البنك المركزي العُماني
Central Bank of Oman

الهيئة العامة لسوق المال
Capital Market Authority
Keep Evolving تطور مستدام

رؤية عمان 2040
ننطلق بثقة
Moving Forward with Confidence

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines for Financial Institutions

AML – CFT Department

CMA & CBO

Table of Contents

Chapter 1
Overview

1. Introduction

1.1 Purpose and Scope

The purpose of the Anti-Money Laundering and Combatting the Financing of Terrorism Guidelines for the Financial Sector (the "Guidelines"), is to assist financial institutions in understanding their AML/CFT obligations under Royal Decree No.30/2016 Promulgating the Law on Combating Money Laundering and Terrorism Financing ("AML/CFT Law"), Central Bank of Oman (CBO) Instructions for all Licensed Financial Institutions under the Supervision of the CBO on implementing Combating Money Laundering and Terrorism Financing Law No.30/206 ("CBO Instructions"), Decision No. E/80/2021 Instructions to the Capital Markets Institutions on the Implementation of the Provision of the Law on Combating Money Laundering and Terrorism Financing ("CMA Capitals Markets Sector Instructions") and Decision No.E/81/2021 Instructions to Insurance and Takaful Companies, Brokers and Agents on the Implementation of the Provision of the Law on Combating Money Laundering and Terrorism Financing ("CMA Insurance Sector Instructions").

Specifically, these Guidelines are applicable to all natural and legal persons in the following categories:

- Banks, finance leasing companies, money exchange establishments, payment service providers
- Insurance and Takaful Companies, agents and brokers;
- Companies operating in the securities sector and Muscat Clearing and Depository Company
- Virtual Asset Service Providers (VASPs)

Financial Institutions should note that guidance on the subject of Targeted Financial Sanctions (TFS) and the related Ministerial Decision No. 1/2022 of the National Committee for Combating Terrorism (NCCT) is outside the scope of these Guidelines.

1.1.2 Status of the AML/CFT Guidelines for Financial Institutions

These Guidelines do not constitute additional legislation or regulation and are not intended to set legal, regulatory or judicial precedent. They are intended to be read in conjunction with the relevant laws, regulations and supervisory instructions, which are currently in force in Oman and supervised institutions are reminded that the Guidelines do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between the Guidelines and the AML/CFT law or Supervisory Instructions, the latter will prevail.

These Guidelines should not be construed as legal advice or legal interpretation. Supervised institutions should perform their own assessments of the manner in which they should meet their statutory obligations, and they should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to their particular circumstances.

These Guidelines, and any lists and/or examples provided in them, are not exhaustive and do not set limitations on the measures to be taken by financial institutions in order to comply with their statutory obligations under the legal and regulatory framework currently in force.

Nothing in these Guidelines should be interpreted as providing any explicit or implicit assurance that the supervisory authorities would defer or refrain from exercising their enforcement, judicial or punitive powers in the event of a breach of the AML/CFT law, regulations or supervisory instructions.

1.1.3 Legal and Regulatory Framework

National Legislative and Regulatory Framework

The Central Bank of Oman (CBO) is the competent authority in Oman for the monitoring and supervision of Banks, FLCs, PSPs, and MEEs compliance with their obligations under the AML/CFT Law and CBO Supervisory Instructions.

The Omani AML/CFT legislative framework is set out in Royal Decree No.30/2016 Promulgating the Law on Combating Money Laundering and Terrorism Financing ("the AML/CFT Law") which obliges all financial institutions to put in place an effective, risk-based AML/CFT Framework which includes the application of a risk-based approach to customer due diligence measures, reporting of suspicious transactions, governance, policies and procedures record keeping and training.

By way of circular BM 1187, CBO issued *Instructions for all Licensed Financial Institutions under the Supervision of the CBO on implementing Combating Money Laundering and Terrorism Financing* which are applicable to all Financial Institutions which are subject to supervision by CBO. These Instructions are binding on all CBO supervised financial institutions, breaches of which are subject to the sanctions set out in Article 52 of AML/CFT Law. These instructions amend and replace Instructions BM 1152.

Decision No. E/81/2021 on the Instructions to Insurance to Insurance and Takaful Companies, Brokers and Agents on the Implementation of the Provisions of the Law on Combating Money Laundering and Terrorism Financing was issued by CMA in 2021. These Instructions are binding on all Insurance and Takaful Companies, Brokers and Agents and breaches are subject to sanctions and penalties as set out in Article 52 of the AML/CFT Law. These instructions amend and repeal Decision No. E/3/2020.

Decision No. E/80/2021 on the Instructions to Capital Markets Companies on the Implementation of the Provisions of the Law on Combating Money Laundering and Terrorism Financing was issued by CMA in 2021. These Instructions are binding on all Capital Markets Companies and breaches are subject to sanctions and penalties as set out in Article 52 of the AML/CFT Law. These instructions amend and repeal Decision No. E/4/2020.

International Legislative and Regulatory Framework

The AML/CFT legislative and regulatory framework of Oman is part of a larger international AML/CFT legislative and regulatory framework made up of a system of intergovernmental legislative bodies and international and regional regulatory organizations. These bodies create laws at the international level, which participating member countries then transpose into their national counterparts. In parallel, international and regional regulatory organizations develop policies and recommend, assess and monitor the implementation by participating member countries of international regulatory standards in respect of AML/CFT.

The Financial Action Task Force (FATF): FATF is an in intergovernmental body established in 1989, which sets international standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF also monitors the implementation of its standards, the 40 FATF Recommendations and 11 Immediate Outcomes by its members and members of FSRBs to ensure that the FATF Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of the AML/CFT frameworks is properly applied.

The Middle East and North Africa Financial Action Task Force (MENAFATF):

Recognizing the FATF 40 Recommendations on Combating Money Laundering and the Financing of Terrorism and Proliferation, and the related UN Conventions and UN Security Council Resolutions, as the worldwide-accepted international standards in the fight against money laundering and the financing of terrorism and proliferation, MENAFATF was established in 2004 as a FATF Style Regional Body (FSRB), for the purpose of fostering co-operation and co-ordination between the countries of the MENA region in establishing an effective system of compliance with those standards. The Sultanate of Oman is a founding member of MENAFATF.

The United Nations (UN):

The UN is the international organization with the broadest range of membership. Founded in October of 1945, there are currently 191 member states of the UN from throughout the world. The UN actively operates a program to fight money laundering, the Global Programme against Money Laundering (GPML), which is headquartered in Vienna, Austria, is part of the UN Office of Drugs and Crime (UNODC).

All financial institutions should ensure that they are aware of and have regard to any information and guidance which is published by these bodies.

1.1.4 Sanctions for non-compliance

The main AML/CFT supervisory objective of the CBO and CMA is to ensure compliance by all financial institutions in Oman. As a result, breaches of the AML/CFT Law and Supervisory Instructions may result in serious penalties as provided for in Article 52 of the AML/CFT Law. In the imposition of sanctions, the CBO and CMA seek to provide a credible deterrent to FIs and individuals, and to encourage high standards in all FIs in the financial sector in Oman. The following sanctions are provided for in the AML/CFT Law:

A) Written warning
B) Order to comply with specific instructions
C) Order to submit regular reports on the measures being taken by the FI
D) Administrative Fine of not less than RO 10,000 and not more than RO 100,000 for each violation
E) Replace or limit the mandate of Compliance officers, directors, board members, or controlling owners including the appointment of a special administrative supervisor
F) Suspend prevent individuals from working in the commercial business sector or in a particular occupation or activity, either temporarily or permanently
G) Imposition of Guardianship over the FI
H) Suspend, cancel or place restrictions on the licence to practice operations or activity.

1.2 Money Laundering and Terrorist Financing

1.2.1 Money Laundering

Article 6 AML/CFT Law

Article 6 of the AML/CFT Law defines Money Laundering as intentionally engaging in any of the following acts, having knowledge or should have knowledge or suspected that the funds are the proceeds of crime, whether the person had committed the predicate offence or not:

- Converting or transferring such funds for the purpose of disguising or concealing the illegal nature or source of such proceeds
- Assisting any person who committed the predicate offence to evade punishment for their acts;
- Disguising or concealing the true nature, source, location, method of disposal, movement or ownership of the funds and their related rights;
- Acquiring, possessing or using proceeds upon receipt

The AML/CFT Law defines "funds" very broadly as "any type of assets or property regardless of its value, nature or the way it is acquired, whether electronic or digital, whether inside or outside the Sultanate of Oman, including any profits or interests on such property that is due or has been fully or partially distributed. This includes local and foreign currency, financial and commercial instruments, immovable or moveable, tangible or intangible and corporeal or incorporeal assets and all the rights or interests vested therein, deeds and documents evidencing all the above, including bank credits, deposits, postal drafts, bank drafts, and letters of credit or anything that the Committee considers as funds for the purposes of this law" Proceeds of crime is defined as "any funds derived or obtained directly or indirectly from a predicate offence, including profits, economic benefits and advantages and any similar funds converted fully or partially into other funds"

The AML/CFT Law designates Money Laundering as a criminal offence. Its prosecution is independent of that of any predicate offence to which it is related or from which the proceeds are derived. The suspicion of money laundering is not dependent on proving that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved, but can be inferred from certain information, including indicators or behavioural patterns.

Predicate Offences

Article (1) of the AML/CFT Law defines a predicate offence as *"any act constituting an offence under the laws of Oman, and acts committed outside Oman if they are considered an offence in accordance with the laws of the country in which the crime was committed and Omani laws"*. A predicate offence is therefore any crime, whether felony or misdemeanour, which is punishable in Oman, regardless of whether it is committed within the State or in any other country in which it is also a criminal offence.

1.2.2 Financing of Terrorism

Article 8 and Article 9 AML/CFT Law

Article (8) of the AML/CFT Law designates the financing of terrorism as a criminal offence and is defined pursuant to in the following way:

- Willingly collecting or providing funds, directly or indirectly and by any means, with the knowledge that such funds will be used in full or in part, to carry out a terrorist act, or by a terrorist individual or a terrorist organisation
- Financing the travelling of individuals to a country other than their country of residence or nationality with the intent to perpetrate, plan, prepare for, participate in or facilitate terrorist acts, or provide the necessary funds for training on terrorist acts or receiving such training.

Article 9 of the AML/CFT Law provides that a crime of terrorism shall be deemed to be committed regardless of the following; whether the act occurred, the country where the act or attempted act was carried out and whether the funds were actually used to commit the act of terrorism.

1.2.3 Phases of Money Laundering

To identify, understand and accurately assess the ML/TF risks to which FIs are exposed, FIs should be aware of the three phases of money laundering. Identifying the phase in which a certain product can be misused or the FI itself can be misused, will help the FI understand its specific inherent ML/TF risks.

The below paragraphs describe the crime of money laundering as consisting of three phases. It should be noted that each of these three stages can occur simultaneously, separately or they can overlap.

Phase 1 - Placement

The placement stage is the first stage in the process whereby criminals attempt to introduce funds or the proceeds of Crime into the financial system using a variety of techniques or typologies

Examples of placement transactions include the following:

Blending of funds: Comingling of illegitimate funds with legitimate funds, such as placing the cash from illegal narcotics sales into cash-intensive, locally owned businesses.

Foreign exchange: Purchasing of foreign exchange with illegal funds.

Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade attention or reporting requirements.

Currency smuggling: Cross-border physical movement of cash or monetary instruments.

Loans: Repayment of legitimate loans using laundered cash

Phase 2- Layering

The second stage in the process is the layering stage. The overriding objective of this stage of the process is to distance the illicit money from its source. Often, this is accomplished by placing the funds into circulation through formal financial institutions, and other legitimate businesses, both domestic and international. In this layering phase, criminals attempt to disguise the illicit nature of the Funds or Proceeds of Crime by engaging in transactions, or layers of transactions, creating complex layers which aim to conceal their source and ownership of the funds.

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and/or markets;
- Moving funds from one financial institution to another or within accounts at the same institution;
- Converting the cash placed into monetary instruments;
- Reselling high-value goods and prepaid access/stored value products;
- Investing in real estate and other legitimate businesses;
- Placing money in stocks, bonds or life insurance products; and
- Using shell companies to obscure the ultimate beneficial owner and asset

Phase 3 - Integration

This is the final stage of the money laundering process whereby the previously laundered funds or proceeds of crime are reintroduced into the legitimate economy or are used to commit new criminal offences through transactions or activities that appear to be legitimate. In this stage, funds appear legitimate as normal business or personal transactions.

A key objective for criminals engaged in money laundering—and therefore a key generic risk underlying the specific risks faced by FIs—is the exploitation of situations and factors (including products, services, structures, transactions, and geographic locations) which favour anonymity and complexity, thereby

facilitating a break in the "paper trail" and concealment of the illicit source of the Funds.

In respect of TF, while the transaction size can be significantly smaller than those involved in ML operations, and some of the typologies and specific techniques used may differ, the overall principles and generic risks are the same. The terrorists and criminals involved in these acts attempt to exploit situations and factors favouring anonymity and complexity, in order to obscure and conceal the illicit source of the Funds, or the illicit destination or purpose for which they are intended, or both. FIs should remain careful that their services are not being used either directly or indirectly to facilitate Money Laundering or the Financing of Terrorism in any of the three stages described above.

1.2.4 ML/TF Typologies

The methods which are used by criminals for ML and TF are continually evolving and becoming more sophisticated. It is therefore critical in combating these crimes that FIs ensure that all of their employees are well trained, knowledgeable and remain up-to-date on the latest ML/TF trends and typologies.

There are numerous useful sources of research and information related to ML/TF typologies, including by the Supervisory Authorities, the FATF, MENAFATF and other FSRBs, the Egmont Group, BASEL and others. FIs should incorporate the regular review of ML/TF trends and typologies into their compliance training programmes as well as into their risk identification and assessment procedures.

Below are some examples of the **key ML/TF typologies** with which FIs should be familiar include (but are not limited to):

- **Currency exchange/cash conversion:** used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimize risk of detection – e.g., purchasing of travellers cheques to transport value to another jurisdiction.
- **Cash couriers / currency smuggling:** concealed movement of currency to avoid transaction / cash reporting measures.
- **Structuring (smurfing):** A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of

small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.

- **Use of credit cards, cheques, promissory notes, etc**.: Used as instruments to access funds held in a financial institution, often in another jurisdiction.
- **Purchase of portable valuable commodities (gems, precious metals, etc.):** A technique to purchase instruments to conceal ownership or move value without detection and avoid AML/CFT measures – e.g., movement of diamonds or gold to another jurisdiction.
- **Purchase of valuable assets (real estate, race horses, vehicles, etc.):** Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.
- **Commodity exchanges (barter):** Avoiding the use of money or financial instruments in value transactions to avoid AML/CFT measures - e.g., a direct exchange of heroin for gold bullion.
- **Use of wire transfers:** to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation.
- **Underground banking / unlicensed remittance services**: Illegal mechanisms based on networks of trust used to remit monies, without the proper license or registration. Often work in parallel with the traditional banking sector and exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.
- **Trade-based money laundering and terrorist financing:** usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.
- **Abuse of non-profit organizations (NPOs):** May be used to raise terrorist funds, obscure the source and nature of funds and to distribute funds for terrorist activities.
- **Investment in capital markets**: to obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low reporting requirements.
- **Mingling (business investment):** A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the illegal source of the funds.

