate in the creation and/ or management of legal entities, may be particularly vulnerable to misuse, exploitation, and even targeted recruitment by criminals and criminal groups involved in money laundering and terrorism financing. In fact, these entities may be created and registered specially in order to facilitate access to the financial institutions and financial services sector in general. In this case, Trust and company service providers (TCSPs) act as intermediaries or focal point that provide criminals and criminal groups with access to the financial system.

In other cases, TCSPs inadvertently assist criminals and criminal groups to achieve their goals of accessing the financial system and breaking the links between funds and criminal activity, when they do not implement the required customer due diligence (CDD) measures. This may be attributed to the lack of sufficient knowledge or experience related to the requirements of AML/CFT system, lack of knowledge of the company's business or of the structures of legal entities to be established and managed, and the absence of appropriate information systems that may allow the detection of ML/TF activities.

For theses reasons, FATF recommended that countries impose AML/CFT obligations on TCSPs, when theses professionals engage or execute transactions for a customer concerning the following activities described in Rec. 20:

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

The common denominator between the various activities mentioned above is that they are considered high-risk because they might be abused for ML/FT purposes. This feature justifies imposing to the TCSPs the obligation to comply with AML/CFT requirements when carrying out those activities.

Qatar's 2019 National Risk Assessment (NRA) stated that the State of Qatar [4] could be exploited either through illicit actors that seek to set up front or shell companies in Qatar — through TCSPs — or by illicit actors using shell or front companies to establish bank accounts or move funds through Qatari financial institutions. The report concludes that the residual risk of money laundering and

3. Money laundering using trust and company service providers, Financial action task force/ OECD/ Caribbean/ Financial action task force, October 2010, Money Laundering and terrorist Financing Vulnerabilities of legal professionals, FATF, JUNE 2013 , and Professional Money Laundering, FATF, July 2018.

terrorism financing associated with the TCSPs sector remains **medium-high.**

In 2020, the Ministry of Commerce and Industry conducted the ML/TF Sectoral Risk of its supervised Designated Non-Financial Businesses and Professions (DNFBPs), and it concludes that the ML/TF residual risk associated with TCSPs remains **medium-high,** reflecting the vulnerabilities related particularly to transparency including the identification of beneficial ownership.

1.2 Purpose of the Guidance:

The guidance is intended to highlight and review the TCSPs compliance with AML/CFT requirements under the Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, as amended by Decree Law N (19) of 2021, Decision of the Council of Ministers No. (41) of 2019 Promulgating the Implementing Regulations of the AML/CFT Law, as amended by Council of Minister's Decision N (14) of 2021, and Decision of the Minister of Commerce and Industry No. (48) of 2020 Promulgating the AML/CFT Compliance Rules for Auditors, Dealers in Precious Metals or Precious Stones, Trust and Company Service Providers (hereinafter referred to as AML/CFT Compliance Rules).

This guidance is intended to clarify and simplify the AML/CFT obligations imposed on TCSPs and assist them in understanding and complying with such obligations, including those related to the application of Risk Based Approach, implementation of CDD measures and suspicious transactions reporting.

The Anti-Money Laundering and Terrorism Financing Section established under the Companies Affairs Department at MOCI pursuant to the Decision No. (95) of 2019 [5] is responsible for the supervision of the compliance of TCSPs with AML/CFT requirements clarified in this guidance, as well as proposing financial and administrative sanctions against anyone who violates the provisions of the AML/CFT Law, its Implementing Regulations and any relevant decisions or instructions and notifying the QFIU of the procedures adopted in this regard.

It should be noted that given the differences that exist in the structure and organization of TCSPs from one institution to another as well as the size and nature of their services and activities, it is worth recalling that there are no uniform or identical procedures for the implementation of the AML/CFT Regime; in orher words, this guidance is limited to setting the broad outlines or general principles whereby each service provider may adopt the appropriate detailed and practical measures which ensure the implementation of the AML/CFT Regime, taking into consideration the particularities, size and nature of the activity being practiced. Meanwhile, this guidance does not substitute to the legal and regulatory texts, which must be reviewed since they are the official reference for specifying the requirements of AML/CFT Regime for all supervised entities.

1.3 Scope of the Guidance :

- **To whom shall this guidance Apply ?**

4. Qatar's 2019 National Risk Assessment.
5. Decision of the Minister of Commerce and Industry No. (95) of 2019 to establish an Anti-Money Laundering and Terrorism Financing Section under the Companies Affairs Department.

The Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing has classified TCSPs within the category of Designated Non-Financial Businesses and Professions, in line with the FATF Recommendations, and imposed a number of AML/CFT requirements on them, when arranging or executing transactions for a customer concerning the activities described in Article (1) of the above law.

Qatar's National Risk Assessment stated that the professions participating in the creation of legal persons and arrangements in the State of Qatar, namely Lawyers and account auditors, are considered the most vulnerable to the risks of exploitation in money laundering and terrorist financing operations. These professions and TCSPs in general can be abused as gatekeepers - either wittingly or unwittingly - for money laundering, terrorism financing, proliferation financing, or sanctions evasion.

Given the fact that lawyers and auditors are subject to compliance with the AML/CFT requirements, 5which are subsequently explained in the AML/CFT Guidance for Lawyers[6] and AML/CFT Compliance Guidance for Auditors (Chartered Accountants[7]), this guidance shall apply to TCSPs operating in the State of Qatar, whether as individual businesses or commercial companies, and to all their foreign and domestic branches and majority-owned subsidiaries.

It would be useful for auditors and lawyers to become acquainted with the provisions of this guidance, particularly those related to business risk assessment, when they conduct one of the activities of TCSPs[8].

- **What are the activities which are subject to AML/CFT requirements ?**

Trust and Company Service Providers are subject to AML/CFT requirements in accordance with Article (1) of the AML/CFT Law No. (20) of 2019, when they arrange or execute transactions for the customers, including the following activities:

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

Acting as, or arranging for another person to act as, a nominee shareholder for another person.
Article (1) of the AML/CFT Law has provided definition for some of the terms used in identifying the activities carried out by TCSPs as follows:

6. AML/CFT Guidance for Lawyers, Ministry of Justice.
7. AML/CFT Compliance Guidance for Auditors (Chartered Accountants) published on the website of the AML/CFT Section at the Ministry of Commerce and Industry (Supervised entities – Account Auditors).
8. Guidance for a risk based approach, Trust and company service providers, FATF, June 2019, p8, "The FATF definition of TCSP relates to providers of trust and company services that are not covered elsewhere by the FATAF recommendations , and therefore excludes financial institutions , lawyers, notaries , other independent legal professionals and accountants . Separate guidance has been issued for those sectors and they should therefore apply that guidance when providing service covered by R.22. However, all those professions/ entities engaged in TCSP activities should also refer to the TCSPs guidance, as it is more specifically tailored of TCSP services."

- **Express Trust:** A legal relationship that does not establish a legal personality, created by a written deed, whereby a person places funds under the control of a trustee for the benefit of one or more beneficiaries or for a defined purpose.
- **Legal arrangement:** Express trusts or any other similar arrangements.
- **Legal Person:** Any entity, other than a natural person, which is capable of conducting a permanent business relationship with a financial institution or of gaining ownership of assets. This includes companies, institutions, foundations, or any relevantly similar entity.

The MOCI Sectoral Risk Assessment has identified (3) three group activities associated with the provision of Trust and company services, in line with the FATF definition and based on the International Standard Industrial Classification of All Economic Activities (ISIC). The group activities are as follows:

- Business Administration Centre.
- Business Centre.
- Businessmen Administrative Centre.

Based on the above, this guidance shall apply to any natural or legal person, who is licensed to practice one of the activities related to the provision of Trust and company services specified by the Ministry of Commerce and Industry in the group mentioned in the preceding paragraph.

Money Laundering and Terrorism Financing Crimes

What is Money Laundering?

Money laundering is the process through which the source of illicit funds or those used for illicit purposes is disguised and made to appear as legitimate funds, which can be circulated in various public activities, in order to distance them from their illegal source. Money laundering is also known as the process of hiding the source of criminal proceeds to enable criminals and their associates to use them without raising attention from law enforcement agencies or financial institutions.

Money laundering includes all illicit funds resulting from a wide range of criminal activities (such as selling drugs & weapons, human trafficking, theft, and tax evasion, etc.). Laundering the proceeds of such different criminal activities is carried out through several stages and according to various methods.