- **Use of shell companies/corporations:** a technique to obscure the identity of persons controlling funds and exploit relatively low reporting requirements.
- **Use of offshore banks/businesses, including trust company service providers:** to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.
- **Use of nominees, trusts, family members or third parties, etc**: to obscure the identity of persons controlling illicit funds.
- **Use of foreign bank accounts**: to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.
- **Identity fraud / false identification**: used to obscure the identity of those involved in many methods of money laundering and terrorist financing.
- **Use of "gatekeepers" professional services (lawyers, accountants, brokers, etc.):** to obscure the identity of beneficiaries and the illicit source of funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.
- **New Payment technologies:** use of emerging payment technologies for money laundering and terrorist financing. Examples include cell phone-based remittance and payment systems.
- **Virtual assets: (VA)** and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. FIs may refer to the FATF Recommendations that place AML/CFT requirements on Virtual Assets (VA) and Virtual Asset Service Providers (VASPs). The FATF has also issued a document on Guidance on Risk Based Approach to VAs and VASPs. FIs should be familiar with the AML/CFT risks of dealing with VAs and VASPs in accordance with the FATF guidance.
- **Life insurance products:** may be used for money laundering when they have saving or investment features which may include the options for full or partial withdrawals or early surrenders.
- **General insurance product:** there are several cases where the early cancellation of policies with return of premium has been used to launder money.

- A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time;
- Return premium being credited to an account different from the original account;
- Requests for return premiums in currencies different from the original premium;
- Regular purchase and cancellation of policies.
- Insurance policy being closed with request of payment to be made to a third party account.

- **Overpayment of premiums:** arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made, in this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally' but on a recurring basis, significantly overpay his premiums and request a refund for the excess.
- **Using of Prepaid cards:** Prepaid cards can be misused for money laundering and terrorist financing due to their potential anonymity and ease of cross-border transactions.
- **Tax Evasion:** This can be through underreporting income or creating false deductions, resulting in the generation of untraceable funds that can be used for illicit purposes.
- **Non-financial Businesses:** Non-financial businesses can be used for money laundering and terrorist financing by providing a means to legitimize illicit funds through transactions or services, making it difficult to trace the origin of the funds. This includes, travel agencies, by facilitating the movement of illicit funds through booking fraudulent or overpriced travel services, car dealerships, by manipulating vehicle sales and transactions to legitimize illicit funds and obscure their origin, cash intensive business, such as, large hypermarkets by using large cash transactions to obscure the origin and nature of illicit funds, etc.

Chapter 2
Identification and Assessment of ML/TF Risks

The AML/CFT Law and Supervisory Instructions require FIs to apply a risk-based approach in the identification and assessment of ML/TF Risks.

2.1 Risk-Based Approach (RBA)

A risk-based approach (RBA) is central to the effective implementation of AML/CFT obligations as provided for in the AML/CFT legislation and Supervisory Instructions. This means that FIs must identify, assess and understand the ML/TF risks to which they are exposed and take AML/CFT measures commensurate to those risks in order to mitigate them effectively. This requires a comprehensive understanding by all FIs of the ML/TF risks which are faced by Oman, as well as the risks to which the sector and the individual FI are exposed.

It should be noted that regardless of the strength and effectiveness of an FI's AML/CFT compliance framework, ML/TF risk cannot be entirely eliminated and there may be situations where an FI has taken all reasonable measures to identify and mitigate ML/TF risks, but it is still used for ML/TF in isolated instances. FIs should nevertheless understand that a RBA is not a justification for disregarding certain ML/TF risks, nor does it exempt them from taking reasonable and proportionate mitigation measures, even for risks that are assessed as low.

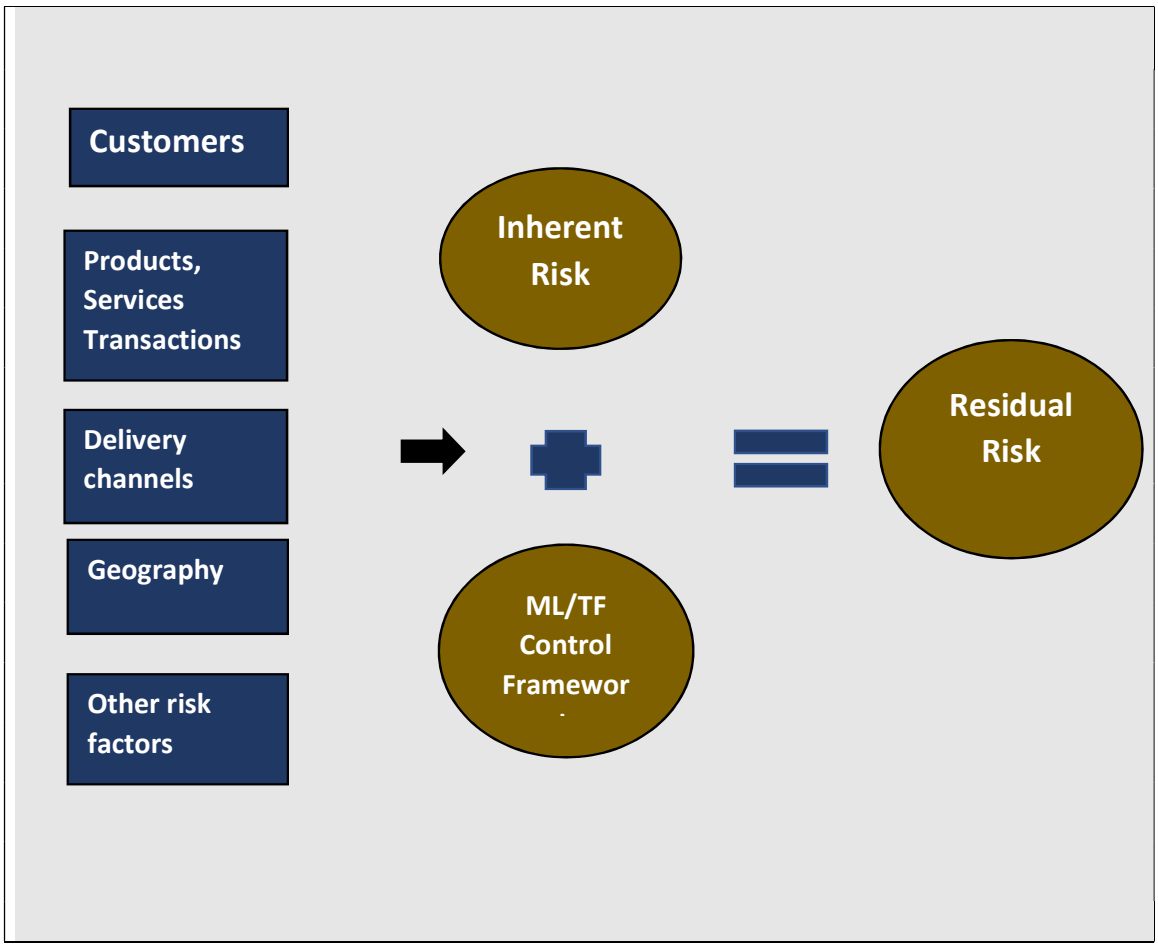
The use of a RBA requires FIs to allocate resources on a risk-sensitive basis, with the objective of using these resources in a more efficient and effective manner

FIs are required to conduct a business ML/TF risk assessment which assists FIs in understanding risk exposure and identifies areas which would be prioritised in combatting ML/TF. Risk assessment is a very important step to allow an FI to establish a good AML/CFT compliance program; as it highlights risks associated with FIs' business and thus the specific controls to be applied.

2.2 ML/TF Business Risk Assessment:

Article 34 AML/CFT Law, Article 3 CMA Decision No.E/80/2021, Article 3 CMA Decision No.E/81/2021, Article 2 CBO Instructions

Overview of ML/TF Risk Assessment process



The first step in implementing a RBA is to identify, assess and understand the ML/TF risks by conducting an ML/FT risk assessment of the entire business.The purpose of such an ML/TF business risk assessment is to improve the effectiveness of ML/TF risk management, by identifying the inherent ML/TF risks faced by the business as a whole, determining how these risks are effectively mitigated through internal policies, procedures and controls, and establishing the residual ML/TF risks and any gaps in the controls that should be addressed.

An effective ML/TF business risk assessment should allow FIs to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are appropriately aligned with residual risks.

A business risk assessment should consist of two distinct but related steps:

- Identifying ML and TF risks relevant to an FI's business, and;
- Assessing the identified ML and TF risks to understand how to mitigate those risks.

The first step of conducting an ML/TF business risk assessment for FIs is to identify and understand the inherent ML/FT risks (i.e., the risks that an FI is exposed to if there were no control measures in place to mitigate them) across all business lines and processes with respect to the following risk factors:

- Customers,
- Products, services and transactions,
- Delivery channels,
- Geographic locations,
- Any other risk factors.

Once the inherent risks have been identified and assessed, the FI can then determine the nature and intensity of risk mitigating controls to apply to the inherent risks. The level of inherent ML/TF risks influence the nature and levels of AML/CFT resources and mitigation strategies which FIs are required to put in place.

The identification and assessment of inherent ML/TF risks and of the effectiveness of the risk mitigation measures will result in a residual risk assessment, i.e., the risks that remain when effective control measures are in place. In situations where the residual risk falls outside the risk appetite of the FI, additional control measures will need to be implemented to ensure that the level of ML/TF risk is acceptable to the FI.

FIs should decide on both the frequency and methodology of their ML/TF business risk assessment, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/TF risks to which they are exposed, as well as the results of the NRA, Sectoral and Topical Risk Assessments. FIs should perform the ML/TF business risk assessment at least annually and prior to the launch of a new product, service, business practice or delivery mechanism an a new or developing technology for new or pre-existing products or services. They should also decide on policies and procedures related to the periodic review of their ML/TF business risk assessment methodology, taking into consideration changes in internal or external factors. These decisions should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

As part of the model or methodology, FIs should consider including in their ML/TF risk assessment the following elements:

- Likelihood or probability of occurrence of identified inherent risks;
- Timing of identified inherent risks;
- Impact on the organisation of identified inherent risks.

The result of an effective ML/TF business risk assessment will be the classification of identified risks into different categories, such as high, medium, low, or some combination of those categories (such as medium-high, medium-low). Such classifications should assist FIs in prioritizing their ML/TF risk exposures more effectively, so that they may determine the appropriate types and levels of AML/CFT resources needed, and adopt and apply reasonable and risk-proportionate mitigation measures.

2.3 Risk Factors

As part of the business-wide ML/TF risk assessment, a thorough identification of risk factors is crucial to the effective assessment of ML/TF Risk. Risks will often occur as combinations of these risk factors. For example, a risk can occur as a result of the interrelationship between a customer and the jurisdictions where that customer is from or is active, or because of the connection between a product and the delivery channel.

The AML/CFT Supervisory Instructions outlines risk factors which FIs should consider when identifying and assessing the ML/TF risks to which they are exposed. In addition to these, FIs should use various relevant sources when conducting their business risk assessment, for example:

- ML/TF red flag indicators
- Information from national sources, including the results of the NRA, relevant sectoral risk assessment, any Topical Risk Assessment with regard to ML/TF trends and sectoral threats and guidance, notices or circulars from the relevant supervisory authorities;
- Communications from the National Centre of Financial Intelligence ("NCFI") or any other competent authority;
- Information from Industry bodies and Representatives
- Information from publications of relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, UNODC, and other.

In keeping with the ever-evolving nature of ML/TF risks, and to ensure that FIs implement a model for conducting the ML/TF business risk assessment that is effective and appropriate to the nature and size of their businesses, FIs should continuously update the risk factors which they consider as part of the risk assessment, in order to reflect new and emerging ML/FT risks and typologies.

A good practice for FIs to assess the inherent risk factors, is to formulate risk scenarios and assess the likelihood that a scenario occurs and the impact should a scenario materialize. The likelihood can be assessed based on the number of times per year that a risk scenario can occur. The impact can be assessed based on the possible financial and reputational effects that can result if a scenario indeed occurs. In this way, the FI can determine the inherent risks of a risk factor.

When assessing the inherent risks, an FI should make an inventory of the customers it services, the products and services it offers, define the scope of business areas to assess, including business units, legal entities, divisions, countries and regions. For this, an FI should have consideration of up-to-date quantitative and qualitative information (variables) on for, for example, the types and number of customers, the volume of operations (deposits or transactions) for the types of customers, volume of business/transactions per product and services and geographic locations.

FIs should note they should always take a holistic view of the risk associated with any situation and unless specifically required by the AML/CFT Law, Supervisory Instructions or any other relevant legislation, the presence of isolated risk factors does not necessarily move a relationship into a higher or lower risk category. The below sections provides guidance on the core risk factors mentioned above which should be taken into account by the FI when conducting the business risk assessment.

2.3.1 Customer Risk

Customer risk factors relate to types or categories of customers. Certain customer or business relationship categories pose a risk that should be taken into account when assessing the overall level of inherent customer risk.

When assessing the risk associated with customers, FIs should consider the following:

- Types of customers: The risks related to retail customers in combination with their product/service needs on one hand, may be different from those related to high net worth or corporate customers and their respective product/service needs. Likewise, the risks associated with resident customers may be different from those associated with non-resident customers. Also, the risks associated with complex beneficial owner is higher than clear 25% beneficial ownership.

- Customer base. FIs with small, similar, customer bases may face different risks from those FIs with larger, more diverse customer bases. Equally, those FIs who are targeting growing or emerging markets may face

different customer risks than those with more established customer bases.

- Status of customer relationship. FIs that rely on more transactional, occasional, or one-off interactions with their customers may be exposed to different risks from institutions with more repetitive, mature or long-term business relationships.

Below is a non-exhaustive list of specific customer risk factors which FIs should consider when assessing customer risk:

- Categories of business relationships with complex legal, ownership, or direct or indirect group or network structures, or with less transparency with regard to beneficial ownership, effective control, or tax residency, may pose different ML/TF risks than those with simpler legal/ownership structures or with greater transparency.
- Categories of Customers involved in highly regulated and supervised activities and those customers who are involved in activities that are unregulated.
- Customers associated with higher-risk persons or professions for example Politically Exposed Persons (PEPs) due to their influential positions, access to significant financial resources, and potential for abuse of power and corruption.
- Customer linked to sectors that are commonly associated with higher ML/TF risks such as import/export, logistics, free zones, real estate investments, third party payment processers, etc.
- Non-resident legal persons or legal arrangements particularly those with connections to offshore and high risk jurisdictions.
- Legal persons that have nominee shareholders or shares in bearer form.
- Legal persons or arrangements that are personal asset management vehicles.
- Professionals (e.g., lawyers, accountants and TCSPs) acting as introducer or intermediary on behalf of customers or groups of customers (whereby there is no direct contact with the customer).

- High net worth individuals or beneficiaries whose source of information is unclear
- Respondent banks from high risk countries.
- Customers which are cash-intensive undertakings or have links to sectors that involve significant amounts of cash
- Customers who are new undertakings without an adequate business profile or track record.
- Customers who are sanctioned by the relevant supervisory authority for non-compliance with AML/CFT obligations and is not engaging in remediation to improve its AML/CFT framework.
- Nationals from high-risk/ sanctioned countries as there are potential of involvement in illicit activities.
- Non-high risk countries nationals but dealing with high-risk countries (remittances, business relationships, etc.) as the regulatory oversight in these countries is limited.

Some of these customer risk factors are also relevant when determining the customer risk classification of an individual customer and the type and extent of customer due diligence to be performed (see Section on Customer Due Diligence)

2.3.2 Product, Service and Transaction Risk

When assessing the inherent ML/TF risks associated with product, service, and transaction types, an FI should consider its lines of business, products and services that are more vulnerable to ML/TF abuse. Some of the risk factors that FIs should consider, among others, are:

- **Complexity**: Products, services, or transactions that favour complexity (especially when that complexity is excessive or unnecessary) can often be exploited for the purpose of ML/TF. FIs should consider the conceptual, operational, legal, technological and other complexities of the product, service, or transaction type.
  Those with higher complexity or greater dependencies on the interactions between multiple systems and/or market participants may expose FIs to

different types and levels of ML/TF risk than those with lower complexity or with fewer dependencies on multiple systems and/or market participants.
The speed of money flow for each product or service shall be considered as it may challenge the seize or freeze of the criminal proceeds as it can be quickly transferred or transported to another country.

- **Transparency and transferability:** Situations that favour anonymity or opaqueness can often be exploited for the purpose of ML/TF. FIs should consider the level of transparency and transferability of ownership or control of products, services, or transaction types, particularly in respect of the ability to monitor the identities and the roles/responsibilities of all parties involved at each stage.

  Special attention should be given to products, services, or transaction types in which funds can be pooled or co-mingled, or in which multiple or anonymous parties can have authority over the disposition of funds, or for which the transferability of beneficial ownership or control can be accomplished with relative ease and/or with limited disclosure of information.
  Regard should also be had to lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify.

- **Value and Size:** Products, services, or transaction types with different size or value parameters or limits may pose different levels of ML/FT risk. In particular, FIs should consider the extent to which the product or service allows high-value or unlimited-value transactions (there is no limit on certain transaction values or levels of premium); the product or service has a global reach; transfers are made from one or more payers in different countries to a local payee.
  FIs should also have regard to the extent to which products and services may be cash intensive, for example, certain types of payment services and current accounts.

- Typology: FIs should consider whether the product, service, or transaction type is associated with any established ML/FT typologies (see Section on ML/TF Typologies)

2.3.3 Country or Geographic Risk

FIs should consider geographic ML/TF risk factors both from domestic and cross-border sources. Geographic risks arise from:

(i) the locations where the FI has offices, branches and majority owned subsidiaries and

(ii) locations in which the customers obtain nationality, reside or conduct their activities.

Examples of some of these factors which FIs should consider include:

Effectiveness of a jurisdictions AML/CFT Regime: Countries with stronger AML/CFT controls present a different level of risk than countries with weaker regulatory and supervisory frameworks, for example, those countries identified by the FATF as high- risk jurisdictions subject to a call for action and jurisdictions under increased monitoring (black list) or those countries which are identified by the National Committee for Combating Terrorism Financing ("NCCT") or those countries which are identified by credible sources as having trends and patterns in terrorism activities (ex: Global Terrorism Index (GTI)

International Sanctions: Countries or jurisdictions which are the subject of international sanctions, such as targeted financial sanctions (TFS), Oman, OFAC, UN and EU restrictive measures, that could impact their ML/TF risk exposure and mitigation requirements.

Reputation: Countries or jurisdictions which are associated with higher or lower levels of ML/TF, corruption, and (lack of) transparency (particularly as regards financial and fiscal reporting, criminal and legal matters, and Beneficial Ownership, but also including such factors as freedom of information and the press).

It should be noted that FIs should consider the geographic risk in conjunction with customers risks, including principal, residential or operating locations of customers.

2.3.4 Delivery Channel Risk

There are different types and levels of ML/TF risk associated with individual delivery channels for the acquisition and management of customers and business relationships, as well as for the delivery of products and services.

When assessing delivery channel-related risk, FIs should pay particular attention to the those delivery channels, whether related to customer acquisition and/or relationship management, or to product or service delivery, which have the potential to favour anonymity and opaqueness. Among others, these may include:

- non-face-to-face channels (especially in cases where there are no safeguards in place such as electronic identification means), such as ATM/CDM, internet banking, mobile banking, electronic wallet, or other remote-access services or technologies;
- Allowing non-FI customers to use the channels.
- Allowing access through international system (such as international cards).
- third-party business introducers, intermediaries, agents or distributors;
- third-party payment, or other transaction intermediaries.;
- reliance on a third party's CDD measures in situations where the FI does not have a long-standing relationship with the referring third party;
- new delivery channels that have not yet been tested

2.4 Emerging and evolving ML/TF Risks

ML/TF risks are always evolving and new risks are constantly emerging, whilst existing ones may increase in importance due to legal or regulatory developments, changes in the marketplace, or as a result of new or disruptive products or technologies. Therefore, it is important for FIs to note that no list of risks can ever be considered as exhaustive.

Nevertheless, some additional factors that may present specific risks are as follows:

- the introduction of new products or services,
- new or developing technologies or delivery processes or
- the establishment of new branches and subsidiaries in Oman and abroad.

FIs should ensure that they have systems and controls in place to identify emerging ML/TF risks and that they can assess these risks and where appropriate, incorporate them into their ML/TF risk assessment in a timely manner. To ensure that FIs are in a position to review and update the ML/TF business risk assessment as well as mitigation measures, FIs should establish a strong culture of information sharing within the FI, engage with relevant industry bodies and relevant authorities and ensure relevant staff within the FI are made aware of such findings. In addition, FIs should take into consideration the results of the NRA, relevant Sectorial Risk Assessments and any Topical Risk Assessment. FIs should also consult publications from official sources on a regular basis, including those of the CMA and CBO, the FATF, MENAFATF and other FSRBs, the Egmont Group, and others.

Examples of some of the types of additional risk factors which FIs may consider in identifying and assessing their ML/FT risk exposure include:

Innovation. FIs should consider the level of experience with and knowledge of the product, service, transaction, or delivery channel type. Products, services, transaction, or delivery channel types that are new to the market or to the business may not be as well understood, and may therefore pose a different level of ML/TF risk than more established ones. Likewise, products, services, transaction, or delivery channel types which are unexpected or unusual with respect to a particular type of customer may indicate a different level of potential ML/TF risk exposure than would more traditional or expected product, service, transaction, or channel types in regard to that same type of customer.

Cyber security/distributed networks.

FIs may consider evaluating the degree to which their operational processes and/or their customers expose them to the risk of exploitation for the purpose

of professional third-party ML/TF through cyber-attacks or through other means, such as the use of distributed technology or social networks.

2.5 Assessing new Products and Technologies Risks

In accordance with Article 41 of the AML/CFT Law, FI's must *"identify, assess and mitigate money laundering and terrorism financing risks that may arise from new technologies and business practices, including new delivery mechanisms, or from the use of new technologies".*

The assessment of such risks and implementation of appropriate risk management measures must occur **prior** to launching or using such new products, business practices or technologies.

For the purpose of assessing the ML/TF risks associated with new products, services, practices, techniques, or technologies, FIs may use the same or similar risk assessment models or methodologies as those which are used for their ML/TF business risk assessments, and updated as appropriate. New product, service, practice, technique, or technology risk assessments should also be documented in line with the nature and size of their businesses

2.6 Risk Assessment Methodology

When assessing ML/TF risk, each FI should determine the type and extent of the risk assessment methodology which is appropriate for the size and nature of their businesses. FIs should note that a business risk assessment does not need to be complex to be effective a good risk assessment can be developed on the basis of relevant risk factors and sources of information. FIs with smaller or less complex business models may have simpler risk assessments than those of institutions with larger or more complex business models, which may require more sophisticated risk assessments. In all cases, the rationale for using a certain methodology must be documented by the FI.

While, the ML/TF risk methodology must be specific to each individual FI, below are some examples of what an effective methodology should be based upon;

Examples of what an effective Risk methodology should include:

i. Quantitative and qualitative data and information, which includes information from internal meetings or interviews; internal questionnaires concerning risk identification and controls; review of internal audit reports;

ii. Is reflective of the FI's AML/CFT risk appetite and strategy which is approved by management

iii. Takes into consideration input from relevant internal sources, including input and views from the designated AML/CFT compliance officer and any other relevant units like risk management and internal control;

iv. Takes into consideration relevant information (such as ML/TF trends and sectorial risks) from external sources, including the NRA, sectorial risk assessment or any Topical Risk Assessment, supervisory and other competent authorities, and the FATF, MENAFATF and other FSRBs, the Egmont Group, and others where appropriate;

v. Describes the weighting of risk factors, the classification of risks into different categories, and the prioritisation of risks.

vi. Evaluates the likelihood or probability of occurrence of identified ML/TF risks, and determining their timing and impact on the organization.

vii. Takes into account whether the AML/CFT controls are effective, specifically whether there are adequate controls to mitigate risks concerning customers, products, services, or transactions.

viii. Determines the effectiveness of the AML/CFT risk mitigating measures in place by using information such as audit and compliance reports or management information reports.

ix. Determines the residual risk as a result of the inherent risks and the effectiveness of the AML/CFT risk mitigating measures.

x. Establishes whether additional AML/CFT controls are required, based on the residual risk and the risk appetite

xi. Determines the rationale and circumstances for approving and performing manual interventions or overrides to model-based risk weightings or classifications.

xii. Is properly documented and maintained, regularly reviewed and updated, and communicated to management and relevant personnel within the organisation.

xiii. Is tested and audited for the effectiveness and consistency of the risk methodology and its output with regard to statutory obligations.

2.7 Documenting, Monitoring and Review of ML/TF Risk Assessment

In accordance with the AML/CFT Law and the Supervisory Instructions, FIs are required to document their ML/TF business risk assessment, including the methodology, analysis, and all supporting data. FIs must also make the business risk assessments available to the CBO and CMA upon request. FIs should incorporate into their documentation, the information used to conduct the ML/TF business risk assessment in order to demonstrate the effectiveness of their risk assessment processes.

Examples of such information include, but are not limited to:

- FI's overall risk policies (for example, risk appetite statement, customer acceptance policy, and others, where applicable).

- ML/TF risk assessment model, methodology and procedures, including such information as organizational roles and responsibilities; process flows, timing and frequency; internal reporting requirements; and review, testing, and updating requirements.

- Risk factors identified, and input received from relevant internal sources, including the designated AML/CFT compliance officer.

- Organization's overall risk policies (for example, risk appetite statement, customer acceptance policy, and others, where applicable).

The documentation measures taken by FIs should be reasonable and commensurate with the nature and size of their businesses.

2.8 Updating of ML/TF Risk Assessment

FIs are obliged to keep their ML/TF business risk assessment under continual review. In fulfilling this obligation, they should review, evaluate and update their ML/FT business risk assessment processes, models, and methodologies periodically, in keeping with the nature and size of their businesses. Where an FI becomes aware that a new risk has emerged or an existing risk has increased, this should be reflected in the risk assessment as soon as possible. FIs should also update their ML/TF business risk assessment whenever they become aware of any internal or external events or developments which could affect their accuracy or effectiveness.

Such developments may include, amongst other things, changes in business strategies or objectives, technological developments, legislative or regulatory developments, or the identification of material new ML/FT threats or risk factors. In this regard, FIs should take into consideration the results of the most recent NRA, Sectorial Risk Assessment or any Topical Risk Assessment, as well as circulars, notifications and any published information from official sources, such as the supervisory authorities; other national Competent Authorities; or relevant international bodies, such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others.

Chapter 3
Mitigation of ML/TF Risks

The AML-CFT Law and Supervisory Instructions, require FIs to apply a risk-based approach when applying AML/CFT compliance measures.

In accordance with the AML/CFT Law, FIs, must *"develop and implement programs for combating money laundering and terrorism financing and apply them to all members of the financial group. Such programmes must include policies, procedures, internal regulations and controls".* Therefore, FI's must establish and maintain compliance programmes which are tailored to mitigate ML/TF risks to which they are exposed and to demonstrate to the CBO and CMA, as appropriate, that all reasonable steps have been taken to ensure compliance with the AML/CFT Law and Supervisory Instructions. Regardless of the nature or size of an FI, a risk-based approach must be implemented in respect of the mitigation of ML/TF Risks.

The basic elements that must be contained in an AML/CFT compliance programme are as follows:

I. A system of internal policies, procedures and controls, including an ongoing employee training program
II. A designated compliance function with a compliance officer or money laundering reporting officer
III. An independent audit function to test the overall effectiveness of the AML program

This is commonly referred to as the three lines of defence model and should be based upon the nature, scale and complexity of the FIs business. FIs should ensure that there is adequate and effective coordination between all lines of defence to ensure robust and well-structured oversight, as well as effective co-ordination of resources to manage overlap in areas of review.

3.1 Internal Policies, Procedures and Controls

Policies:	Clear and simple high-level statements that are uniform across the entire organization and which sets the "tone from the top".
Procedures:	Translates the AML/CFT policies into an acceptable and work-able practice, tasking the stakeholders with their respective responsibilities.
Controls:	The internal systems, tools or technology which the FI utilizes to ensure the AML/CFT program is effective, functioning as intended and within predefined parameters.

FIs must ensure that the internal policies, procedures and controls which have been implemented allow them to effectively manage and mitigate the ML/TF risks which have been identified in their ML/TF business risk assessment. Such AML/CFT policies, procedures and controls must be:

- Documented and accessible by all members of staff who are expected to abide by them
- Reasonable, proportionate to the risks involved and consistent with the results of the ML/TF Risk Assessment
- Commensurate with the nature and size of the business
- Approved by senior management
- Reviewed for effectiveness and subject to continuous updating
- Applicable to all branches and subsidiaries
- Take into consideration the results of the NRA, relevant Sectorial Risk Assessment, any Topical Risk Assessment and the FI's own ML/TF business risk assessment and any other relevant information.

In developing the internal AML/CFT control systems, FIs should also take into account their IT infrastructure and management information systems capabilities. In particular, FIs should consider how well their technical infrastructure, including their data management and management information reporting capabilities, are suited to the ML/FT risk mitigation requirements of the types of customers they deal with, particularly in respect of the size and growth dynamics of their customer base.

A robust internal control framework, which includes policies and procedures is a fundamental element for ensuring an FI's AML/CFT compliance and is comprised of the following elements:

A. The identification and assessment of ML/TF Risks (see Section 4)
B. Customer Due Diligence (including enhanced due diligence and simplified due diligence)
C. Ongoing monitoring of Customers and Transactions
D. Reporting of Suspicious Transactions
E. AML/CFT governance
F. Record Keeping

The below sections provides guidance in respect of each of these areas.

3.2. Customer Due Diligence (CDD)

CDD is a critical element in an FI's AML/CFT compliance program and requires FIs to take specific steps to identify their customers. The inadequacy or absence of identification measures can expose an FI to serious reputational, operational and regulatory damage which can result in significant financial cost to the business.

The AML/CFT law requires the implementation of a risk-based approach to the CDD process by obliging FIs to "*apply due diligence measures taking into consideration the results of the risk assessment…"* It is further provided in the legislation that FIs must *"establish and implement enhanced due diligence measures in high risk cases"* and *"may identify and conduct simplified due diligence measures in low risk cases, provided that there is no suspicion of money laundering or terrorist financing".*

FIs should note that a customer's ML/TF risk profile is subject to continuous review and may change as a result of certain factors. The appropriate level and type of due diligence which should be applied by the FI will always depend on the specific situation and the risk factors which have been identified.

3.2.1 Assessment of the Customer and Business Relationship Risk

Article 36 AML/CFT Law, Article 3(6) Decision No E/80/2021, Article 3(6) Decision No E/81/2021, Article 2 (2) CBO Instructions

A customer of an FI is anyone who:

- performs a one-off or occasional financial activity or transaction or
- anyone who establishes an ongoing commercial or financial relationship with the FI.

FIs are required to identify and assess the ML/TF risk in relation to a customer or business relationship to determine the level of CDD that is required. An accurate assessment therefore is essential to ensure the application of risk-based due diligence measures and should incorporate the results of the ML/TF business Risk Assessment, the NRA, the relevant sectorial risk assessment, any Topical Risk Assessment as well as relevant input from internal stakeholders, including the AML/CFT Compliance Officer.

In assessing customer or business relationship risk, FIs should analyze customers on the basis of the identified risk factors in order to arrive at a risk classification and may use different methodologies to accomplish their risk classification, depending on the nature and size of their businesses, and of the risks involved.

Regardless of the methodologies chosen, FIs should ensure that their business relationship risk assessment processes and the rationale for their methodologies are well-documented, approved by senior management, and communicated at the appropriate levels of the organization. FIs should also develop policies and procedures related to both the periodic review of their business relationship risk assessment processes, and to the frequency for updating the individual business relationship risk assessments and customer risk classifications produced by them, taking into consideration changes in internal or external factors.

Risk classification: FI's should establish a risk classification for the customers which is commensurate with the nature of and levels of ML/TF risk involved, for example, Low Risk, Normal Risk and High Risk. Risk classifications allow FIs to compare a customer's actual activity with the expected activity more effectively, which provides them with information which may lead to the discovery of unusual circumstances or potentially suspicious transactions.