1. Stages of money laundering:

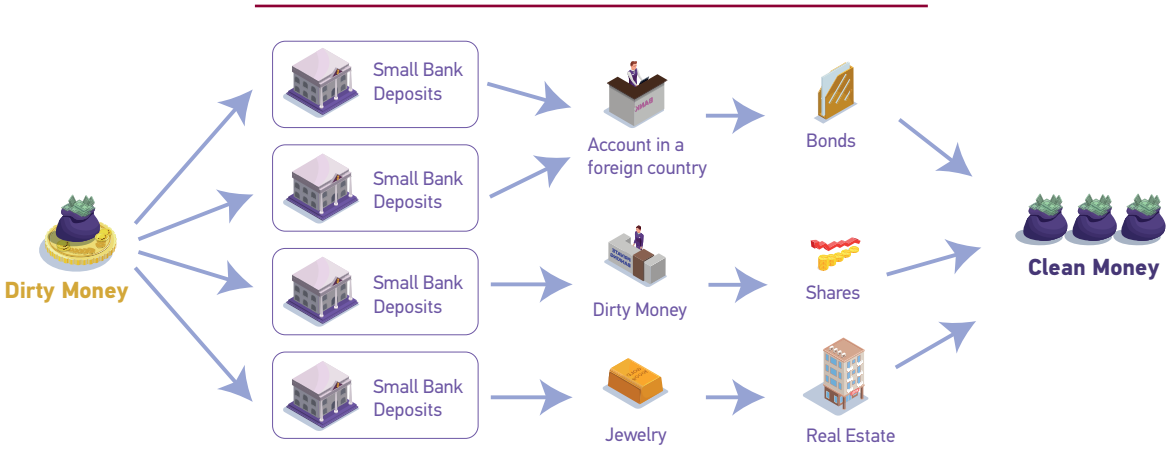
Money is usually laundered through the following three consecutive stages[9] :

9. It is worth noting that money laundering may include all the three stages. However, this is not a fundamental rule as two or more stages can be combined or skipped.

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. Proceeds of crime are also not cash proceeds in all cases; they may include the income, interest, revenue or any other product, whether or not it has been transferred in whole or in part into properties or other investment proceeds. Criminal proceeds can also take the form of cryptocurrencies, such as Bitcoins.

2. **Layering: Also referred to as "obscuring":** This second stage of money laundering 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 through conducting several complex financial transactions to make such illicit funds appear legitimate and that their source is difficult to trace. For instance, funds or securities can be transferred 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 bank secrecy, known as "financial havens", or by layering the transferred amount through fictitious goods or services.

3. **Integration / Extraction:** It is the final stage of money laundering, where 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 overpriced front companies, concluding successive sales and false loans, etc.



2. Frequent Methods of Money Laundering related to the Activities of Trust and Company Service Providers.

The FATF considers that professionals, practitioners and experts may largely contribute to the enhancement of the capacities of perpetrators by planning and conducting complex and advanced ML schemes to conceal, collect, move or use illicit sources of wealth. In certain ML methods

the contribution of DNFBPs (specifically legal and accounting professions and TCSPs) is critical in planning and implementing ML schemes which includes the following:

- **Establishing trusts:** trusts may be used to conceal or obscure the beneficial owners of funds, by dissociating the legal ownership from the beneficial ownership (or the effective control) of the assets.
- **Establishing shell companies:** Shell companies are often established with several forms of ownership structures and with the participation of partners from several countries in order to conceal the beneficial owner.
- **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 to obtain bank accounts in order to justify and make the illicit financial flows appear legitimate[10] , as well as used by certain typologies of illicit finance through other ways, such as trade and import/export operations, since these companies are often used to disguise trade based money laundering or sanction evasion, including targeted financial sanctions.
- **Planning and preparing schemes to conceal the beneficial owner of legal persons[11] which allows the 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 distance the beneficial owners from 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.

3. Money Laundering Crime in The Qatari Law

Article (2) of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing stipulates "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.

10. Guidance for a risk-based approach, Trust and company service providers, FATF, June ٢٠١٩, p-٢٢ ,٩ Vulnerabilities of TCSP services
11. The natural person who ultimately owns or controls a customer, through ownership interest or voting rights, or the natural person on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate, or by any other form of representation. It also includes any person who exercises ultimate effective control over a legal person or arrangement, including any person exercising ultimate effective control by any means (please refer to Part ٦ of the Guidance on Beneficial Owner).

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:

- **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 predicate offence.
- **Money laundering is an independent crime of the predicate offence:** A person may be prosecuted for committing a money laundering crime, even if he was not prosecuted for the predicate offence, and his punishment for the predicate offence shall not prevent his punishment for the money laundering crime..

Article (78) of the Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing Any person stipulates "who commits any of the money laundering crimes stipulated in Article (2) of this Law, shall be sentenced to imprisonment for a term not exceeding ten (10) years, and a fine not less than (QR 2.000.000) two million Qatari Riyals and not more than (QR 5.000.000) five million Qatari Riyals, or twice the value of the money laundered, whichever is greater".

What is Terrorism Financing?

- Terrorists and terrorist organizations need funds and other assets to purchase weapons, training, travel, accommodation, etc to plan and execute terrorist operations, and such funds may come from legitimate or illegitimate sources. Additionally, terrorist organizations often need to obscure and camouflage the sources of funds in their possession as well as to break the links with the parties that provide them with financial support, thereby implementing schemes that are similar to money laundering schemes in order to use such funds without raising the suspicion or attention of law enforcement authorities.
- Terrorism financing includes all forms of material support to terrorism or those who promote terrorism, plan or participate in terrorist acts. It also includes the provision or collection of funds, whether from a licit or illicit source, to be used:
  - for perpetrating a terrorist act(s);
  - by a terrorist or terrorist entity, even in the absence of any relation with a specific terrorist act(s).

1. Terrorism Financing Crime in the Qatari Law

- Article (3) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing stipulates " 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:

12. Article (1) of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism defines the "Predicate Offence" as any act constituting a misdemeanour 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.

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".

- As stated above, terrorism financing is to provide or collect funds, whether from a licit or illicit source, to be used:
  - for perpetrating a terrorist act(s);
  - by a terrorist or terrorist entity, even in the absence of any relation with a specific terrorist act(s).

- 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.

- Article (79) of the same as amended by the Decree law No (19) of 2021 stipulates "any person who commits any of the terrorism financing crimes stipulated in Article (3) of this Law shall be sentenced to life imprisonment and 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 twice the value of the financing provided for, whichever is greater".

2. The Abuse of TCSPs in terrorist financing

Qatar's 2019 National Risk Assessment (NRA) stated that funds placed or moved through legal persons and arrangements, including through the abuse of TCSPs is a method used by terrorist organizations and groups through trade-based means or under the cover of shell companies via the abuse of legal persons and arrangements. However, in Qatar, there have been no cases associated with the abuse of TCSPs for terrorism financing, and the relevant residual risk is therefore considered low.

Shall the Legal Person be punished for ML/TF Crime?

Article (77) of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing stipulates "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, shall 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".

Trust and company service providers compliance with AML/CFT requirements

1. Application of the Risk-Based Approach

I. What is the Risk-Based Approach?

- Risk-Based Approach is a series of measures and procedures that aims at identifying, assessing, understanding and mitigating Money Laundering (ML) and Terrorism Financing (TF) risks, in order to allocate sufficient resources to focus on prioritized areas such as high-risk activities, customers or transactions, to achieve effectiveness[13].

13. Guidance for a risk-based approach, Trust, and company service providers, FATF, June 2019, p12.

RBA Challenges for TCSPs

Culture of compliance and adequate resources:

Implementing an RBA requires that TCSPs have a sound understanding of the risks and are able to exercise sound judgement. A Above all, TCSP and their management should recognise the importance of a culture of compliance across the organisation and ensure sufficient resources are devoted to its implementation appropriate to the size, scale and activities of the organisation. This requires the building of expertise including for example, through training, recruitment, taking professional advice and 'learning by doing'. It also requires the allocation of necessary resources to gather and interpret information on risks, both at the country and institutional levels, and to develop procedures and systems, including ensuring effective decision-making.

Significant variation in services and clients:

TCSPs may vary substantially in the breadth and nature of services provided and the customers they serve, as well as the size, form and degree of complexity of the firm and the level of specialty of its employees. In implementing the RBA, TCSPs should make reasonable judgements for their services and activities. This may mean that no two TCSPs are likely to adopt the same practices.
Appropriate mitigation measures also depend on the nature of service and the provider's role. Circumstances may vary considerably between providers who represent customers directly as trustees or directors controlling the affairs of the legal arrangement or legal person to those that are engaged for distinct purposes such as provision of registered office only services and who have to rely on information on the company's activities from external directors.