The risk classification is based on sufficient knowledge of the customer and BO, intended nature of the business relationship and the source of funds.

Based on the risk profile, FIs should carry out ongoing due diligence of their business relationships, so as to be able to ensure that the transactions conducted are consistent with the information they have about the customer, the type of activity they are engaged in, the risks they entail, and, where necessary, their source of funds.

The risk classifications must be documented and FIs must be in a position to demonstrate to CBO and CMA that the CDD measures are commensurate to the level of risk identified.

3.2.2 Circumstances for undertaking CDD measures

Article 33 AML/CFT Law, Article 6 CBO Instructions, Article 8 Decision No E/81/2021, Article 9 Decision No E/80/2021

In accordance with Article 33 of the AML/CFT Law, FIs are required to apply CDD measures in the following situations:

(i) prior to establishing a business relationship,
(ii) prior to carrying out a transaction for a customer with whom it does not have an established business relationship[1]

[1] In line with Article 33 AML/CFT Law, a transaction threshold of OMR 5000 or above, whether the transaction is carried out in single or multiple operations that appear to be linked is provided for in CBO Instructions.

(iii) prior to executing a wire transfer for a customer with whom it does not have an established business relationship (occasional transaction)[2]

(iv) where there is a suspicion of money laundering or financing of terrorism

(v) where there are doubts concerning the accuracy or adequacy of identification documents and information which have been obtained.

In line with the AML/CFT Law and Supervisory Instructions, FIs should note that in circumstances where they form a suspicion of ML/TF and they reasonably believe that performing CDD measures would tip off the customer, then they should not apply CDD measures, but should instead report their suspicion to the NCFI.

(i) Establishment of a Business Relationship

A relationship is established with a customer when an FI conducts any activity for, on behalf of, or at the direction or request of the customer, which us intended to be ongoing or recurring in nature. The following are non-exhaustive examples of such activities which lead to the establishment of a business relationship:

- Assigning an account number or opening an account in the customer's name;
- conducting any transaction in the customer's name or on their behalf, or at the customer's direction or request for the benefit of someone else;
- Providing any form of tangible or intangible product or service (including but not limited to granting credits, guarantees, or other forms of value) to or on behalf of the customer, or at the customer's direction or request for the benefit of someone else;
- Signing any form of contract, agreement, letter of intent, memorandum of understanding, or other document with the customer in relation to the performance of a transaction or series of transactions, or to the provision of any form of tangible or intangible product or service as described above;

[2] In line with Article 33 AML/CFT Law, a transaction threshold of OMR 350 or its equivalent in foreign currency is set by CBO.

- Accepting any form of compensation or remuneration (including a promise of future payment) for the provision of tangible or intangible products or services, as described above, from or on behalf of the customer;
- Receiving funds or proceeds of any kind (including those held on a fiduciary basis, for safekeeping, or in escrow) from or on behalf of the customer, whether for their account or for the benefit of someone else;
- Any other act performed by FIs in the course of conducting their ordinary business, when done on behalf of, or at the request or direction of, a customer.

In such situations, the FI is obliged to undertake the appropriate risk-based CDD measures which are outlined in this Guidance.

Aside from situations in which business relationship is established, CDD must also always be conducted in the following situations:

a) Where there is the existence of an ML/TF suspicion
b) There are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

(ii) Occasional Transaction

FIs may also be required to perform occasional or non-recurring transactions for customers with whom there is no ongoing business relationship. Examples of such transactions include, but are not limited to:

- Exchange of currencies;
- Issue or cashing/redemption of cheques;
- Transfer of money or other value for a walk-in customer.

In such situations, FIs are required to identify the customer and verify the customer's identity as well as that of the beneficial owners, beneficiaries, and controlling persons and are also required to understand the nature and purpose of the customer's business and transactions in the following circumstances[3]:

[3] This relates to CBO supervised institutions only.

- Before carrying out occasional transactions for a customer for amounts equal to or exceeding OMR 5,000 (or equivalent in any other currency), whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- Before carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding OMR 350 (or equivalent in any other currency)
- When there is a ML/TF suspicion
- When there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Indicators of transactions that may appear to be linked include:

- Multiple transactions with the same or similar customer reference codes;
- Transactions executed sequentially or in close time proximity, and involving the same or related counterparties;
- Multiple transactions attempted by a customer with whom there is no business relationship at different branches of the same FI on the same day.

3.2.3 Timing of CDD Measures

There are certain situations where an FI may deviate from the normal CDD process;

- **Where the ML/TF risks are identified as low:** FIs may complete the verification of the customer's identity after establishing the business relationship under the conditions specified in the relevant provisions of the AML/CFT Law and Supervisory Instructions. In such circumstances, the verification of the identity must be conducted as soon as possible and FIs must ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefiting from the business relationship prior to the completion of the verification process. Examples of such measures which FIs may consider taking in this regard are, among others:
  - Limiting the number, types and/or amounts of transactions that can be performed;

- Holding funds in suspense or in escrow until the verification of the identity is completed;
- Making the completion of the verification of the identity a condition precedent to the closing of a transaction.

- **Legal Arrangements** such as Trusts, or of life insurance policies (including funds-generating transactions, such as life insurance products relating to investments and family Takaful insurance) in which there are beneficiaries who are not named, but instead belong to a designated class of future or contingent beneficiaries, FIs are required to obtain sufficient information about the details of the class of beneficiaries so as to be in a position to establish the identity of each beneficiary at the time of the settlement, pay-out, or exercise of their legally acquired rights. Furthermore, FIs must verify the identity of the beneficiaries at the time of settlement or pay-out and prior to the exercise of any related legally acquired rights. They should also ensure that they implement appropriate and effective measures to manage and mitigate the risks of crime and of the customer benefiting from the business relationship prior to the completion of the verification process. Examples of such measures which FIs may consider taking in this regard are, among others:
  - Holding funds in suspense or in escrow until the verification of the identity is completed;
  - Making the completion of the verification of the identity a condition precedent to the closing of a transaction.

- **When a legal entity customer is a public company listed on a stock exchange** FIs are exempted from identifying and verifying the identity of any shareholder or beneficial owner of that company once the company is subject to adequate disclosure requirements to ensure transparency of beneficial ownership. Examples of reliable information sources in this regard include, but are not limited to:
  - Credit reporting agencies;
  - Stock exchange disclosure reports or websites;
  - Corporate annual reports, websites, or other forms of official public disclosure;

- Official or public registries;
- Credible and well-established media outlets.

In such situations, an FI is only required to obtain customer identification documentation on the company itself.

3.2.4 Customer Due Diligence Measures

Chapter 3 CMA Decisions No E/80/2021 and No E/81/2021,

Chapter 4 CBO Instructions

FIs are required to apply a number of CDD measures under the AML/CFT Law and Supervisory Instructions. However, in line with the risk-based approach, FIs should be aware that the CDD measures which are taken must always be in line with the customers ML/TF risk classification and the identified risk factors. The following is a list of (non-exhaustive) risk-based CDD measures which FIs must apply:

a) Identification of the customer, beneficial owner, beneficiaries and controlling person on the basis of independent sources, data and information and verification of their identity as appropriate
b) Obtaining an understanding of the intended purpose and nature of the business relationship, as well as, in the case of legal persons or arrangements, of the nature of the customer's business and its ownership and control structure
c) Screening of the customer, beneficial owners, beneficiaries, and controlling persons, for the applicability of targeted or other international financial sanctions, and, particularly in higher risk situations, to identify any potentially adverse information such as criminal history
d) Ongoing monitoring of the business relationship, to ensure consistency between the transactions or activities conducted and the information that has been gathered about the customer and their expected behaviour
e) Scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are

consistent with the FI's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

f) Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

In cases of higher risk, FIs are required to apply additional or enhanced CDD measures. (See Section 3.2.7)

FIs should ensure that they have implemented adequate CDD policies and procedures which are proportionate to the risks involved, approved by senior management and communicated to relevant employees of the FI. Such policies and procedures should include but are not limited to the following:

- The circumstances, timing, and composition in regard to the application of CDD measures;
- Frequency of reviews and updates in relation to CDD information;
- Extent and frequency of ongoing supervision of the business relationship and monitoring of transactions in relation to customers to which CDD measures are applied.

I. Identification and Verification of Identity

The identification and verification of identity of customers is a crucial component of an effective AML/CFT compliance program. The AML/CFT Law requires FIs to "*determine and verify the identity of customers based on reliable and independent sources, documents and data…"* and to "*identify beneficial owners and take reasonable measures to verify their identity in a satisfactory manner"*

As outlined earlier in this Guidance, the specific requirements concerning the timing, extent and methods of identifying and verifying the identity of customers and beneficial owners is dependent on the type of customer (natural or legal person) and the level of risk associated with that customer. The required documentation is outlined in detail in the Supervisory Instructions.

FIs are obliged at a minimum to identify and verify the identity of the customer as outlined in the relevant provisions of the CBO and CMA supervisory

Instructions. FIs should also have risk-based policies and procedures in place in relation to the identification and verification of customers (including beneficial owners and those with a controlling interest)

Where an FI is unable to comply with the required identification and verification requirements, it is not permitted to open the account, commence the business relationship, or carry out the transaction. In such cases, the FI must immediately file a report with the NCFI.

II. Nature and purpose of the business relationship

FIs must obtain information reasonably warranted by ML/TF risk, on the intended nature and purpose of the business relationship. This information should be sufficient to allow FIs to effectively monitor the customer's activity and transactions and to ensure that the account is operating in line with the intended purpose. Depending on the type of customer, the information which an FI might obtain is as follows:

- Information concerning the customers or beneficial owners business or occupation/employment
- Information on the types of financial products or services which the customer is seeking
- Establishing the source of funds in relation to the expected pattern of transactions
- Copies of the customers most recent financial statements
- Establishing any relationships between signatories and customers
- Any relevant information pertaining to related third parties and their relationship to an account
- The expected level and nature of activity that is to be undertaken through the business relationship, which may include the number, size and frequency of transactions that are likely to pass through the account.

FIs should ensure that they review any know information on the customer and monitor the transactions and activity to ensure that they understand the potentially changing purpose and nature of the business relationship.

III. CDD measures for Legal Persons and Arrangements[4]

Article 33(C) AML/CFT Law, Article 9-12 CBO Instructions, Article 12-15 Decision No. E/80/2021, Article 12- 15 Decision No. E/81/2021

In situations where a customer is a legal person or legal arrangement, FIs are obliged to identify any natural person who owns or holds a controlling interest of 25% or more. In order to achieve an effective understanding of the ownership and control structure of a customer that is a legal person or arrangement, FIs should obtain from the customer (and include in the risk profile) a detailed explanation or a company structure chart which provides details of any ownership interests of 25% or more, outlines all intermediate entities (whether legal persons or arrangements, or natural persons who are nominee stakeholders) through to the natural persons who ultimately own or control them.

FIs should take reasonable measures to identify and verify the beneficial owners by looking through each layer of legal persons or legal arrangements until the natural persons with owning or controlling interests of 25% or more in aggregate are identified. Furthermore, in the event of multiple legal persons or arrangements with ownership or controlling interests, even where each legal person or legal arrangement owns or controls less than 25%, FIs should consider whether there are indications that the entities may be related by common ownership, which could reach or surpass the beneficial ownership threshold level of 25% in aggregate. FI has to take appropriate measures to identify if the beneficial owner is Politically Exposed Person (PEP) regardless of the ownership size.

To ensure an understanding of the nature of the business of a legal person or legal arrangement, FIs should obtain and include in the profile a detailed explanation or company structure chart showing the entity's internal

[4] For more details on identifying BO refer to Beneficial owner guidelines issued by CBO and CMA.

management structure, identifying the persons holding senior management positions, or other positions of control. They should also obtain information about the legal person's or arrangement's majority-owned or controlled operating subsidiaries, including the nature of the business and the operating locations of those subsidiaries.

When undertaking CDD measures on a trust or a legal arrangements FIs should identify and take reasonable measures to verify the identity of the beneficial owners, and to understand the nature of their relationship with the legal arrangement. For customer that are trusts or other legal arrangements, the FI should identity and take reasonable measures to verify the trustee(s), managers, directors or persons in equivalent positions; settlor, founders or persons in equivalent positions, the trust or legal arrangement, including any persons settling assets into the trust or legal arrangement, the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership), or equivalent or similar positions for other legal arrangements.

For beneficiaries of trusts or other legal arrangements that are designated by characteristics or by class, the FI should obtain sufficient information concerning the beneficiary to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the payout or when the beneficiary intends to exercise vested rights.

IV. CDD measures for Life Insurance Activities

Article 16, Decision No. E/81/2021

For life or other investment-related insurance business, FIs should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary or beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiary or beneficiaries have been identified/designated:

a) For a beneficiary that is identified by name - take the name of that person;
b) For a beneficiary that is designated by characteristics, class (e.g spouse or children at the time that the insured event occurs) or by other means (e.g under a will) - obtain sufficient information on the beneficiary so that FI is satisfied that it is able to establish the identity of the beneficiary at the time of payout;

For both of the above situations, the verification of the identity of the beneficiary beneficiaries should occur prior to the payout of the policy.

If an FI determines that, a beneficiary of a policy is a legal person or legal arrangement that presents a higher risk, the licensed entity must take enhanced due diligence measures and take reasonable measures to identify and verify the identity of the beneficial owner(s) of the beneficiary prior to the time of payout.

V. CDD measures regarding Wire Transfers

Article 46 AML/CFT Law, Article 31-40 CBO Instructions

Pursuant to the AML/CFT Law and CBO Supervisory Instructions, FIs are obliged to undertake certain CDD measures concerning wire transfers. The specific requirements are set out in detail in the above-referenced articles of the CBO Supervisory Instructions. In particular, these measures relate to the following:

- identification of the originators and beneficiaries;
- the maintenance of information in regard to the same; and
- the implementation of risk-based policies and procedures for handling the disposition of wire transfers and for taking appropriate follow-up action.

The purpose of the specific measures is to ensure that information on the originator and the beneficiary shall accompany (meaning sent at the same time but not necessarily in the same message) cross-border wire transfers at all stages of its execution.

The FI of the originator (or payer) shall ensure that the transfer of funds is accompanied by the information on the originator and beneficiary (or payee) as follows:

Information on the originator:

a) The full name of the originator
b) The purpose of the transfer
c) The originator's account number (or in absence thereof the transfer shall be accompanied by a unique transaction reference number which permits traceability of the transaction);
d) The originator's address, identification document number or customer identification number, and date and place of birth.

Information on the beneficiary:

- The name of the beneficiary (in the case of natural person – the name and surname);
- The beneficiary's account number (or in absence thereof, a unique transaction reference number which permits traceability of the transaction).

Best practice for cross-border wire transfers includes the following considerations:

Outward transfers to lower-risk jurisdictions: Conducting due diligence before executing transactions above a specific threshold based on the FI's risk assessment.

Outward transfers to higher-risk jurisdictions: Conducting enhanced due diligence (EDD) before executing any transaction to a high-risk jurisdiction.

Inward transfers from lower-risk jurisdictions: Conducting due diligence upon receiving transactions above a specific threshold, based on the FI's risk assessment, before making funds available to the customer.

Inward transfers from higher-risk jurisdictions: Conducting enhanced due diligence (EDD) upon receiving transactions from any high-risk jurisdiction before making funds available to the customer.

For domestic wire transfers, the FI of the originator is required to apply IBAN requirements as per the instructions issued by CBO.

The FI of the originator shall not execute the transfer if it has not verified the identity of the originator. The FI of the beneficiary shall not credit the beneficiary's account or make the funds available for the beneficiary if it has not conducted verification of the beneficiary's identity (this applies in situations where the identity has not been previously verified).

In situations where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, FIs may decide not to apply the above requirements in respect of the information on the originator, once the account number of the originator, or unique transaction reference number is included and the batch file contains the required information on the originator and full beneficiary information that is fully traceable in the country of the beneficiary.

The FI of the beneficiary is required to implement effective procedures to identify the received transfers that lack information about the originator or the beneficiary, in real-time or as part of the post-event monitoring process. This will include risk-based procedures for identifying cross border wire transfers that lacked the required information on the originator and/or beneficiary; determining whether to execute, return, or suspend a transfer which lacks the required originator or beneficiary information and consider filing a report with the Centre, as well as procedures related to the follow-up actions regarding these transfers, which may include restricting or terminating business relationships

An intermediary FI ensures that all information about the originator and the beneficiary accompanied with the cross-border wire transfer is transferred to the beneficiary or other intermediary provider. Should there be technical limitations that prevent the required information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the

intermediary FI shall keep a record of all the information received from the ordering FI or another intermediary FI for at least 10 years.

The intermediary FI is required to implement effective risk-based procedures to identify cross border transfers that lack information about the originator and the beneficiary,

The procedures can include defining and documenting specific AML/CFT system parameters (such as transaction value, aggregate transaction amounts at the customer level, customer risk classification, or others) which would trigger an exception to straight-through processing and require manual review and intervention. This will also include procedures for determining when to execute, reject, or suspend a wire transfer lacking required information and consider filing a Report with the Cere, as well as procedures for appropriate follow-up action.

In respect of reporting suspicions, FIs that control both the ordering and beneficiary side of a wire transfer must take into account all information from both sides in determining whether a report should be filed with the Centre. In addition to this, FIs are obliged to file an STR in any country that is affected by the suspicious wire transfer and make the relevant information available to the Centre or Financial Intelligence Unit (FIU) of that country.

Where an FI repeatedly fails to provide the required information on the originator and the beneficiary, the beneficiary's or intermediary FI, taking into consideration the risks and frequency of the violations by the FI of the originator, shall take steps, which may initially include the issuing of warnings and setting deadlines. These steps can ultimately consist of rejecting any future transactions from the FI or restricting or terminating its business relationship with that FI.

Similar requirements apply to VASPs. Originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or FI (if any) immediately and securely. Beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers. For the purposes of applying the wire transfer requirements to VASPs, all virtual asset transfers are to be treated as cross-border.

In addition to the above, as part of their ongoing account monitoring procedures, FIs should also review the purpose of wire transfers, as indicated in their description fields, for potential red-flag indicators. FIs should also have procedures in place to detect wire transfers with countries identified pursuant to Article 13(k) of the AML/CFT Law.

3.2.5 Ongoing Monitoring of the Business Relationship

Article 36, AML/CFT Law. Article 17, Decision No. E/80/2021, Article 19, Decision E/81/2021

The AML/CFT Law and Supervisory Instructions require FIs to undertake ongoing monitoring of customers including monitoring of transactions to ensure that they are consistent with the information, activities, and risk profile of the customers. FIs should ensure that they have effective and appropriate on-going monitoring policies and procedures in place relating to monitoring of transactions and customer activities, as well as the extent of monitoring required for specific categories of customers, which is demonstrative of the risk-based approach. Such policies and procedures must be in operation and adhered to by employees.

In line with a risk-based approach, in the case of customers or business relationships identified as high risk, FIs are expected to investigate and obtain more information about the purpose of transactions, and to enhance ongoing monitoring and review of transactions in order to identify potentially unusual or suspicious activities. In the case of customers or business relationships that are identified as low risk, FIs may consider monitoring and reviewing transactions at a reduced frequency.

Therefore, FIs should monitor and examine transactions against CDD information and the profile of the customer and to the extent reasonably warranted by the risk of ML/TF. Where necessary, FIs should also obtain sufficient information on the counterparties and/or other parties involved

(including but not limited to information from public sources, such as internet searches), in order to determine whether the transactions appear to be:

- **Normal** (consideration should be given as to whether the transactions are typical for the customer, for the other parties involved, and for similar types of customers);
- **Reasonable** (consideration should be given as to whether the transactions have a clear rationale and are compatible with the types of activities that the customer and the counterparties are usually engaged in);
- **Legitimate** (consideration should be given as to whether the customer and the counterparties are permitted to engage in such transactions, such as when specific licenses, permits, or official authorizations are required).

Examples of some of the methods that may be adopted by FIs for the ongoing monitoring of transactions include, but are not limited to:

- Threshold-based rules, in which transactions above certain pre-determined values, numerical volumes, or aggregate amounts are examined;
- Transaction-based rules, in which the transactions of a certain type are examined;
- Location-based rules, in which the transactions involving a specific location (either as origin or destination) are examined;
- High risk Product/Service based rule, in which the transactions involving a specific high risk product or service above certain thresholds are examined
- Customer-based rules, in which the transactions of particular customers are examined.
- Customer Behavior based, in which the behavior looks at activity in comparison to customer's historical or expected activity.

FIs may use all or any combination of the above methods, or any others that are appropriate to their particular circumstances, to effect ongoing monitoring of the business relationship. Furthermore, pursuant to the Supervisory

Instructions, the monitoring and scrutinizing of customer transactions by FIs should be conducted by way of automated systems. These automated systems should be subject to periodic review and testing to ensure their effectiveness. For customers and business relationships which have been reported as suspicious to the Centre, specific monitoring procedures should be established.

Complex, Large or Unusual Transactions:

FIs are required to examine the purpose of all complex, large or unusual transaction that have no apparent economic or lawful purpose. FIs should put in place policies and procedures to identify such transactions or patterns of transactions . Example of such transactions may include:

- Larger than the FI would normally expect based on its knowledge of the customer, the business relationship and risk profile of the customer or in the relevant industry.
- Unusual or unexpected pattern compared with the customers normal activity or pattern of transactions associated with similar customers/peers, products or services or in the industry.
- Complex compared with other similar transactions associated with similar customer types/peers, products or services, in the relevant industry and the FI is not aware of an economic rationale or lawful purpose or doubts the veracity of the information which it has been given.

Where such transactions are detected, EDD measures should be applied to assist the FI in understanding whether the transactions give risk to suspicion. Such EDD measures include, but are not limited to:

- Taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds,, acquiring further information on the customer's business to ascertain the likelihood of the customer making such transactions
- Monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. An FI may decide to monitor individual transactions where this is commensurate to the risk identified.

3.2.6 Review and Updating of CDD Information

Article 33 (e) and Article 36 AML/CFT Law. Article 13, 14 CBO Instructions, Article 16,17 Decision No. E/80/2021, Article 18,19, Decision E/81/2021

A timely review and update of CDD documentation is an important part of an effective AML/CFT compliance program. FIs are obliged to review existing records on an ongoing basis to ensure that documents, data and information collected under the due diligence process remain up to date and relevant. This is particularly important for higher risk customers. The Supervisory Instructions provide that for lower risk customers, this information may be updated on a less frequent basis. However, this only applies in cases where there is no suspicion of ML/TF.

FIs should develop internal policies, procedures and controls in relation to the periodic or triggered review and updating of CDD information. These policies and procedures should be reasonable and proportionate to the risks involved and in line with the nature and size of the business. A reassessment or recategorization of customers may be required upon material updates to CDD information and or other records gathered through a trigger event or period review. The following are examples of factors which FIs should include in such policies and procedures:

- **Circumstances, timing and frequency of reviews and updates.** Generally, FIs should establish clear rules per customer risk category with respect to the maximum period of time that should be allowed to elapse between CDD reviews and updates of customer records. Examples of circumstances that require an update of a customer's file includes: the expiry of a customer's identification documents or changes in legislation or internal procedures.
- **Triggered reviews:** FIs should also establish clear rules with respect to circumstances (trigger events) that would trigger an interim review or the expedition of a particular customer's review cycle. These trigger events should be reviewed on a regular basis by the FI and examples revised where appropriate. Targeted training should also be provided to employees on how

to identify and interpret possible trigger events. Circumstances or events that might trigger an interim review include[5]:

- Discovery of information about a customer that is either contradictory or casts doubt on the appropriateness of the customer's existing risk classification or the accuracy of previously gathered CDD information;
- Material change in ownership, legal structure, or other relevant data (such as name, registered address, purpose, capital structure) of a legal person or arrangement;
- Initiation of legal or judicial proceedings against a customer or Beneficial Owner;
- Materially adverse information regarding a customer or Beneficial Owner, such as media reports about allegations or investigations of fraud, corruption or other crimes;
- Qualified opinion from an independent auditor on the financial statements of a legal entity customer;
- Transactions that indicate potentially unusual or suspicious transactions or activities.

- **Elements of and extent of reviews and updates.** FIs should clearly define the timelines, extent and elements involved in CDD reviews for Business Relationships in different risk categories. This should include which data elements, documents, or information should be examined and updated if necessary. In this regard, FIs are advised that tools such as checklists and procedural manuals will help to enhance the effectiveness of CDD reviews and updates. Examples of procedures might include, but are not necessarily limited to:

  – When the source of wealth or the source funds of a customer should be verified;

[5] FIs should note that these are just examples of trigger events. Furthermore, FIs should be aware that definitive lists of trigger events may lead to complacency within the FI, as employees may not be open to considering suspicious activity outside of the listed triggers. Therefore, FIs should list examples of triggers which should provoke staff to 'think outside the box'.

- When additional inquiries or investigations should be made pertaining to the nature of a customer's business, the purpose of a Business Relationship, or the reasons for a transaction;
- How much of a customer's transactional history, including how many and which specific transactions or transaction types, should be reviewed as part of a periodic or an interim review.

- **Internal responsibilities:** Policies and procedures should contain details in respect of arrangements in relation to the CDD review and update process within the FI. Examples of such responsibilities might include, but are not necessarily limited to:

  - Conducting reviews and updates;
  - Escalating and/or reporting situations in which risk classifications should be changed, Business Relationships should be suspended or terminated, or potentially unusual or suspicious activities should be further investigated;
  - Approving or rejecting reviews of Business Relationships (including senior management involvement with regard to PEPs and other High Risk Customers);
  - Undertaking CDD file remediation measures when necessary;
  - Auditing the quality of CDD reviews and updates;
  - Maintaining records with regard to CDD reviews and updates, in accordance with statutory record-keeping requirements

3.2.7 Enhanced Due Diligence (EDD Measures)

Article 34 (b) AML/CFT Law. Article 2 CBO Instructions. Annex 2 CBO Instructions, Articles 3(6) and 4 Decision No. E/80/2021, Article 3(6) and 4 Decision

FIs are required to enhance their CDD measures in situations where the FI has determined that customers or business scenarios present a higher level of ML/TF risk to manage and mitigate those risks appropriately. EDD measures

cannot be substituted for regular CDD measures but must be applied in addition to regular CDD measures. FIs should apply risk proportionate levels of EDD measures which are commensurate to the with ML/TF risks identified. The AML/CFT Law and Supervisory Instructions prescribe a number of circumstances in which FIs are required to apply EDD measures:

a) Non-Face to Face Business Relationships or transactions
b) Politically Exposed Persons (PEPs)
c) Correspondent relationships
d) High-Risk Countries
e) Any other situation that the FI has identified as being of higher risk

Examples of such measures include:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to customer identity;
- More detailed examination of the nature and purpose of the business relationship, nature of the customers business, source of funds and source of wealth and purpose of individual transactions
- Enhanced level of ongoing monitoring of the business relationship, including more frequent review and updating of customer due diligence information and senior management approval

As part of EDD, FI's should consider obtaining further information, documentation and evidence regarding the customer and the customers business such as:

- Source of fund and source of wealth
- Occupation and type of business
- Financial statements and banking references
- Description of the customer's primary trade area and whether international transactions are expected to be routine;
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers; and
- Explanations for changes in account activity.

- Require first payment to be carried out through an account in the customer's name with a financial institution subject to similar CDD standards

In situations where an FI has doubts about the accuracy of a customer's ML/TF risk classifications, EDD measures should be applied to determine the appropriate risk profile. Furthermore, EDD should be applied where there are red flag indicators of potentially unusual or suspicious transactions or activities.

FIs should develop and implement risk based policies and procedures in controls in respect of EDD measures. Such policies and procedures should be proportionate to the nature and size of the FI's business and the risks identified.

Examples of components which such be addressed in the policies and procedures include:

- ML/TF risks as identified in the ML/TF business risk assessment
- Nature of the EDD measures to be applied
- Circumstances, and timing, of application of EDD measures;
- Frequency of reviews and updates in relation to information on high-risk customers;
- Extent and frequency of ongoing monitoring of the Business Relationship and monitoring of transactions in relation to high-risk customers

I. EDD in relation to Politically Exposed Persons (PEPs)

Individuals who have or have had a high political profile or hold, or have held political office have the potential to be vulnerable to corruption and therefore politically exposed persons (PEPs) are classified as high-risk individuals from an AML/CFT perspective. Article 36 of the AML/CFT Law defines a PEPs as:

1. *"Any natural person currently or formerly appointed to a prominent position in the Sultanate of Oman or a foreign country, members of their family and close associates.*
2. *Any person currently or formerly appointed to a prominent position in an international organization, members of their family and close associates."*

This definition of a PEP is expanded in the Supervisory Instructions to include:

any natural person, whether as customer or beneficial owner, including but not limited to;

i. who is or was entrusted with a prominent public function in the Sultanate of Oman or in a foreign country, such as Head of States or of governments,
ii. senior politicians,
iii. senior government employee,
iv. Senior judicial or military officials,
v. senior executives of state owned corporations,
vi. important political party officials;
vii. With a prominent function by an international organization, such as directors, deputy directors and members of the board.

The term also includes close associates and family members of a politically exposed person which include widely and publicly known close business colleagues or personal advisors or any persons who are in position to benefit significantly from close business associations with the politically exposed person.

FIs are required to implement appropriate risk management systems to determine whether a customer, beneficial owner, beneficiary or controlling person is a PEP. In this respect, and in line with the nature and size of their business, FIs should take the following (non-exhaustive) measures:

- Implement automated AML/CFT screening systems which screen customer and transaction information for matches with known PEPs;
- Conducting background checks as part of CDD procedures using tools such as manual internet search protocols; public or private databases; publicly

accessible or subscription information services; commercially available background investigation services.

If a customer has been identified as a PEP, the following enhanced CDD measures should be applied by the FI;

- Take reasonable measures to determine the **source of funds and the source of wealth.** FI's should at least consider the activities that have generated the total net worth of the customer (activities that produced the customer's funds and property) and the origin and means of transfer for funds that are involved in the transaction. FIs should also evaluate the legitimacy of the source of funds and source of wealth, which may include making reasonable investigations into the individual's professional and financial background.

- **Enhanced ongoing monitoring** of the relationship. FIs should regularly review the information which is held on PEP customers to ensure that any new or emerging information that could affect the risk assessment is identified in a timely manner. The frequency of such ongoing monitoring should be determined by the FI commensurate with the higher risk associated with the PEP relationship.

- **Obtain senior management approval** before establishing or continuing an existing business relationship. In this respect, senior management should be notified and their approval obtained each time any of the following situations occur:
    a. An existing customer becomes, or is newly identified as, a PEP;
    b. An existing PEP business relationship is reviewed and the CDD information is updated, either on a periodic or an interim basis, according to the FIs internal policies and procedures;
    c. A material transaction that appears unusual or does not follow a similar pattern is identified in relation to a PEP;
    d. The beneficiary or beneficial owner of a life insurance policy or family takaful insurance policy is identified as a PEP, and in which case higher risks are identified, the overall business relationship should also be thoroughly examined and consideration given to

filing an STR. Senior management should be informed before the payout of the policy proceeds.

When considering whether to approve a PEP relationship, FIs should take into consideration:

- The level of ML/TF risk that the FI would be exposed to upon entering the relationship
- The resources which would be required in order to mitigate the risk effectively.