Transparency of beneficial ownership on legal persons and arrangements:

TCSPs are involved in the formation, management, or administration of legal entities and arrangements, though they may be challenged in obtaining and keeping current and accurate beneficial ownership information depending upon the nature and activities of their customers. Other challenges may arise when on-boarding new customers, controlling persons or beneficial owners established in another jurisdiction. Finally, whether the source of beneficial ownership information is obtained from a public registry, another third party or the customer, there is always potential risk in the correctness of the information, particularly in the situations where the underlying information has been self-reported. The questions shall be raised directly to the customer, having determined that none of the relevant exceptions to ascertaining beneficial ownership apply, e.g. the customer is a publicly listed company. The information provided by the customer should then be appropriately confirmed by reference to public registers and other sources where possible. This may require further and clarifying questions to be put to the immediate customer. The goal is to ensure that the TCSP is reasonably satisfied about the identity of the beneficial owner (Please refer to Part 6 of this guidance).

Risk of criminality:

TCSPs should be alert to ML/TF risks posed by the services they provide to avoid the possibility that they may commit or become an accessory to the commission of a substantive offence of ML/TF. TCSPs must protect themselves from misuse by criminals and terrorists. This includes the screening and vetting of the sources and methods used for providing payments for the TCSP's services, in order to ensure that there are no unusual or suspicious activity.

II. How do TCSPs assess their ML and TF risks?

- TCSPs must take appropriate steps to identify and assess risks, both at the organizational or corporate levels, given their particular customer base that could be used for money laundering and terrorism financing crimes. They should document those assessments, keep them up-to-date on an ongoing basis and have appropriate mechanisms in place to provide risk assessment information to the AML/CFT Section and competent authorities. Additionally, TCSPs should ensure that the nature and extent of any ML/TF risk assessment is appropriate to the type of business, nature of customers and size of operations.

- To comply with the AML/CFT requirements, TCSPs should:

1. Develop and apply a risk assessment for their business. The goal of the risk assessment is to identify, assess and understand the TCSPs' ML/TF risks commensurate with the size and nature of their business, especially that larger businesses need a more in-depth and comprehensive risk assessment.

2. The risk assessment must consider the following:

   • **Risks identified in the National Risk Assessment (NRA) and Sectoral Risk Assessments (SRAs):** The NRA discusses the primary proceeds-generating crimes in the State of Qatar, as well as ways through which criminals may seek to launder the proceeds of those crimes or terrorist financiers may seek to move funds. In this context, TCSPs must have access to the findings of the NRA and consider whether any of them apply to their business, including their customer base. They must also refer to the specific risk factors applicable to them, as described in the sectoral risk assessments conducted by the regulatory authorities.

   • **Risk factors associated with the customer base:** The risk associated with the customer base may be high if the customer is a high-ranking official or a family member or close associate of a high-ranking official, referred to as "politically exposed persons" (discussed below), or reside in high-risk jurisdictions, or is not physically present for identification purposes (non-face to face transactions). Additionally, the risk associated with the customer may be higher if the customer is a legal person who manages a significant part of his activities, or has branches in high risk jurisdictions, or is a legal person or legal arrangement where its structure or nature makes it difficult to identify beneficial owners thereof; or if the customer attempts to obscure understanding of his transactions carried out through the use of shell or front companies, i.e. those with a complex ownership structure or companies managed across multiple countries without a clear economic purpose; or if the customer attempts to conceal the identity of the beneficial owner.

   The customer associated risk factors that TCSPs should particularly consider are as follows :

   - Customers of the sectors where opportunities for ML/TF are particularly prevalent.

   - PEPs or persons closely associated with or related to PEPs (Please refer to Part 7 of this guidance regarding politically exposed persons).

14. FATF - RBA-Trust-Company-Service-Providers June 2019, p 25.

- Customers conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the customer's representation).

- Customers where the structure or nature of the entity or transaction makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or customers attempting to obscure understanding of their business, ownership or the nature of their transactions, such as:

    - ✓ Unexplained use of shell and/or shelf companies or legal persons with ownership through nominee shares or bearer shares, control through nominee or corporate directors, legal persons or legal arrangements splitting company in establishment and asset administration over different countries, all without any apparent legal or legitimate tax, business, economic or other reason.

    - ✓ Unexplained use of family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason.

    - ✓ Use of trust structures for tax evasion or to obscure ownership in order to protect assets and avoid future losses.

    - ✓ Unexplained use of family or close associates acting as nominee shareholders or directors without any apparent legal or legitimate tax, business, economic or other reason.

    - ✓ Use of trust structures for tax evasion or to obscure ownership in order to protect assets and avoid future losses.

- Unusual complexity in control or ownership structures, or supervision and management without a clear explanation.

- Unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile.

- The offer by the person giving instructions to the TCSPs to pay extraordinary fees for services, which would not ordinarily warrant such a premium.

- The number of employees working for customers is high compared to customers with similar size and businesses (e.g. the turnover of a company is unreasonably high considering the number of employees compared to similar businesses).

- Sudden activity from a previously dormant client[15] without a clear explanation.

- Customers that establish or develop an enterprise with abnormal expenses or customers that enter into new/emerging markets unexpectedly.

15. A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established , Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019, p9

- Indicators that the customer does not wish to obtain necessary approvals and licenses.
- Payments received from multiple un-associated third parties, or payments in cash.
- Inexplicable changes in ownership.
- Customers who have funds that are obviously and inexplicably disproportionate to their situation (e.g. their age, income, occupation or size of wealth).
- Customers who appear to actively and inexplicably avoid face-to-face meetings or who make every possible way to provide instructions intermittently and are otherwise very difficult to reach directly, when this would not normally be expected.
- The legal structure of the entity has been altered frequently and/or without adequate explanation (e.g. change of trade name, transfer of ownership, change of beneficiaries, or change of nominee shareholders, directors, or trustees, etc).
- The activities of the legal person, establishment or legal arrangement are unclear or different from the purposes stated in their internal regulations.
- Management of the legal person, establishment or legal arrangement appears to be acting according to instructions and directives of unknown or inappropriate person(s).
- Unreasonable choice of TCSPs without a clear explanation, given the size or specialization of the TCSP.
- Customers who request that services or transactions be completed in unusually tight or accelerated timeframes without a reasonable explanation for accelerating the transaction, which would make it difficult or impossible for TCSPs to perform a proper risk assessment.
- Frequent or unexplained change of the members of board of directors.
- Customers who insist, without adequate justification or explanation, that transactions be effected through the use of virtual assets for the purpose of preserving their anonymity.
- Customers who change their means of payment for a transaction at the last minute and without justification (or with unclear and doubtful justification), or where there is a lack of information or transparency in the transaction. This risk extends to situations where last minute changes are made to enable funds to be paid by or for a third party.
- Customers with previous convictions for proceeds- generating predicate offences.
- Customers seeking to obtain residents rights in exchange for injecting significant funds into

15. A shelf company is an incorporated company with inactive shareholders, directors, and secretary, which has been left dormant for a longer period even if a customer relationship has already been established , Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019, P.9

the country in which they seek to obtain such right.

- **Risk factors associated with jurisdictions and geographical areas:** the services provided by TCSPs may be high risk when there are factors evidencing that these transactions are connected with jurisdictions identified by credible and reliable source documents (such as by NAMLC, or in Financial Action Task Force (FATF) statements), as not having effective AML/CFT regimes or having significant level of corruption and other criminal activities. The risk factors include, in particular, the following:

  - The origin or location of assets of the establishment, legal person or the express trust;
  - The country in which the establishment, company or the express trust is created or established.
  - The country in which the settlor, beneficial owner or any other natural person exercising effective control over the legal person or legal arrangement.

On the other hand, the risk factors associated with countries/jurisdictions or geographical areas may be lower if the transaction is related to countries having effective AML/CFT regimes, or countries identified by credible and reliable sources as having low level of corruption and other criminal activities, or countries subject to mutual evaluations conducted by credible and reliable organizations.

There is no universally agreed definition of a high risk country/jurisdiction or geographic area but TCSPs should pay attention to:

- Countries/areas identified by credible sources (e.g. FATF or Qatar's regulatory authorities) as providing funding or support for terrorist activities.