When considering whether to enter into or continue a business relationship with a PEP, FIs should ensure that

- The matter is discussed at senior management level
- The corresponding ML/TF risks are acknowledged
- The rational for the decision is documented

Customers who are no longer a PEP: The management of a customer who no longer holds a prominent public function should be based on an assessment of risk by the FI and take action to mitigate this risk. This is demonstrative of the risk-based approach. Possible risk factors which the FI might consider are as follows:

- The level of (informal) influence that the individual could still exercise;
- the seniority of the position that the individual held as a PEP; or
- whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

FIs should note that the CBO Supervisory Instructions provide that the obligations apply in respect of foreign PEPs only. In relation to domestic PEPs and persons who have been entrusted with a prominent function by an international organisation, the Supervisory Instructions provide that FIs should implement these additional measures only in cases where there is a higher risk associated with the business relationship. The CMA Instructions requires that the measures are applied equally to foreign, domestic and international PEPs.

Internal Policies and Procedures should be implemented by the FI which include the following:

- How PEP relationships will be identified by the FI
- Procedure to be followed when a customer is identified as a PEP at onboarding
- Procedure to be followed when a customer becomes a PEP during the business relationship
- Nature and extent of EDD measures to be taken

For CBO supervised institution, CBO's *"Guidelines on PEPs and persons with prominent public functions*" provide in-depth explanation and the obligations apply in respect of all the aspects mentioned above

II. EDD requirements for Correspondent Relationships

Correspondent relationships include correspondent relationships between banks and between banks and other financial institutions, including relationships established for securities transactions or funds transfers. Where a correspondent institution processes and executes transactions on behalf of customers of a respondent institution, the correspondent institution often faces a heightened level of ML/TF risk due to the correspondent institution not having a direct relationship with the customer of the respondent institution. As a result, FIs are obliged to fulfil certain due diligence requirements with regard to the correspondent banking relationships which they maintain, regardless of whether these involve foreign or domestic financial institutions.

In accordance with the AML/CFT Law and Supervisory Instructions, FIs are prohibited from entering into or maintaining correspondent relationships with shell banks, or with institutions that allow their accounts to be used by shell banks. The AML-CFT Law defines a shell bank as a "bank that has no physical presence in the country or the region where it is established and licensed, and is not affiliated to any financial group which is subject to an effective unified regulation and supervision.

The enhanced measures which FIs are obliged to take in respect of correspondent relationships include:

- Gathering sufficient information about any respondent institution for the purpose of identifying and achieving a full understanding of the nature of its business, and to determine, through publicly available information, its reputation and level of AML/CFT controls, including whether it has been subject to a ML/FT investigation or regulatory action.
- Evaluating the AML/CFT controls which are implemented by the respondent institution.
- Obtaining the approval from senior management before establishing new correspondent relationships.
- Ensuring the performance of the full range of CDD obligations by the respondent institution on its customers that have direct access to third party payment accounts of the correspondent financial institution.
- FIs are obliged to understand the responsibilities of each institution in the field of combating the crimes of money laundering, the financing of terrorism and of illegal organisations.

FI should be aware at all times that regulatory and supervisory environments governing the operation of financial institutions around the world vary greatly. Thus, not all foreign financial institutions are subject to the same AML/CFT requirements as FIs in Oman and as a consequence, some of these foreign institutions may pose a higher ML/FT risk. To mitigate against these risks, FIs that maintain correspondent relationships with foreign financial institutions should consider implementing adequate procedures to assess and periodically review the relevant regulatory and supervisory frameworks of the countries concerned.

Furthermore, when gathering information about financial institutions with which they maintain correspondent relationships, whether foreign or domestic, FIs should take appropriate steps to assess the nature, size and extent of their businesses in the countries where they are incorporated and licensed, as well as their ownership and management structures (taking into consideration the nature and extent of any PEP involvement), in order to evaluate whether they exhibit the characteristics of shell banks, and whether they offer downstream correspondent services (also known as “nested accounts”) to other banks. If they do offer downstream correspondent services, FIs should also take

reasonable steps to understand the types of services offered, the number and types of financial institutions they are offered to, the types of customers those institutions serve, and to identify the associated ML/FT risk issues.

In order to collect sufficient information about the nature of a financial institution and the AML/CFT controls it applies, and to assess the ML/TF risks associated with it, FIs should take appropriate measures such as (for example) implementing a suitable correspondent relationships questionnaire and, when necessary, conducting follow-up interviews. (FIs may find the correspondent banking questionnaire which has been developed by the Wolfsberg Group, as well as the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking, instructive in this regard. FIs should also ensure that the correspondent entity meets AML/CFT requirements and applies due diligence and record keeping requirements in line with the AML/CFT Law and its Regulations, and it should also consider the country risk of the correspondent entity.

FIs should periodically review and update their due diligence information in relation to the financial institutions with which they maintain correspondent relationships, commensurate with the risks involved. In the event of a deterioration in the risk profile of a financial institution with which a correspondent relationship is maintained, including the discovery of material adverse information concerning the institution, FIs should ensure that senior management is informed and appropriate risk-based measures are taken to assess and mitigate the ML/FT risks involved.

FIs should also maintain agreements or contracts with financial institutions with which they maintain correspondent relationships. In addition to operational details concerning the products and services covered, these agreements should clearly describe each party's responsibilities in regard to ML/FT risk mitigation, due diligence procedures, and the detailed conditions related to any permitted third-party usage of the correspondent account.

III. EDD Requirements for High-Risk Countries

Pursuant to the AML/CFT Law and supervisory instructions, FIs are obliged to apply risk-based and enhanced due diligence measures that are commensurate with the ML/TF risks associated with transactions and business relationships with customers from high risk countries, including natural and legal persons and financial institutions, and those acting on their behalf. High-risk countries are

considered to be those countries which are subject to a call for Action and jurisdictions under increased monitoring (grey list) which have been identified by FATF and those countries identified by the National Committee for combatting money laundering and terrorism financing. Due diligence measures taken by FIs, must always be proportionate to the risks arising from business relationships and transactions with natural or legal persons of such countries and be sufficiently effective to mitigate such risks.

FIs should regularly check the Committee's homepage and other credible sources such as the FATF list of High-Risk Jurisdictions subject to a Call for Action and Jurisdictions under Increased Monitoring, UN website and any circulars issued by CMA and CBO.

Below is a non-exhaustive list of EDD measures which an FI may decide to take to mitigate the ML/TF risk associated with high risk countries:

- Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to the identity of customers, Beneficial Owners, beneficiaries and other controlling persons;
- Seeking further documentation on and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions.
- Increased investigation to ascertain whether the customers or related persons (beneficial owners, beneficiaries and other controlling persons, in the case of legal persons and arrangements) are foreign PEPs;
- Increased supervision of the business relationship, including the requirement for higher levels of internal reporting and management approval, more frequent monitoring of transactions, and more frequent review/ updating of customer due diligence information

Additionally, FIs are obliged to implement all specific CDD measures and countermeasures regarding High Risk Countries as defined by the National

Committee for Combating Money Laundering and the Financing of Terrorism, including those related to the implementation of the decisions of the UN Security Council under Chapter VII of the Charter of the United Nations, and other related directives, and those called for by the Financial Action Task Force (FATF) and/or other FSRBs.

In order to fulfil these obligations, and commensurate with the nature and size of their businesses and the risks involved, FIs should establish adequate internal policies, procedures and controls in relation to the application of EDD measures and risk-proportionate effective countermeasures to customers and business relationships associated with high-risk countries.

Some of the factors to which FIs should give consideration when formulating such policies, procedures and controls, include but are not limited to the following:

- The organisation's risk appetite with respect to business relationships involving high-risk countries;
- Methodologies and procedures for assessing and categorising country risk, and identifying high-risk countries, including the statutorily defined High Risk Countries as established by the Committee, and taking into consideration advice or notifications of concerns about weaknesses in the AML/CFT system of other countries issued by the relevant Supervisory Authorities and/or Competent Authorities;
- Determination and implementation of appropriate risk-based controls (for example, certain product or service restrictions, transaction limits, or others) with regard to customers and Business Relationships associated with high-risk countries;
- Organisational roles and responsibilities in relation to the monitoring, management reporting, and risk management of high-risk country Business Relationships;
- Appropriate procedures for the enhanced investigation of Business Relationships involving high-risk countries in relation to their assessment for possible PEP associations;

- Independent audit policies in respect of EDD procedures pertaining to customers/Business Relationships involving high-risk countries and the business units that deal with them.

FIs should note that for all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply EDD, and in the most serious cases, countries are called upon to apply countermeasures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing risks emanating from the country. Specific countermeasures which need to be applied by FIs shall be advised by the Committee trough decision 3/2022 which mandates the following:-

1- Apply enhanced due diligence measures proportionate to the risks involved with all business relationships and transaction with persons from high risk countries including natural and legal persons, FIs or any one acting on their behalf.

2- Enhance internal reporting mechanism with regard to monitoring transactions and business relationships with high risk countries and report to NCFI when suspicion raise.

3- Shall not rely on third partied located in high risk countries to conduct elements of the CDD process.

4- Apply Targeted Financial Sanctions according to related UN decisions.

IV. Other situations that the FI has identified as being of higher risk

Article 34(b), Article 41 AML/CFT Law, Article 5, Article 22, Decision No. E/80/2021, Article 5, Article 24, Decision E/81/2021,

FIs are obliged to apply EDD measures to manage and mitigate the risk associate with high risk situations such as high risk customers and high risk transactions. In all such situation, FIs should take an informed decision about which EDD measures are appropriate for each high risk situation. For example, in certain high-risk situations, an FI may consider it appropriate to focus on enhanced ongoing monitoring during the business relationship as opposed to applying other EDD measures.

A list of examples of EDD measures that should be taken in such situations are contained in the Supervisory Instructions and include:

- Performing background checks (among other via internet searches, public databases, or subscription information aggregation services) to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information;
- Using more rigorous methods for the verification of the customer's or beneficial owner's identity
- Seeking more information on the intended nature and purpose of the business relationship such as the number, size and frequency of transactions that are likely to pass through the account, the destination of the funds, the reason as to why the customer is looking for a particular product or service.
- Reviewing the business relationship on a more frequent basis and conducting more in depth transaction monitoring.

When carrying out such measures (especially as regards acquiring and investigating more information about the nature of the customer's business, purpose of the Business Relationship, or reason for the transaction), FIs should pay particular attention to the reasonableness of the information obtained, and should evaluate it for possible inconsistencies and for potentially unusual or suspicious circumstances. Examples of factors that FIs should take into consideration in this regard include, but are not limited to:

- A reason for a foreign customer's or Beneficial Owner's presence, or establishment of a Business Relationship, in Oman without good rationale;
- Consistency between the nature of the customer's business and transactions and the customer's or Beneficial Owner's professional background and employment history (FIs may find it helpful to obtain background information from reliable and independent sources, as well as from internet and social media searches)
- The level of complexity and transparency of the customer's transaction especially in comparison with the customer's or Beneficial Owner's educational and professional background;
- The level of complexity and transparency of the customer's legal structure of legal persons or arrangements;
- The nature of any other business interests of the customer or Beneficial Owner, including any other legal persons or arrangements owned or controlled;
- Consistency between the customer's line of business and that of the counterparty to the customer's transactions (as identified, for example, through internet searches).

Additionally, and commensurate with the nature and size of their businesses, when carrying out EDD measures in respect of High Risk Customers, FIs should take appropriate risk-mitigation measures such as, but not limited to:

V. EDD Requirements for Non-Profit Organisations

Non-Profit Organisations (NPOs) can often pose increased risks with respect to ML and TF. As part of an effective risk-based approach to AML/CFT, FIs that enter into or maintain business relationships with NPOs should take adequate CDD measures that are commensurate with the risks involved.

Examples of measures that FIs should consider include, but are not limited to:

- Ensuring that the NPO is properly licensed or registered;

- Obtaining information about and assessing the adequacy of the NPO's AML/CFT policies, procedures and controls;

- Obtaining sufficient information about the NPO's legal, regulatory and supervisory status, including requirements relating to regulatory disclosure, accounting, financial reporting and audit (especially where community/social or religious/cultural organisations are involved, and when those organisations are based, or have significant operations, in jurisdictions that are unfamiliar or in which transparency or access to information may be limited for any reason);

- Obtaining sufficient information about the NPO's ownership and management structure (including taking into consideration the possibility of PEP involvement); the nature and scope of its activities; the nature of its donor base, as well as of that of the beneficiaries of its activities and programmes; and the geographic areas in which it operates, so as to be in a position to identify, assess, and manage or mitigate the associated ML/FT risks;

- Performing thorough background checks (including but not limited to the use of internet searches, public databases, or subscription information aggregation services) on the NPO's key persons, such as senior management, branch or field managers, major donors and major beneficiaries, to screen for possible matches with targeted and other international financial sanctions lists, indications of criminal activity (including financial crime), or other adverse information.

FIs that have business relationships with NPOs should implement a risk-based approach to determine the appropriate internal AML/CFT policies, procedures and controls the FIs implement in relation to the risk assessment, risk classification, and the type and extent of CDD they perform on NPOs. The policies and procedures that FIs apply should be reasonable and proportionate to the risks involved, and should be adequately documented, approved by senior management and communicated to the relevant employees of the organisation.

3.2.8 Simplified Due Diligence (SDD) Measures

Article 34(b), AML/CFT Law, Article 3, CBO Instructions, Article 6, 7 Decision No. E/80/2021, Article 6,7 Decision E/81/2021,

In situations where an FI has identified a lower risk, or pursuant to Article 40 of the AML/CFT Law a where a supervisory authority and the Centre have identified low risk situations, FIs are permitted to apply simplified due diligence measures. SDD is not an exemption from any of the CDD measure, rather FIs may adjust the amount, timing or type of each or all of the CDD measures in a way that is commensurate to the low risk they have identified. Therefore, SDD can only be applied by FIs following an adequate assessment of ML/TF risks.

SDD generally involves a more lenient application of certain aspects of CDD measures.

For *Banks, FLCs, PSP's and MEEs*, the following examples of SDD measures has been identified by CBO:

- Verifying the identity of the customer and beneficial owner after the establishment of the business relationship
- Reducing the frequency of customer identification updates
- Reducing degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

For *Capital Markets Companies* the following examples of SDD measures has been identified by CMA:

- Obtaining the relevant identification data from a public register, from the customer or from other reliable sources.

- Verifying the identity of customer and beneficial owner after establishment of the business relationship.
- Reducing frequency of customer identification updates.
- Reducing degree of on-going monitoring and scrutinizing transactions.
- Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

The same examples of SDD measures are applicable to the *Insurance sector* as the Capital Markets, with the following additional example provided:

- Postponing the identification of the beneficiary to a later time after their designation.

For *Banks, FLCs PSPs and MEEs*: the application of SDD may be permitted in the following situations:

Low risk customers:

- FIs or DNFBPs that are subject to AML/CTF requirements which are consistent with the FATF requirements, have effectively implemented those requirements and are effectively supervised with to ensure compliance with those requirements
- Public companies which are listed on a stock exchange and subject to disclosure requirements (either by law, or stock exchange rules or other binding instructions), which impose requirements to ensure adequate disclosure of beneficial ownership.
- Public administration or enterprises.

Products, services, transactions or delivery channels:

- A pension, superannuation or similar schemes that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme.
- Financial products or services that are of a limited nature that are provided to a certain category of customer for financial inclusion purposes, with the prior approval of the CBO.

For *Capital Market Institutions* the application of SDD may be permitted in the following situations:

Low risk customers:

- FIs or DNFBPs that are effectively supervised or monitored to ensure compliance with the requirements of the law.
- Companies listed on the stock exchanges of countries with disclosure requirements consistent with international standards, to ensure adequate transparency of their subsidiaries or the subsidiaries of the beneficial owner.
- Public enterprises.

Country or geographical area risk factors:

- Countries classified by credible sources as having effective systems to combat money laundering and financing of terrorism.
- Countries classified by credible sources as having a low level of corruption or other criminal activity.

Product, service, transaction or delivery channel risk factors:

- Where cash withdrawals are not permitted.
- Where redemption or withdrawal of proceeds are not permitted to be paid to another party.
- Where it is not possible to change the characteristics of products or accounts at a future date to enable payments to be received from, or made to, other parties.

For *Insurance companies* the application of SDD may be permitted in the following situations:

Customer Risk Factors:

- Long business relationship with customer with track record of regular premium payments in line with customer profile and source of funds.
- Customer was directly identified and on boarded by licensed entity, without involvement of other party intermediaries.

- Financial institutions or non-financial businesses and professions that are effectively supervised or monitored to ensure compliance with the requirements of the law.
- Companies listed on the stock exchanges of countries with disclosure requirements consistent with international standards, to ensure adequate transparency of beneficial ownership, or majority-owned subsidiaries of such companies.
- Public administrations or enterprises.

Country or geographical risk factors:

- Countries classified by credible sources as having effective systems to combat money laundering and financing of terrorism.
- Countries classified by credible sources as having a low level of corruption or other criminal activity.

Product, service, transaction or delivery channel risk factors:

- Where cash withdrawals are not permitted.
- Where redemption or withdrawal of proceeds are not permitted to be paid to other party.
- Where it is not possible to change the characteristics of insurance products or policies at a future date to enable payments to be received from, or made to, other parties.
- Insurance products that provide benefits similar to retirement to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of members' interests under the scheme.
- Insurance benefit only pays out against a pre-defined event or date.
- No surrender value.
- Low, regular premium payments.
- No other party payment facility.
- No early surrender option.
- Total investment is curtailed at low value.

FIs should be aware that SDD measures are not permitted in situations where there is a suspicion of ML/TF or where a specific higher risk situation applies. Furthermore, when applying SDD measures, FI's should obtain sufficient information to satisfy themselves that their assessment that the ML/TF risk associated with the business relationship or transaction is low, is justified.

As part of their overall AML/CFT framework, FIs should use a risk-based approach to determine the internal policies, procedures and controls they implement in connection with the application of SDD procedures. Examples of some of the factors they should consider when developing their risk-based policies include:

- the ML/TF risks identified in the ML/TF business risk assessment, especially with regard to low-risk categories of customers;
- Circumstances, timing, and composition in regard to the application of SDD measures;
- Frequency of reviews and updates in relation to customer SDD information;
- Extent and frequency of ongoing supervision of the Business Relationship and monitoring of transactions in relation to customers to which SDD measures are applied.

Such policies, procedures and methodologies should be reasonable and proportionate to the risks involved, and, in formulating them, FIs should consider the results of both the NRA, Sectorial risk assessment and any Topical Risk Assessment and their own ML/TF business risk assessments. Commensurate with the nature and size of the FI's businesses, the policies, procedures and methodologies should also be documented, approved by senior management, and communicated at the appropriate levels of the organisation.

3.2.9 Third Party Reliance

Article 45 CBO Instructions, Article 35
Decision No. E/80/2021, Article 37
Decision E/81/2021

Pursuant to the Supervisory Instructions, there are certain situations where FI's are permitted to rely on third party to undertake the following CDD measures:

- Identify and verify the customer
- Identify the beneficial owner and verify the beneficial owner, as appropriate
- Obtain information on the intended nature and purpose of the business relationship

Should an FI place reliance on a third party to conduct the above CDD requirements, a number of conditions have been set out in the Supervisory Instructions which FIs are obliged to comply with:

- Immediately obtain all necessary information on the identity of the customer and/or beneficial owner and/or the purpose and intended nature of the business relationship as required under the AML/CFT law and supervisory instructions. This includes the identification and verification of the identity of customers and beneficial owners, beneficiaries or controlling persons of legal entities or arrangements, as well as the investigation and assembly of other relevant customer documents, information and data, as per the statutory CDD and record-keeping requirements.
- Copies of the identification data and other relevant documentation relating to customer due diligence requirements must be made available from the third party upon request and without delay;
- The third party must be regulated and supervised for and has measures in place for compliance with customer due diligence and record keeping requirements in line with the obligations stipulated in the AML/CFT Law and Supervisory Instructions. For FIs that rely on third parties that are part of the same financial group, they may consider that the third party relied upon meets the requirements under the supervisory instructions, provided the group applies due diligence and record keeping requirements in line with the AML/CFT and supervisory Instructions, the implementation of such requirements is supervised at the group level by a competent authority, and any higher country risk is adequately

mitigated by the group's policies and controls. In determining in which countries the third party may be based, FIs should have regard to all of the information which is available on the level of country risk, including those high risk countries which are identified by the Committee and the specific measures which are required in such instances.

FIs that place reliance on third parties to undertake CDD measures on their behalf should implement adequate measures, in keeping with the nature and size of their businesses, to ensure the third party's adherence to the requirements of the AML/CFT Law and the Supervisory Instructions in relation to CDD measures.

Examples of such non-exhaustive measures include:

- Putting in place a service-level agreement with clear provision which sets out the roles and responsibilities of the FI and the third party and specifying the nature of the CDD and record-keeping requirements to be fulfilled, having consideration of the specific requirements outlined above.
- The implementation by the FI of clearly defined policies and procedures which set out an approach for determining the adequacy of a third-party's CDD and record-keeping measures, including the evaluation of such factors as the comprehensiveness and quality of its AML/CFT policies, procedures and controls; the number of personnel dedicated to CDD; and its audit and/or quality assurance policies in regard to CDD. In this regard, FIs are advised that tools such as questionnaires, scorecards, and on-site visits may be useful in evaluating the adequacy of a third party's adherence.

- The FI should conduct regular assurance testing to ensure documentation can be retrieved from the third party without undue delay and the quality of the underlying documentation is sufficient.

FIs should be aware that at all times, ultimate responsibility for compliance with CDD obligations and third party requirements rests with the FI. Furthermore, FIs should themselves assess the risks of the customer, including the customer's risk profile. FIs should thus document their rationale for the assignment of relevant customer risk classifications, as well as their analysis of the CDD information obtained from the third parties. Moreover, FIs remain themselves responsible for conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship. FI's must ensure that in placing such reliance, it can meet its obligations under the AML/CFT Law and Supervisory Instructions.

3.3 Suspicious Transaction Reporting

Article 47 AML/CFT Law. Article 41 CBO Instructions, Article 32 Decision No. E/80/2021, Article 34 Decision E/81/2021

Suspicious Transaction Reports ("STRs") play a pivotal role in the fight against ML and TF. Information provided in STRs assist Omani Law Enforcement Authorities in their investigations, resulting in the disruption of criminal and terrorist activities. STRs also provide authorities with valuable market intelligence on trends and typologies.

Under the AML/CFT legal and regulatory framework of Oman, all FIs are obliged to immediately[6] notify the NCFI if they suspect or have reasonable grounds to suspect that the funds are the proceeds of crime, or are related to terrorism financing. When assessing potential suspicious transactions, FIs should consider attempted transactions as well as completed transactions. Suspicious transaction reports include all relevant information, documentation and records

[6] For CBO supervised institutions, notification shall occur as soon as possible but no later than 48 hours in the case of forming a suspicion or having reasonable grounds to suspect. For CMA supervised institutions, reporting shall occur as soon as possible but no later than 24 hours after forming a suspicion or having reasonable grounds to suspect.

relating to the transaction, customer or account involved and must comply with the procedures and requirements which are set out by the NCFI. To fulfil these obligations, FIs should implement adequate internal policies, procedures and controls in relation to the identification and the immediate reporting of suspicious transactions. The following sub-sections provide additional guidance in this regard.

3.3.1 Meaning of Suspicious Transaction

Pursuant to the AML/CFT Law and Supervisory Instructions, a suspicious transaction refers to any transaction, attempted transaction, or funds which an FI has reasonable grounds to suspect as constituting—in whole or in part, any of the following:

- The proceeds of crime (whether designated as a misdemeanour or felony, and whether committed within the State or in another country in which it is also a crime);
- Being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations;
- Being intended to be used in an activity related to such crimes.

FIs should note that there is no minimum monetary threshold for reporting and no amount should be considered too low for suspicion. This is particularly important when considering potential terrorist financing transactions which often involve very small amounts of money.

It should be noted that the only requirement for a transaction to be considered as suspicious is “reasonable grounds” in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators, behavioural patterns, or customer due-diligence (CDD) information. It is not dependent on obtaining evidence that a predicate offence has actually occurred or on proving the illicit source of the proceeds involved. FIs are not required to have knowledge of the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; reasonable grounds are sufficient.

FIs should also note that transactions need not be completed, in progress or pending completion in order to be considered as suspicious. Attempted transactions, transactions that are not executed and past transactions,

regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

3.3.2 Identification of suspicious transactions

When making a determination of suspicion, FIs should consider their specific products, and services and the customers in the context of their risk profile, as what might be considered suspicious for one product, service or customer may not be for another. For this reason, clear internal policies and procedures with regard to alert escalation and investigation, and internal suspicious transaction reporting are critical to an effective ML/TF risk-mitigation programme. This includes an adequate training program that will allow staff to detect possible unusual or suspicious transactions.

FIs should note that the presence of an indicator or red flag may not always mean that a transaction *is* suspicious, however, it does require that a transaction is immediately assessed to determine whether the transaction needs to be reported to the NCFI. When investigating alerts it is important to examine the customer's earlier and related transactions.

Below are some non-exhaustive examples of potentially suspicious transaction types that FIs should take into consideration:

- Transactions or series of transactions that appear to be unnecessarily complex, that make it difficult to identify the beneficial owner, or that do not appear to have an economic or commercial rationale;
- Numbers, sizes, or types of transactions that appear to be inconsistent with the customer's expected activity and/or previous activity;
- Transactions that appear to be exceptionally large in relation to a customer's declared income or turnover;
- Large unexplained cash deposits and/or withdrawals, especially when they are inconsistent with the nature of the customer's business;
- Loan repayments that appear to be inconsistent with a customer's declared income or turnover;
- Early repayment of a loan followed by an application for another loan;
- Third-party loan agreements, especially when there are amendments to or assignments of the loan agreement;

- Requests for third-party payments, including those involving transactions related to loans, investments, or insurance policies;
- Transactions involving high-risk countries, including those involving "own funds" transfers, particularly in circumstances in which there are no clear reasons for the specific transaction routing;
- Frequent or unexplained changes in ownership or management of Business Relationships;
- Illogical changes in business activities, especially where high-risk activities are involved;
- Situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide CDD documentation, or provide documentation that is false, misleading, fraudulent or forged.
- Purchases of Insurance products that appear outside the normal wealth range of a customer.
- Refunds request during a life policy's cancellation period of free-lock period.
- The customers' account shows unexplained high level of activity with very low levels of securities transactions.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfer

As part of their overall AML/CFT framework, and commensurate with the nature and size of their businesses, FIs should determine the internal policies, procedures and controls they apply in connection with the identification and evaluation of potentially suspicious transactions.

FIs should ensure that they have an adequate process and dedicated, experienced employees for the investigation of and dealing with alerts. The investigation of alerts and the conclusion of the investigation should be documented, including the decision to close the alert or to promptly report the transaction as suspicious.

The prompt filing of an STR to the NCFI is one of the key elements of the AML/CFT process. This means that FIs must immediately report the transaction to the NCFI once the suspicious nature of the transaction becomes clear. This

will be the case when from an objective point of view, taking the available information into account, there is a reason to believe that a transaction is suspicious. This means that FIs quickly investigate alerts and possible indications of ML/TF and immediately report the transaction upon determining that the transaction should be reported to the NCFI. FIs therefore need to able to show that from the moment of the alert immediate and continuous action has been taken. In this respect, FIs must have a procedure in place that defines the reporting process, and what steps to take in such cases.

3.3.3 Internal Procedures for Reporting Suspicious Transactions

As part of their overall risk-based AML/CFT framework and commensurate with the nature and size of their businesses, FIs should establish appropriate policies, procedures and controls pertaining to the internal reporting by their employees of potentially suspicious transactions, including the provision of the necessary records and data, to the designated AML/CFT compliance officer for further analysis and reporting decisions, as well as to the reporting of STRs to the NCFI. The relevant policies, procedures and controls should take into consideration such factors as:

- Organisational roles and responsibilities with respect to the implementation and review/updating of the relevant indicators;
- Operational and IT systems procedures and controls in connection with the application of relevant indicators to processes such as transaction handling and monitoring, customer due diligence measures and review, and alert escalation;
- Employee training in relation to the identification and reporting of suspicious transactions (including attempted transactions), the appropriate use and assessment of the relevant indicators, and the degree and extent of internal investigation that is appropriate prior to the reporting of a suspicious transaction.
- Operational procedures including conditions, timeframes, and methods for filing internal potentially suspicious transaction reports;
- Content requirements and format of internal potentially suspicious transactions;
- Appropriate controls for ensuring confidentiality and the protection of data from unauthorized access

- Procedures related to the provision of additional information, follow-up actions pertaining to the transactions, and the handling of Business Relationships after the filing of STRs;
- Policies and procedures for the analysis and decision-making of suspicious transactions by the compliance officer in regard to reporting to the NCFI.
- Other conditions deemed appropriate by the AML/CFT compliance officer.

Such policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation, in keeping with the nature and size of the FI's business.

3.3.4 Timing of Suspicious Transactions Reports

Under the AML/CFT legal and regulatory framework of Oman, all FIs are obliged to immediately notify the Centre if they suspect or have reasonable grounds to suspect that the funds are the proceeds of crime, or are related to terrorism financing. Without prejudice to the above, FIs should note that some potentially suspicious transactions or indicators of suspicion may require a degree of internal investigation before a suspicion or reasonable grounds for suspicion are established. The FI should however be able to demonstrate that this investigation is started immediately and has been ongoing continuously until the transaction is reported to the NCFI. The CMA supervisory Instructions require reports to be filed as soon as possible and no later than 24 hours after the forming of the suspicion or having reasonable grounds to suspect that any transaction or attempted transaction involves the proceeds of crime or funds related to financing of terrorism. For CBO supervised entities, the requirement to file an STR is no later than 48 hours.

In this regard, and commensurate with the nature and size of their businesses, FIs should establish clear policies, procedures and staff training programmes pertaining to the identification, investigation and internal reporting of suspicious transactions (including attempted transactions), and the degree and extent of investigations that are appropriate prior to the internal reporting of a suspicious transaction. These policies and procedures should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

For CBO supervised institution, CBO's *"Guidelines on transaction monitoring and suspicious transaction reporting*" provide in-depth explanation in respect of all the aspects mentioned above.

3.3.5 'Tipping off'

Article 49 AML/CFT Law. Article 41(3) CBO Instructions, Article 32 Decision No. E/80/2021, Article 34 Decision E/81/2021

When reporting suspicious transactions to the Centre, FIs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person with due regard to the conditions and exceptions provided for in the law

As part of their risk-based AML/CFT framework, and in keeping with the nature and size of their businesses, FIs, and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

Such policies and procedures should include operational guidance with regard to core systems used for case management and notifications and secure information flows. Training should be provided for all staff in respect of the statutory obligation to report suspicious transactions and the internal procedures which must be followed. This guidance and training is primarily important for the front-line employees who have contact with customers. It is essential that these employees know when there may be cases of suspicious transactions, what questions they have to ask the customer and which information they must not under any circumstances disclose to the customer.

FIs should note that in cases where they form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the customer due diligence process will tip-off the customer, they shall not pursue the customer due diligence process and instead shall file a report with the Center,

It should be noted that the confidentiality requirement does not pertain to communication within the FI or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/FT.

It is an offence for FIs or their managers, employees or representatives, to inform a customer, beneficial owner or any other person, whether directly or indirectly, that a report has been made or will be made, or of the information or data contained in the report, or that an investigation is under way concerning the transaction.