- Countries identified by credible sources (e.g. FATF or Qatar's regulatory authorities) as having significant levels of organized crime, corruption, or other criminal activity, including being a major source or a major transit country for illegal drugs, human trafficking or smuggling.

- Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations.

- Countries identified by credible sources (e.g. FATF or Qatar's regulatory authorities) as having weak governance and law enforcement, including countries identified by FATF statements as having weak AML/CFT regimes.

- Countries identified by credible sources (e.g. FATF or Qatar's regulatory authorities) to be non cooperative in providing beneficial ownership information to competent authorities, which can be determined by consulting FATF mutual evaluation reports or reports issued by organisations that also evaluate various co-operation levels such as the OECD Global Forum and reports on compliance with international tax transparency standards.

- **Risk factors associated with delivery channels**[16]: TCSPs must take into consideration delivery channels and understand the extent to which those channels may be misused for money laundering and terrorism financing. These risks may be higher for non-face to face

services and transactions such as transactions concluded through, phone, post or any other arrangement which does not require the personal presence of both parties. Additionally, the risks may be higher for the services and products that ensure anonymity of the person and those which are completed through intermediaries (legal representatives or agents), without direct contact between the customer and the TCSP.

- **Risk factors associated with products, services, transactions and professional practices provided or developed by TCSPs[17]:**

Certain services provided by TCSPs may be higher risk for money laundering and terrorism financing, and may serve as a cover for suspicious transactions that help money launderers, including:

- Services that conceal the real beneficial owner from the competent authorities.

- Services that are delivered deliberately to conceal or disguise the identity of the customer at third parties other persons of interest.

- Services in which TCSPs may represent the customer for third parties, without adequate knowledge of the customer's affairs.

- The use of virtual assets and other anonymous methods of payment in a transaction without a legal, tax, business, or economic reason or other legitimate reason.

- Transactions that use unusual methods of payment (e.g. precious metals or stones).

- Deferment of payment for an asset or service, that is delivered immediately, to a date far from the time when the payment would normally be expected, without adequate safeguards that such payment will be made.

- The acquisition of a company under liquidation without a legal, tax, business, economic or other legitimate reason.
- Where the power of attorney is granted under conditions that are unusual (e.g. it is irrevocable or related to specified assets), without a clear or logical explanation.

- Successive contributions to the share capital of a company over a short period of time without a legal, tax, business, or other justification.

- Transactions or business or real estate services carried out through the trust, company or other legal entity, without any legal or legitimate tax, business and economic reasons.

- The customer's engagement in multiple transactions or activities in a relatively short time span

16. Guidelines for Designated Non-Financial Businesses and Professions- Supplemental Guidance for Trust and Company Service Providers: https://www.economy.gov.ae/english/Pages/AML.aspx
17. Guidelines for Designated Non-Financial Businesses and Professions- Supplemental Guidance for Trust and Company Service Providers: https://www.economy.gov.ae/english/Pages/AML.aspx

or on regular basis, especially when such transactions or activities appear to be inconsistent or in conflict with each other or with the customer's stated business purpose or his licensed activities as stated in the commercial register.

- Suspicion related to fraudulent transactions or transactions that have not been correctly recorded in accounting documents, including but not limited to over-or under- invoicing of goods or services, multiple invoicing of the same goods or services, and false description of goods and services, etc.).

- The risk-based approach does not imply an option left to the free and absolute discretion of the TCSPs, insofar as the said professionals must be able to demonstrate the basis for identifying the risks they face, the methods adopted for complying with the NRA, other sources for identifying such risks, and the methods and timing related to business risk assessment.

- The table below represents a risk assessment matrix, which can be adopted by TCSPs in conducting the business relationship risk assessment or the company/establishment overall risk assessment, in order to identify the necessary steps for risk management and mitigation.

Geographic/Jurisdiction Risks	Customer Risks	Transactions and Services Risks
Low/Medium/High	Low/ Medium/High	Low/ Medium/High
Explanation	Explanation	Explanation
Overall Assessment: Low/Medium/High		
Action plan		

III. What is the Methodology adopted by TCSPs to address and mitigate their ML/TF risks?

1. TCSPs should rely on an appropriate methodology that addresses the risks they face when applying their approach to mitigate ML/TF risks (threat assessment methodology), which is particularly based on the following:
   - Identifying the nature of the business relationship with each customer and understanding its purpose.
   - Assessing the risk profile of the business relationship by rating that relationship (see table above).

2. The threat assessment methodology must be developed in a manner that will enable TCSPs identify and detect any changes in their ML/TF risks.

3. TCSPs must change the risk assessment methodology, as necessary.

4. TCSPs should take into account the findings of the risk profile of the business relationship when determinating the due diligence level and ongoing monitoring measures that will be applied to the customer.

IV. What should TCSPs do with the results of their ML/TF risk assessments?

TCSPs should:

1. Document their ML/TF risk assessments and any basic information in order to be able to demonstrate the basis and sources on which they relied to identify, assess and understand their ML and TF risks, taking into account the National Risk Assessment and any other sources to identify those risks, particularly the sectoral assessment conducted by the Ministry of Commerce and Industry, the risk mitigation procedures taken after the business risk assessment and the relevant outcome, in terms of effective risk mitigation or failure.

2. Monitor the implementation of the risk assessment's findings and the risk assessment on ongoing basis.

3. Provide relevant reports to the AML/CFT Section at the MOCI periodically within the set timeframe and upon its request.

2. AML/CFT Programme:

TCSPs must:

1. Develop an AML/CFT programme that includes internal policies, procedures and controls that take into consideration the identified risks and the size, nature and complexity of their business.

2. Implement the programme effectively to manage and mitigate risks commensurately with the size and nature of their business.

3. Review, update and enhance the programme where necessary.

4. Apply the programme to all their branches and majority-owned subsidiaries in the State and abroad.

5. Provide a copy of the AML/CFT programme along with the annual report of the compliance officer once a year to the AML/CFT Section, as well as any papers or supporting documents that may be required for that purpose.

I. Content of the AML/CFT Programme:

The AML/CFT programme shall include internal policies, procedures, systems and controls aiming at preventing money laundering and terrorism financing, and shall include, in particular, the following:

- Appropriate compliance management arrangement, including the appointment of a

compliance officer and his/her deputy.
- Adequate screening procedures to ensure high standards of efficiency and integrity when employing or appointing officers or employees.
- Preparing an ongoing appropriate training programme for officers and employees.
- Conducting an Independent review and testing to ensure compliance with AML/CFT policies, procedures, systems, and controls.
- Conducting an appropriate and ongoing assessment and review of policies.

TCSPs shall develop and implement policies, programmes and controls to ensure compliance with AML/CFT requirements, and such controls should be:

- In a written form and made available to the concerned persons.
- Updated to keep pace with the latest applicable legislations, the non-compliance cases reported and the outcomes of the independent review and testing.
- Approved by the senior management.

The policies and controls should include the risks faced by TCSPs and detailed measures indicating how these risks are addressed and mitigated. It is also recommended that the policies should include a detailed list of the services delivered by the establishment or company and the risks associated with each service, taking into consideration the risks associated countries and geographic regions.

In practice, TCSPs should develop a guidance on procedures, systems, and internal controls aimed at combating money laundering and terrorism financing, which should be disseminated to the relevant employees of the company or establishment in order to be understood and implemented.

Additionally, it should be noted that TCSPs have general obligations related to the conduct and management of their business, including the following:

- Compliance with the general standards related to the governance system, when exercising their activity as a commercial company.
- Compliance with the supervisory and regulatory standards related to the financial sector.

- Compliance with the legal rules and provisions regulating the commercial companies in general, when exercising their activity as a commercial company.

- Establishing and applying accurate, detailed and robust rules regarding fulfillment of the interests of customers and their business. This requires that, inter alia, the TCSP should:

✓ Develop and implement clear rules regarding the separation and dissociation between customer's funds and obligations and TCSPs' funds and obligations.
✓ Implement effective rules related to the safe and secure custody and conservation of the customer's funds.
✓ Implement effective rules related to the use of highest standards in the management of customer funds, including, in particular, the avoidance and disclosure of any conflict of interests.
✓ Keep records, account files and other documents related to the management of the customer business.
✓ Keep the customer documents such as the deed of incorporation of the commercial company or the deed of the trust.

- ✓ Ensure that all decisions taken, or transactions entered into for the customer are realized by persons (employees, directors, or other persons) with an appropriate level of knowledge and experience to make the appropriate decision, taking into consideration the nature of transaction or decision, customer interest and the provisions of the legal and regulatory texts[18].
- ✓ Comply with and implement the standards related to the financial soundness of the establishment, particularly in relation to the capital, insure the civil liability, maintain the appropriate financial resources and comply with the International Accounting Standards and tax laws.

1. Appointing a Compliance Officer and his/her Deputy

- If the TCSP exercises his activity in an individual establishment, he should personally undertake the responsibilities of the compliance officer within his establishment, and may designate one of his employees as a compliance officer. However, if the TCSP exercises his activity in a commercial company, he should appoint a compliance officer and his permanent deputy from either the governing body or employees.

- The compliance officer shall be responsible for managing the company or establishment's compliance with the AML/CFT requirements stipulated in the AML/CFT Law, its implementing regulations and the MOCI AML/CFT Compliance Rules. The compliance officer shall particularly prepare and submits STRs[19] to the QFIU and shall be responsible for the effective implementation of the AML/CFT Programme (ensuring that appropriate policies and procedures are established, and ongoing training, risk assessment and review & testing are conducted to ensure the effectiveness of this Programme).

- The compliance officer shall act as a primary focal point between the TCSPs and the AML/CFT Section at MOCI and other competent authorities in all matters related to money laundering and terrorism financing.

- The compliance officer should be granted the necessary powers to perform his duties in an effective, objective and independent manner, in accordance with the AML/CFT Compliance Rules. The compliance officer should be able to communicate, directly and periodically, with the senior management of the company, 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 company, 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 DNFBPs under the AML/CFT Law and its implementing regulations.

- The AML/CFT Section and the QFIU should be informed of the name of the compliance officer and his full details, as per the form prepared for this purpose[20].

18. Group of international finance centre supervisors, Trust and company service providers statement of best practice.
19. Article (1) of the MOCI AML/CFT Compliance Rules defines the suspicion report as "The report that the compliance officer at the regulated entity must immediately make to the Unit, upon suspicion or when having reasonable grounds to suspect that a transaction or operation or an attempt to conduct a transaction or operation, irrespective of its value, is linked to or involves proceeds of a predicate offence or relates to terrorism financing".

2. Implementing the necessary Screening Procedures to Ensure High Standards of integrity and efficiency when Appointing Employees and Officers:

- TCSPs shall develop and implement appropriate screening procedures to ensure high standards of efficiency and integrity when appointing or recruiting officers and employees, as stipulated in the AML/CFT Compliance Rules.
- Enhanced screening procedures must be adopted in particular for individuals entrusted with a prominent role or position at the establishment or company, such as front-line agents who deal directly with customers or who supervise transactions[21].
- In order to comply with this requirement, TCSPs 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. Examination may also be performed to verify whether employees meet the required standards of efficiency.

3. Development and Implementation of an Ongoing and appropriate Training Program for Officers and Employees:

- The effectiveness of the developed AML/CFT program is primarily dependent on the ability of officers and employees at the TCSPs to be fully aware of their obligations by virtue of the AML/CFT system and of the responsibilities that may be incurred in case of non-compliance with such obligations, whether intentionally or mistakenly.
- On this basis, TCSPs must develop and design an appropriate and ongoing training programs for officers and employees to acquire and develop the necessary AML/CFT knowledge, skills and qualifications, and keep up with the latest risks, techniques, trends, patterns and indicators of money-laundering and terrorist financing, and ensure they are well acquainted with the risk management and mitigation systems, as well as STRs reporting mechanisms. Training programs must also ensure all officers and employees acquire the adequate awareness and understanding of their legal and supervisory responsibilities and obligations, their role in combating ML/TF, the importance of customers due diligence and supervisory measures towards customers.
- When developing and designing appropriate training programs, TCSPs 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[22] , and ensure the program is a risk based.
- The training program shall include all officers and employees including senior management. Training is provided to new employees upon boarding, without waiting for the next training course, in order that new employees are aware of the applicable policies and controls prior to

20. Anti-Money Laundering Compliance Officer and His Deputy Appointment Form published on the MOCI AML/CFT Section (Supervised Entities).
21. Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019, p17
22. "TCSPs should also develop an ongoing employee training programme. They should be trained commensurate with the complexity of their responsibilities." Guidance for a risk-based approach, Trust, and company service providers, FATF, June 2019, p17

commencement of work. Compliance Officer must ensure that sufficient funds are allocated for the delivery of training.

- There is no uniform and identical training formula for all TCSPs. The best training method is developed 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 training is realized annually and is updated whenever necessary, specifically upon changing of laws, implementing or executive regulations, or the emergence of new methods and policies. TCSPs are also required to review the training needs of their officers and officials at regular and appropriate intervals and to ensure that training program respond effectively to their needs. TCSPs must also develop a plan to address any shortcomings in the approved training program in light of the findings of reviews.

- TCSPs shall document the training program, for example by keeping record of the training attendance. The programme must also be updated to keep pace with the development of applicable legal and implementing texts and international standards as well as new ML/TF patterns.

4. Independent Audit Unit for Ongoing Review Function to Test Compliance with AML/CFT Policies:

TCSPs should carry over 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 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 or company'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 management of the company of TCSPs.

- The methods carried out to test the effectiveness of the AML/CFT programme vary depending on the scale of activity of the TCSPs, 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.

3. Customer Due Diligence Measures:

CDD measures are the set of measures applied to ensure TCSPs are aware of the customers identity, legal status, activity, the purpose and nature of the business relationship, and the beneficial owner.

1. When do TCSPs Apply CDD?

TCSPs should conduct CDD when:

- Establishing business relationship. Many indicators may suggest that the customer wants to establish a permanent business relationship rather than occasional. For example: (1) the customer expects or plans the relationship to be permanent, (2) The work custom requires that the business relationship is permanent in relation to certain situations, (3) the nature of the customer or the transaction indicates or suggests that the customer wants to conduct multiple transactions, (4) The nature of the transaction requires time to complete, such as sale or purchase of real estate[23].

23. Legal Sector Affinity Group Anti-Money Laundering Guidance for the Legal Sector 2021; p. 56

- 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. An occasional transaction is the transaction that does not meet all requirements of a permanent transaction. This is the case when TCSPs expects that the "time factor" is not an element of the transaction. Based on this definition, the relationship between the service provider and the customer is limited to one single transaction provided in a specified period of time.

- 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.

2. Can CDD measures be delayed?

- **In principle,** TCSPs 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. For example, risks are low if the customer is financial institution or DNFBPs subject to AML/CFT requirements, or listed public shareholding companies that are subject to disclosure requirements, or public institutions or agencies.

  - 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 TCSP conducts CDD measures after the establishment of the business relationship, he must document each instance and be prepared to demonstrate to the AML/CFT Section at MOCI, as the supervisory authority, that delayed CDD was appropriate and justified in that context.

3. What are the CDD measures required by TCSPs?

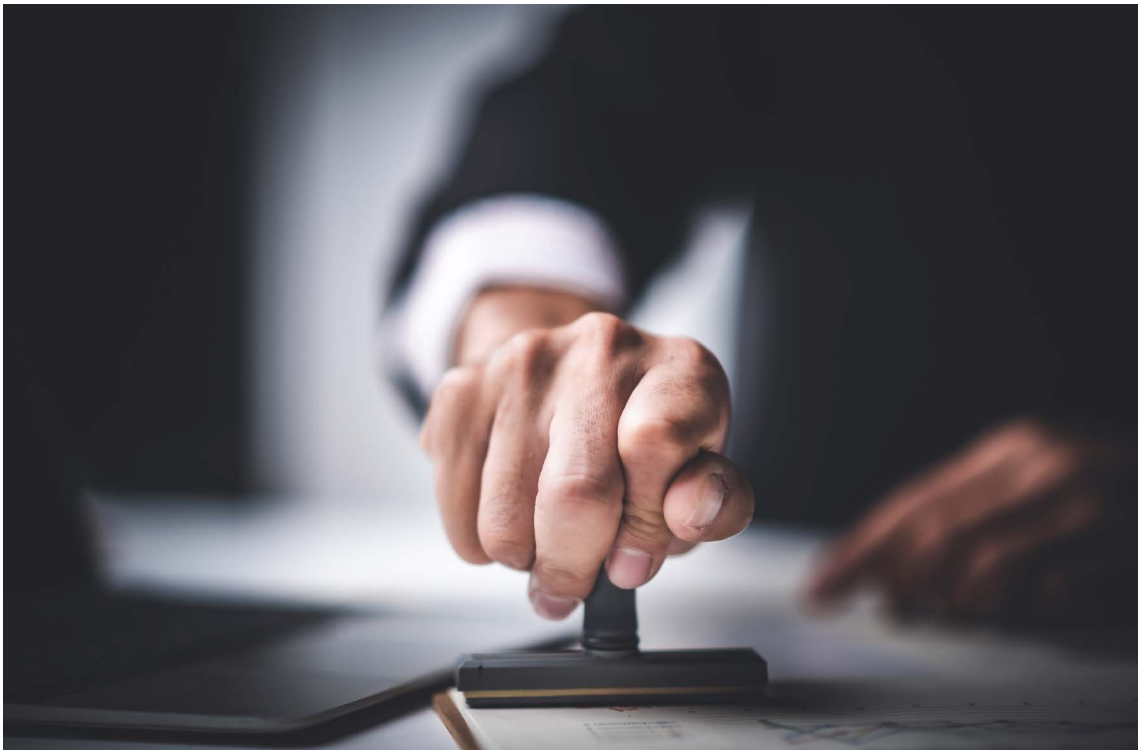
- TCSPs are prohibited to keep anonymous accounts or accounts in obviously fictitious names.
- TCSPs, in particular, shall:

1. Identify the identity the customer, whether permanent or occasional and verify that customer's identity using reliable, independent source documents, data or information.
2. Verify if any person purporting to act on behalf of the customer is so authorised, and identify and verify the identity of that person.
3. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source.
4. Obtain information on, the purpose and intended nature of the business relationship.
5. Determine the nature of the customer's activity in relation to legal persons or arrangements, understand the structure of its ownership and control, and verify the identity of the beneficial owner.
6. Obtain and verify any additional information, depending on the level of risks associated with

the customer, his business or his transactions.

7. 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.

8. Scrutinising transactions to ensure that the transactions being conducted are consistent with theTCSPs' knowledge of the customer, their business and risk profile, including where necessary, the source of funds.



- All the above is verified using reliable, independent source documents, data or information.

- TCSPs 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:

  - **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.

  - **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.

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

- **For customers acting on behalf of another person:** TCSPs shall verify 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.
-

4. Can TCSPs rely on third parties to conduct CDD?

1. In principle: TCSPs may rely on third parties such as financial institutions and DNFBPs to conduct CDD measures including identifying the customer, the beneficial owner and understanding the nature of the business.
2. However, TCSPs remain the ultimate responsible for the proper conduct of CDD measures.

5. What are the Requirements to Reliance on Third Parties to Conduct CDD?

TCSPs, when relying on third-party to perform the CDD measures, 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.

3. Verify that the third party is regulated and supervised and complies with the CDD measures requirements and maintains the records in conformity with the AML/CFT Law, its Implementing Regulations and the AML/CFT Compliance Rules.

4. 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 the third party provides them with all information about the customer obtained from the CDD conducted by the third-party introducer for the customer that they would obtain if they had conducted the CDD themselves

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

TCSPs:

a. Should not establish or continue the business relationship with the customer or carry out the transaction for the customer.
b. Should strongly consider filing 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. What should TCSPs do when they suspect that the transaction is associated with ML or TF?

- TCSPs, upon suspecting that the transaction is associated with ML or TF, when establishing the business relationship or in the course of the said relationship or when conducting the occasional transaction, should carry out the following measures:

  1. Identify the customer's and beneficial owner identity, whether permanent or occasional, and regardless of any exemption or applicable designated threshold.

  2. Submit an STR to the QFIU.

- In cases where TCSPs suspect money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should cease pursuing CDD measures and refuse to establish the business relationship or carry out the transaction.

4. Enhanced CDD Measures:

Enhanced CDD is aimed at obtaining more information about the customer or transaction in order to minimize the risk or probability that the customer or transaction is involved in ML/TF.

1. When should TCSPs apply enhanced CDD measures?

TCSP should apply enhanced CDD:

1. For business relationships and transactions carried out with customers or third parties including financial institutions and DFNBPs from:

- Countries subject to a FATF enhanced due diligence requirement. Information about these countries will be published on NAMLC's website
- 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[24] .

[24] See Circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers on High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring, is published on the webpage for the AML/CFT Section (Legal, International and national framework – Circulars)

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.
- Non-face-to-face business relationships or transactions, including those conducted via the internet, mail, services or transactions provided or carried out via the internet, through the use of ATM machines, telephone or fax.
- Business relationships or transactions involving legal or contractual arrangements which contribute to reduce transparency and conceal the identity of the applicant or customer, particularly those of non-resident customers.
- Business relationships or transactions conducted with PEPs, their family members and close associates of PEPs, as will be discussed later in Part VII of this Guidance.

3. For other cases that are identified by NAMLC and the AML/CFT Section of the MOCI.

2. What are the Enhanced CDD measures to be conducted by TCSPs?

TCSPs should generally carry out the following enhanced measures:

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 undertaking 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. When necessary, make the first payment through an account in the customer's name in a bank that is subject to similar CDD measures[25].

25. FATF Guidance on Risk Based Approach, page 33.

5. Simplified CDD Measures:

1. When can TCSPs conduct simplified CDD?

- TCSPs 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.

  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 high-risk factors, such as a link to a high-risk jurisdiction, present.

- TCSPs 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.

- In all cases where simplified CDD measures are applied, TCSPs are required to document their risk assessment process conducted prior to taking the decision to apply simplified CDD measures. TCSPs must also show evidence to the AML/CFT Section that risks were low.

2. What are the simplified CDD measures that TCSPs can conduct?

Simplified CDD measures may include the following:

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.

6. Beneficial Ownership:

1. Who is the beneficial owner?

The beneficial owner is the natural person (s) who:

a. ultimately owns or controls a customer, through ownership interest or voting rights

b. on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate, or by any other form of representation.

c. who exercises ultimate effective control over a legal person or arrangement, including any person exercising ultimate effective control by any means.

2. What are the TCSPs' obligations in relation to the Beneficial Owner?

a. Before entering into a business relationship with the customer, TCSPs are required to identify the customer and take reasonable measures to verify the identity of the customer, using the relevant information or data obtained from a reliable source, such that TCSPs are satisfied that they know who the beneficial owner is.

b. For customers that are legal persons or arrangements, TCSPs should be required to understand the nature of the customer's business and its ownership and control structure, in line with the criteria set out below.

3. How to identity the beneficial owner?

TCSPs should identify the beneficial owners as follows:

- Identifying the beneficial owner of legal persons:

1. Identify the natural person(s) who ultimately has an effective controlling interest of at least 20% of a legal person or voting rights.

2. If no individual can be identified as the beneficial owner of the legal person, or there is a doubt that a natural person who ultimately owns effective control is the beneficial owner under (1) above; or if no natural person exerts control through ownership interests, TCSPs must identify the natural person (s) exercising de facto or legal control in the legal person and arrangement through any means, whether directly or indirectly, over the executives, the general assembly, or the operations of the legal person, or any other control instruments.

3. In case no natural person is identified under (1) and (2) above, TCSPs should identify and verify the identity of the relevant natural person holding a senior managing position in the legal person (e.g. the legal representative of the commercial company).

- Identifying the beneficial owner of legal arrangements:

1. **If the customer is a trust:** identifying the settlor, the trustee and the protector (if any) and the beneficiaries or class of beneficiaries, and any other natural person exercising, directly or indirectly, ultimate effective control over the trust.

Generally, the above terms should be understood as follows:

- A settlor is generally any person (or persons) by whom the trust was made. A person is a settlor if he or she has provided (or has undertaken to provide) property or funds directly or indirectly for the trust. A settlor may or may not be named in the trust deed. TCSPs should

have policies and procedures in place to identify and verify the identity of the real settlor[26] .

- The trustee: is the person who has the power and the duty to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law.[27]

- In case where no service provider is designated as trustee, TCSP must obtain information for the purposes of identifying and verifying the trustee. If the trustee is a legal person, the service provider must obtain information on the legal person and the beneficial owners of the legal person identified (appointed as the trustee) and take reasonable measures to verify its identity.

- The beneficiary: is the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. All trusts are required to have ascertainable beneficiaries[28] . In line with the RBA, TCSPs are required to adopt policies and procedures which allow them to have reasonable knowledge of the real identity of the beneficial owner, and take reasonable measures to verify the said identity.

- Any other natural person exercising, directly or indirectly, ultimate effective control over the trust: any person exercising, whether alone or jointly with another person or with the consent of anther person, control:

  - ✓ Dispose of or invest trust property,
  - ✓ Direct, make or approve trust distributions
  - ✓ Vary or terminate the trust,
  - ✓ Add or move a person as a beneficiary or to of from a class of beneficiaries
  - ✓ Appoint or remove trustees.

2. **For other types of legal arrangements:** identify the natural person in equivalent or similar positions.

Considering that Endowment (Waqf) is a similar legal arrangement, as provided for in Article (1) of the Decision of the Minister of Commerce and Industry No. (12) of 2020 on issuing the Implementing Regulations of the Unified Economic Register, TCSPs are required to identify the beneficial owners of the Endowment, and take reasonable measures to verify their identity, by verifying the identity of the following:

- The Endower who is responsible for the creation of the endowment, or the the testator of an endowment or deeds of kindness and charity (for bequests of a charitable, family or joint endowment and bequests of acts of kindness and charity). He is in equivalent or similar position as the settlor in Trust.

- The Supervisor who is responsible for the maintenance and care of the endowment. He is the representative of the endowement before third parties and court, whether it is the Ministry or otherwise,[29] and the administrator (or guardian) (for bequests of a charitable,

26. FATF, Guidance for risk-based approach, Trust and company service providers, June 2019, p. 54-55.
27. FATF, international standards on combating money laundering and the financing of terrorism and proliferation, General glossary.
28. FATF, international standards on combating money laundering and the financing of terrorism and proliferation, General glossary.
29. Article (1) of Law No. (9) of 2021 on Endowment.

family or joint endowment and bequests of acts of kindness and charity). He is in equivalent or similar position as the trustee in Trusts.

- The beneficiary who is the person designated by the Endower to receive disbursements from endowment proceeds[30] . He is in equivalent or similar position as the beneficiary or beneficiaries in Trusts.
- The protector, if any[31], and he is in equivalent or similar position as the protector in Trusts.
- Any other natural person exercising ultimate effective control over the endowment, whether directly or indirectly.

3. Taking the necessary measures to identify whether the customer acts as a trustee of a trust or

Obligations related to Beneficial ownership information

R.10 sets out the instances where TCSPs will be required to take steps to identify and verify beneficial owners, including when there is a suspicion of ML/TF, when establishing business relations, or where there are doubts about the veracity of previously provided information. INR.10 indicates that the purpose of this requirement is two-fold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the client to be able to properly assess the potential ML/TF risks associated with the business relationship; and, second, to take appropriate steps to mitigate the risks. TCSPs should have regard to these purposes when assessing what steps are reasonable to take to verify beneficial ownership, commensurate with the level of risk. TCSPs should also have regard to the AML/CFT 2013 Methodology Criteria 10.5 and 10.810.12-.

At the outset of determining beneficial ownership, steps should be taken to identify how the immediate client can be identified. TCSPs can verify the identity of a client by, for example meeting the client in person and then verifying their identity through the production of a passport/identity card and documentation confirming his/her address. TCSPs can further verify the identity of a client on the basis of documentation or information obtained from reliable, publicly available sources (which are independent of the client).

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the TCSP is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity.

This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client, and may include conducting public searches as well as by seeking information directly from the client. TCSPs will likely need to obtain the following information for a client that is a legal entity:

a. the name of the company;
b. the company registration number;
c. the registered address and/ or principal place of business (if different);
d. the identity of shareholders and their percentage ownership;

30. Review, for example, Article (1) of Law N (9) on Endowement (waqf).
31. For more about the "Secretary", review, for example, Article (35) of Law No. (9) of 2021 on endowement.

e. names of the board of directors or senior individuals responsible for the company's operations; and
f. the law to which the company is subject and its constitution; and
g. the types of activities and transactions in which the company engages.

To verify the information listed above, TCSPs may use sources such as the following:

a. constitutional documents (such as a certificate of incorporation, memorandum and articles of incorporation/association);
b. details from company registers; and
c. shareholder agreements or other agreements between shareholders concerning control of the legal person;
d. filed audited accounts.

TCSPs should adopt an RBA to verify beneficial owners of an entity. It is often necessary to use a combination of public sources and to seek further confirmation from the immediate client that information from public sources is correct and up-to date or to ask for additional documentation that confirms the beneficial ownership and company structure. The obligation to identify beneficial ownership does not end with identifying the first level of ownership, but requires reasonable steps to be taken to identify the ownership at each level of the corporate structure until an ultimate beneficial owner is identified.

7. Politically Exposed Persons (PEPs):

In the context of combating money laundering, Politically Exposed Persons are considered high-risk customers. Given that they are entrusted with prominent public functions by the State of Qatar, a foreign state; or by an international organization, PEPs may be involved in or exploit their powers and influence for personal gain, or may misuse or seize public funds. Most often PEPs seek assistant from their family members or close associates to conceal funds resulting from exploiting their prominent functions. Therefore, TCSPs must apply the same measures applied to PEPs to their family members and close associates.

- TCSPs must develop appropriate risk management system to identify whether the customer or the beneficial owner of the customer is a PEP, a family member or a close associate. The risk management system shall include, in particular, requesting information from customers, refer to the publicly available information and review data bases to the extent permitted by the enforced legislation. If the customer or beneficial owner is a PEP or a family member or close associate of a PEP, TCSPs should perform the following CDD measures.

1. Who are the Politically Exposed Persons (PEPS), their family members and close associates?

1. Individuals who are or have been entrusted by the State or by a foreign State with prominent public functions, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned companies, members of Parliaments, and important political party officials, and members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organizations.

2. A wife or a husband and any natural person relative by blood or marriage up to the second degree, who are: Father/ Mother, Father-in-Law/ Mother-in-Law, Son/Daughter, Stepson/ Stepdaughter, Grandfather/Grandmother, Brother/Sister, Brother-in-Law/ Sister-in-Law, Grandson/Granddaughter.

3. PEPs' close associate includes 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.

2. What are the Measures that should be applied by TCSPs if the customer or the beneficial owner is a PEP, family member or close associate?

- If the customer or the beneficial owner is a PEP, a family member or close associate, TCSPs must take further CDD measures:

    - Obtain senior management approval before establishing or continuing a business relationship with existing customers.
    - Take reasonable measure to obtain additional information on the customer's source of wealth and funds, beneficial ownership of PEPs, family members or close associates.
    - Applying enhanced ongoing monitoring to the business relationship by furthering the intensity and degree of supervision, and ensure it is consistent with the pattern of the customer's activity and risks.

- There are several key factors that affect the nature and extent of CDD measures to be applied towards PEPs, such as the PEPs country of origin, quality of services to be provided by TCSPs, whether the PEP is residing in the country where the TCSPs provide their services or in a

foreign country. In cases where the PEP has a business relationship with a customer of a TCSPs, the following factors must be taken into account:

- The nature of the business relationship between the customer and the PEP. If the customer is a direct trust or company or a legal person, even if it is not the natural person who ultimately has an effective controlling ownership interest of the legal person or arrangement, its existence shall have an effect on the assessment of risks.
- The nature of business, for instance, if it is a listed company and is subject to the disclosure requirements which ensure verification of the beneficial ownership with complete transparency.
- The quality of services required, for examples if the risks are low when the PEP is not a customer but a director of a customer who is a public listed compagny, or it is a regulated entity and is purchased for reasonable amount[32].

8. Ongoing Monitoring

- Ongoing monitoring is crucial to understand the customer activities, and it is a key component and part of the effective AML/CFT systems. Ongoing monitoring helps in understanding the nature and size of the customer activities, which allows for monitoring and detecting unusual or suspicious transactions.

- TCSPs shall monitor the business relationship with the customer on an ongoing basis through the following:

- Review of documents, data and information related to the customer to ensure it is up-to-date and relevant.
- Monitor activities (including cash and non-cash transactions) related to the customer to ensure it is consistent with the nature of businesses, the risk profile and source of funds in such a way that the transaction is considered unusual whenever there is inconsistency with the normal or expected pattern of the customer's activity.
- Identify Complex, unusual large transactions, or unusual patterns of transactions which have not any apparent legal or business purpose, suggesting committing a money laundering or a terrorist financing.

- Within the framework of ongoing monitoring, TCSPs must take into account the following:

- Nature and type of transactions (such as unusual size and unusual frequency)
- Value of the transaction, with special consideration given to significant and key transactions.
- Geographical origin/ geographical destinations of paid or received amounts.
- Normal activities or usual sales operations of the customer.

- TCSPs must remain vigilant in addressing changes in the business relationship that may occur over time, which may include: (A.) providing new products or services that involve higher risks, (B.) establishment of new company's structures or new trusts. (C.) change or increase in customers declared activities or customers incomes, (D.) change in the nature of transactions or increase in transactions size and value.

32. Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019, p37

- When there are significant changes in the business relationship, TCSPs must implement further CDD measures to the customer to ensure understanding of ML and TF risks related to the customer and the basis of such business relationship.

9. Reporting Suspicious Transactions:

1. When and to whom shall TCSPs report suspicious transactions?

- TCSPs shall promptly report to the QFIU any transaction or operation or any attempt thereto, regardless of its value, when there is a suspicion or reasonable grounds to suspect that it is associated with, or involves the proceeds of a predicate offence, or may be used in terrorism financing.

- The Compliance Officer at the TCSPs must notify the AML/CFT Section at the MOCI on the filing of STR to the QFIU without providing information or details on the content of the said report.

- TCSPs must submit an STR to the QFIU, regardless of the following:

✓ the value of the transaction or the operation.

- ✓ Whether the transaction is related to tax matters.
- ✓ Whether no transaction or attempt to begin a transaction has been, or will be, conducted.
- ✓ Whether TCSPs has terminated any relationship with the customer.
- ✓ Whether any attempted money laundering or terrorism financing activity in relation to the funds has failed.

- Before deciding whether the unusual transaction or the transaction inconsistent with the custome's known legitimate business and risk profile, is suspicious or not, TCSPs must particularly take into account the following:

1. The transaction has no apparent economic or lawful purpose.
2. The transaction has a reasonable explanation or when the customer has failed to give an adequate explanation for the transaction or to fully provide information about it.
3. When the transaction involves the use of a newly established business relationship or is a one-off transaction.
4. When the transaction involves the use of offshore accounts, companies or structures that are not supported by the customer's economic needs.
5. When the transaction involves unnecessary routing of funds through third parties.

2. Confidentiality and Tipping-off

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

    1. customer knowing or suspecting that he is or may be the subject of:
        b. a suspicion report; or
        c. an investigation relating to money laundering or terrorism financing; and

    2. may compromise the prevention or detection of ML and TF offences, the apprehension or prosecution of offenders or the recovery of proceeds of crime.

- Any violation to the above mentioned prohibition leads to the imposition of the penalties provided for in Article (84) of the AML/CFT Law which stipulates that "Any person who commits the offense 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."

- It shall be prohibited to disclose to the concerned person or others any information relating to the submission or non-submission of a suspicious report to the Financial Information Unit or any other relevant information. This prohibition is 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 TCSP must be mindful when dealing or communicating with the customer after reporting a suspicious transaction to QFIU;inquiries can be presented to the customer as long as they fall within the conduct of business relationship and within the regular diligences that are normally applied by the TCSP. For example, TCSPs may request information from the customer on holding of a general assembly by the company or failure to do so, or certain data relating to tax returns from the customer or in relation to the customer's finances (net income earned, absorbing previous years losses, distribution of profits or a change in the value of capital by increasing or decreasing ...).

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

- If the TCSP reasonably believes that performing the CDD measures will tip-off the customer, he he must cease pursuing these measures and should file an STR with the QFIU. The TCSP shall take all reasonable procedures to ensure that information relating to suspicious transaction reports are kept confidential.

3. How to submit STRs and what are the consequences of reporting ?

- TCSPs shall submit STRs to the QFIU and complete all relevant fields in the standard form with as much accurate information as is available in the Suspicious Transaction Report Form adopted by the QFIU[33] and the instructions issued by the QFIU.

- In this context, TCSPs can usefully consult the Guidance on Reporting STRS, prepared by the QFIU[34].

- TCSPs are protected from both criminal and civil liability for breach of any restriction on disclosure of information imposed by law or regulation or by administrative order or contract, if they report their suspicions in good faith. This protection shall be available even if they did not know precisely what the underlying predicate offence was, and regardless whether it actually occurred.

33. The Suspicious Transaction Report Form adopted by the QFIU is published on the AML/CFT webpage/ reporting STRs.
34. The Guidance on Reporting STRs for DNFBPs is published on the AML/CFT webpage/ reporting STRs.

10. Record Keeping:

A: What Records should TCSP Keep?

Trust and Company Service Providers should keep:

1. Records, documents and data on all domestic and international transactions and operations.
2. Records, documents and data obtained or collected while performing CDD.
3. Account files, business correspondence, and results of any analysis undertaken.
4. All relevant information that enables tracing all financial transactions, when when attempting to perform financial transaction by the customer, and all related reports.

B: How Long Must Records be Kept?

- Pursuant to the requirements set forth in Article (20) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, TCSP shall maintain all records, documents and data for all domestic and international transactions and operations, for a minimum of ten (10) years:

    1. From the date of concluding the transaction, domestic or international occasional transaction or operation.

2. Following the termination of the business relationship

- TCSP must retain records beyond the end of the ten-year period mentioned above.

1. If TCSP has filed with the QFIU a suspicious transaction report relating to the applicant for business or customer.

2. If he knows that the applicant for business or customer is under investigation by law enforcement authorities for issues related to money laundering or terrorism financing.

C: To Whom Should TCSPs Make Records Available?

- TCSP should ensure that all CDD records, data and documents on transactions and operations are available without delay to the competent authorities upon request.

- TCSP should also establish adequate systems to ensure prompt response to the requests of the competent authorities.

D: What is the Purpose of Keeping Records?

1. They provide proof of TCSP's compliance with AML/CFT requirements.
2. They allow authorities to reconstruct individual transactions so as to provide, if necessary, evidence for the prosecution of criminal activity.
3. They allow the TCSP to respond to requests by QFIU, supervisory authorities, competent authorities, law enforcement authorities or judicial authorities.

Sanctions and Penalties Imposed on TCSPs for Breach of AML/CFT Obligations

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

A. Penalties:

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 enhanced due diligence 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.

B. 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/CFT, 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 submitting 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.

TCSPs may appeal the decisions referred to, in accordance with the controls, procedures and timelines set forth in article (64) and (65) of the implementing regulations of law No.(20) of 2019 promulgated by Council of Ministers' Decision No. (41) of 2019.

References

1. Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

2. Law No. (1) of 2020 on the Unified Economic Register.

3. Law No (9) of 2021 on endowement (Waqf).

4. Decree law No (19) of 2021 amending some provisions of law No (20) of 2019 on combatting Money Laundering and Terrorism Financing .

5. Council of Minister's Decision No. [41] of 2019 Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism as amended by Council of Ministers› Decision No. (14) of 2021.

6. Council of Ministers' Decision No. (12) of 2020 Promulgating the Implementing Regulations of Law No. (1) of 2020 on the Unified Economic Register.

7. Decision of the Minister of Commerce and Industry No. (95) of 2019 to establish an Anti-Money Laundering and Terrorism Financing Section under Companies Affairs Department.

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

9. FATF, the misuse of corporate vehicles including trust and company service providers, October 2006.

10. Guidance for a risk-based approach, Trust and company service providers, FATF, June 2019.

11. Money laundering using trust and company service providers, Financial action task force/ OECD/ Caribbean/ Financial action task force, October 2010,

12. Money Laundering and terrorist Financing Vulnerabilities of legal professionals, FATF, JUNE 2013.

13. Professional Money Laundering, FATF, July 2018.

14. Guidelines for Designated Non-Financial Businesses and Professions- Supplemental Guidance for Trust and Company Service Providers: https://www.economy.gov.ae/english/Pages/AML.aspx

15. UAE- Ministry of economy – Anti Money laundering and combatting the Financing of Terrorism and illegal Organisations, Supplemental Guidance for Trust & Company Service Providers, May 2019.

Useful Links

- **Financial Actions Task Force**

https://www.fatf-gafi.org/

- **Middle East and North Africa Financial Action Task Force on Combating money laundering and financing of terrorism (MENAFATF)**

http://www.menafatf.org/

- **National Anti-Money Laundering and Terrorism Financing**

http://www.namlc.gov.qa/en/index.html

- **Qatar Financial Information Unit**

http://www.qfiu.gov.qa/

- **Webpage of the Ministry of Justice**

https://www.moj.gov.qa/en/pages/default.aspx

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

https://www.moci.gov.qa/en/anti-money-laundering-and-terrorism-financing/

- Email: control.aml@moci.gov.qa
- Address: 2 floor Ministry of Commerce and Industry Lusail City, Qatar

وزارة التجارة والصناعة
Ministry of Commerce and Industry