3.3.6 Protection against Liability for Reporting Persons

FIs together with their employees, members of the board of directors, agents and authorized representatives are protected by the relevant articles of the AML/CFT Law and Supervisory Instructions from any penal, civil or administrative liability resulting from their statutory obligation to report suspicious activity to the NCFI, once this is done in good faith. This is also the case even if the reporting person did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. However, it should be noted that such protections do not extend to the unlawful disclosure to the customer or any other person, whether directly or indirectly, that they have reported or intend to report a suspicious transaction, or of the information or data the report contains, or that an investigation is being conducted in relation to the transaction.

3.3.7 Measures to be taken following the reporting of a Suspicious Transaction

Following the reporting of a suspicious transaction to the NCFI, FIs are expected to implement additional measures in relation to the customer and business

relationship to mitigate the associated ML/TF risks. Examples of such measures include:

- Reviewing and reassessing the business relationship and risk classification to ascertain whether a change to the risk profile is necessary
- Obtain approval from senior management before executing certain transactions
- Implementing enhanced risk-based on-going monitoring measures
- Any other reasonable steps, commensurate with the nature and size of the business remembering the obligation to avoid "tipping off" the customer.

3.4 Governance

Article 42 AML/CFT Law. Article 23 CBO Instructions, Article 26 Decision No. E/80/2021, Article 28 Decision E/81/2021

The attitude and culture which is embedded within an FI is of critical importance in the fight against ML and TF and recognises the important public interest aspect of an FI's role in this respect. This includes implementing an approach to AML/CFT compliance that considers the legislative obligations as only the starting point. FIs should engage with the CBO and CMA in a positive and transparent way and should be proactive in bringing relevant matters to the attention of the appropriate supervisory authority. Insufficient or absent AML/CFT risk management, governance, policies, procedures and controls exposes the FI to significant risks, not only financial, but also reputational;, operational and compliance risks.

FIs should ensure appropriate governance and oversight with regard to their compliance with obligations under the AML/CFT Law and Supervisory Instructions taking the following into consideration:

- Clearly established organizational structure with clearly defined and documented accountability lines and responsibilities to ensure that there is appropriate and effective oversight of staff who engage in activities which may pose a greater ML/TF risk.
- A mechanism of informing the board of directors/ committee of the board/partners meeting and senior management of compliance initiatives, compliance deficiencies, STRs filed or discounted and corrective actions taken;
- Development of a system of reporting that provides accurate and timely quantitative and qualitative information on the status of the AML/CFT program, including statistics on key elements of the program, such as the number of transactions monitored, alerts generated, cases created and STRs filed;
- Effective quality assurance testing programs to assess the effectiveness of the AML/CFT program's implementation and execution of its requirements

FIs should be aware of the importance of the existence of management structures which are accountable for ML/TF risk management measures as well as independent control functions.

3.4.1 Compliance Officer

In line with the AML/CFT supervisory Instructions, FIs are obliged to *"appoint a compliance officer at senior management level, who is responsible for the FI's compliance with and implementation of its AML/CFT obligations."* The Supervisory Instructions also provide that FI's must also provide the details of the Compliance Officer to the relevant supervisory authority, including the name, qualifications, contact number and email address and also to the NCFI. Should there be any change of Compliance Officer within the FI, the relevant supervisory authority and the NCFI must be promptly informed by the FI.

The appointed CO must be knowledgeable, have appropriate AML/CFT experience and qualifications and have the authority to act independently and

perform the statutory obligations and responsibilities of the role effectively. CO's should also have adequate access to resources and information to allow them to discharge their duties effectively.

In determining the competencies, level of experience, and organizational reporting structures that are appropriate for their COs, FIs should take several factors into consideration, including but not limited to:

- The results of the NRA, relevant sectorial risk assessment and any topical risk assessment
- The nature, size, complexity, and risk profile of their industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- The organisation's governance framework and management structure, with particular consideration given to the independent nature of compliance as a control function;
- The specific duties and responsibilities of the CO's role

Where appropriate, FIs may also consider engaging in dialogue with supervisory authorities, professional associations in their sectors, and industry peers, in relation to the competencies, experience, and governance structures that make for an effective compliance officer and an effective AML/CFT programme.

3.4.2 Role of the Compliance Officer

The supervisory instructions set out the specific roles and responsibilities of the CO as follows:

- **Management of the AML/CFT Program:** The CO is responsible for ensuring the quality, strength and effectiveness of the FI's AML/CFT programme. As such, the CO should be a stakeholder with respect to the FI's ML/TF business risk assessment, and the overarching AML/CFT risk mitigation framework, including its AML/CFT policies, controls and CDD measures. As outlined above, the CO is responsible for informing and reporting to senior management on the level of compliance.

- **Reporting to the Board of Directors/Partners Meeting:** The CO is obliged to provide periodic reports to the Board of Directors/Partners Meeting. For CMA supervised entities, these reports should be submitted at least on a quarterly basis. Such reports should be sufficiently comprehensive and provide detailed qualitative and quantitative information regarding suspicious transactions detected and the internal process which was followed, measures taken by compliance staff to strengthen the AML/CFT policies, procedures and controls, any gaps which have been observed in the compliance framework and subsequent actions which are required, an assessment of the adequacy of the FI's human resources and automated information systems which are allocated to AML/CFT compliance. The reports should provide the Board with an overall assessment of the effectiveness of the AML/CFT compliance program which has been implemented by the FI such that the senior management is in a position to make timely, informed and appropriate decisions on AML/CFT matters. These reports should be made available to the relevant supervisory authorities upon request.

  The compliance officer is also responsible for reviewing, scrutinizing and reporting STRs. In this capacity, the CO is ultimately responsible for the detection of transactions related to the crimes of money laundering and the financing of terrorism and for reporting suspicions to the Centre.

- **AML/CFT Training and Development:**The CO is responsible for helping to establish and maintain a strong and effective AML/CFT compliance culture within the FI. This duty includes working with senior management and other internal and external stakeholders to ensure that the FI's staff are well-qualified, well-trained, well-equipped, and well-aware of their responsibility to combat the threat posed by ML/TF.

3.4.3 Senior Management Responsibility

An integral part of any solid governance structure, including those related to AML/CFT compliance, is senior management involvement and accountability. The members of an FI's senior management (together with the members of the board of directors in those organisations that have one) are ultimately responsible for the quality, strength and effectiveness of the FI's AML/CFT

framework, as well as for the robustness of its compliance culture. In this regard, an FI's senior management should set the ML/FT risk appetite and a positive "tone at the top," by demonstrating their commitment to ensuring an effective AML/CFT compliance programme is in place, and by clearly articulating their expectations with regard to the responsibilities and accountability of all staff members in relation to it. FIs should ensure that the AML/CFT role and responsibilities of Senior Management is clearly defined and documented within the institution.

3.4.4 Training of Employees

Well trained employees who are alert to ML/TF risks is a critically important control for FIs in the detection and prevention of ML and TF. Therefore, FIs should ensure that their employees have a clear understanding of the ML/TF risks that the FI is exposed to and can exercise sound judgment, both when adhering to the FI's AML/CFT risk mitigation measures and when identifying suspicious transactions. Furthermore, due to the ever-evolving nature of ML/TF risks, FIs should ensure that their employees are kept up to date on an ongoing basis in relation to emerging ML/TF typologies and new internal and external risks.

Thus, to ensure a high level of competence and AML/CFT programme effectiveness, FIs should formulate and implement appropriate policies, procedures and controls with regard to staff training. FIs should ensure that all new and existing employees are trained in respect of the following:

- The relevant AML/CFT laws and regulations so that they can demonstrate an understanding of their own individual obligations as well as those of the FI
- The FI's policies and procedures used to mitigate ML/TF risks so that they can recognise and address potential instances of ML/TF, are aware of the internal reporting procedures in respect of STRs and the identity of the FI's CO.

FI's must ensure that all relevant employees are adequately trained which includes:

- Customer-facing staff.

- AML/CFT compliance staff.
- Senior management, including directors, board members, compliance officer, executive and supervisory management

Training should be specific and targeted to the role which is carried out by the individual employee and should be provided on an ongoing basis. A comprehensive record should be maintained by the FI all employees who attended the AML/CFT training, the nature of the AML/CFT training and the date on which the training was provided. FIs must be in a position to demonstrate effectiveness of training and employee understanding of the training provided, for example by ensuring that the training includes an assessment or examination during the training session which is passed by employees.

Some factors that should be considered when determining appropriate employee training measures include, but are not limited to:

- The specific role which is carried out by the employee within the FI. For example, customer facing staff who interact with customers and perform transactions and services should be provided with AML/CFT training relevant to the performance of that role. Enhanced training which is tailored to the specific needs of employee who perform key AML/CFT roles within the FI, for example the CO or senior management and board of directors responsible for AML/CFT oversight.
- The results of the NRA, sectorial risk assessment and any topical risk assessment
- The FI's business wide risk assessment including the nature, size, complexity, and risk profile of FIs' sectors and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve;
- Assessment of staff AML/CFT competency in relation to training and development needs;
- The type, frequency, structure, content, and delivery channels of AML/CFT training programmes and development opportunities;
- Appropriate methods and tools for assessing the effectiveness of employee training and development programmes

FIs should note that training content should be reviewed and updated on a regular basis to ensure that it remains relevant to the FI. FIs should also be aware that senior management should take appropriate remediation action where there are concerns in relation to training issues.

3.4.5 Screening of Employees

Pursuant to the AML/CFT Law and Supervisory Instructions, to ensure a to ensure a high level of competence and AML/CFT programme effectiveness, FIs should formulate and implement appropriate and effective policies, procedures and controls with regard to employee screening. Such screening should be conducted on all employees, directors, board members and executive or supervisory management, compliance officers and internal auditors and ensure :

- A high level of competence which is necessary for discharging their duties
- The appropriate ability and integrity to conduct the business activities of the FI
- Consideration of potential conflicts of interest, including the financial background of the employee
- Persons who have been charged with convicted of offences involving fraud, dishonesty or associated with criminals who may generally increase a risk of ML/TF or other similar offences are not employed by the FI.
- Perform screening against UN ,local TF list and may include any other sanction lists.

3.4.6 Independent Audit Function

A robust and independent audit function is a key component to a well-functioning governance structure and an effective AML/CFT framework. FIs are obliged to have in place an independent audit function to test the effectiveness and adequacy of their internal policies, controls and procedures relating to combating the crimes of ML and TF. In this regard, FIs should ensure that their independent audit function is appropriately staffed and organized, and that it has the requisite competencies and experience to carry out its responsibilities effectively, commensurate with the ML/TF risks to which the FIs are exposed, and with the nature and size of their businesses.

It should be noted that, while most FIs are expected to have the capacity to meet these requirements internally, depending on the nature and size of their

businesses, some FIs (particularly smaller ones) may not necessarily have the resources to maintain a fully functioning and effective internal audit unit. In such cases, those FIs should ensure that they take adequate measures to obtain the necessary capabilities from qualified external sources. They should also ensure that they have in place adequate internal capabilities to provide sufficient coordination with and oversight of any external resources they may utilise, and that such external resources are adequately regulated and supervised by relevant competent authorities.

FIs should ensure that the periodic inspection and testing of all aspects of their AML/CFT compliance programmes, including ML/TF business risk assessment and AML/CFT mitigation measures, and CDD policies, procedures and controls, transaction monitoring system is incorporated into their regular audit plans. They should also ensure that all their branches and the subsidiaries in which they hold a majority interest, whether domestic or foreign, are part of an independent audit testing programme that covers the effectiveness and adequacy of their internal AML/CFT polices, controls and procedures.

Some of the factors which FIs should consider in determining the appropriate frequency and extent of audit testing of their AML/CFT programmes by their independent audit functions include but are not limited to:

- The results of the NRA , relevant sectorial risk assessment and any topical risk assessment,
- The nature, size, complexity, and geographic scope of the FIs' businesses, and the results of their ML/TF business risk assessments;
- The risk profile associated with the products and services they offer and the markets and customer base they serve;
- The frequency of supervision and inspection by, and the nature of the feedback (including the imposition of administrative sanctions) they receive from CBO/CMA relative to enhancing the effectiveness of their AML/CFT measures;
- Internal and external developments in relation to ML/FT risks, as well as developments pertaining to the management and operations of the FIs.
- Law enforcement cases or requests related to customer of FIs.

The scope of such audits should include but not limited to:

- Examining the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements.

- Examining the adequacy of the transaction monitoring system and ensure data integrity and mapping.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems and processes, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity

3.4.7 Group Obligations

Article 42 AML/CFT Law. Article 24 CBO Instructions, Article 27 Decision No. E/80/2021, Article 29 Decision E/81/2021

When an FI is part of a group, there is an obligation to implement appropriate group-wide AML/CFT programmes, and to apply them in relation to all domestic and foreign branches and majority-owned subsidiaries of the financial group. The specific requirements that must be met by FIs with respect to their foreign branches and majority-owned subsidiaries are set out in the relevant provisions of the Supervisory Instructions, reflect those to which FIs are subject within Oman. In addition, AML/CFT policies, controls and procedures should contain:

- Policies and procedure for sharing information for the purposes of CDD and ML/TF risk management
- The provision, at group level compliance, audit and AML/CFT functions, of customer account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes, including information and analysis of transactions and activities which appear unusual, including STRs and underlying information.

- Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off
- Adequate controls on outsourcing arrangements of AML/CFT related functions, be it inside or outside the group.

Where the minimum AML/CFT requirements of the foreign country in which their branches and majority-owned subsidiaries operate are less strict that those which are applied under the Omani AML/CFT Law and Supervisory Instructions, FIs must ensure that the branches and majority-owned subsidiaries implement the requirements as set out in the AML/CFT Law and Supervisory Instructions to the extent permitted by the host countries legislative framework.

In situations where such host countries do not permit the proper implementation of the AML/CFT requirements consistent with those of Oman, financial groups should apply appropriate additional measures to manage and mitigate the ML/TF risks FIs should implement the necessary and appropriate additional measures, commensurate with the nature and size of their businesses, that will enable them to manage and mitigate appropriately the ML/FT risks that relate to their foreign operations.

Examples of some of the measures that should be considered include but are not limited to:

- Assessing the effectiveness of foreign branches and majority-owned subsidiaries' AML/CFT measures, including evaluating such factors as the comprehensiveness and quality of their policies, procedures and controls, and performing gap analyses in relation to the requirements of the AML/CFT Law and Supervisory Instructions.

- Establishing clear policies, procedures and controls in relation to the type and extent of access which managers and employees of foreign branches and majority-owned subsidiaries have to the FIs' IT and operational systems, including CDD and transaction processing systems;

- Establishing clear policies, procedures and controls in relation to the type and extent of access which customers and business relationships of foreign branches and majority-owned subsidiaries have to the FIs' products, services and transactional processing capabilities;

- Establishing clear policies, procedures and controls in relation to the type of CDD and transaction-related information, data, and analysis FIs accept from their foreign branches and majority-owned subsidiaries in relation to customer or business relationship referrals, and the extent of their reliance on such information

- Implementing service-level agreements, clearly setting out the roles and responsibilities of the parties and specifying the nature of the CDD and record-keeping requirements to be fulfilled in relation to customer or business relationship referrals;

- Establishing protocols for the certification by the foreign branches and subsidiaries of documents and other records pertaining to the CDD measures undertaken in relation to customer or business relationship referrals.

FIs should also inform CBO/CMA, as relevant, of the circumstances and comply with any additional supervisory actions, controls, or requirements of the supervisory authorities (up to and including, if requested, terminating their operations in the host countries).

3.4.8 Governance in Small Organisations

It is recognised that some FIs may operate as small or mid-sized businesses, without large staff organisations or sophisticated IT infrastructures. In such cases, individual managers and employees may often be required to undertake multiple roles and responsibilities in the course of day-to-day business activities, and it may be difficult at times to maintain a clear separation of duties or functions in such situations. While an FI's small size does not in any way exempt it from fulfilling its obligations under the AML/CFT Law and Supervisory Instructions, and without prejudice to guidance provided in the previous sections, the following additional considerations are of particular importance to small and mid-sized FIs.

- In situations in which the responsibilities of the AML/CFT compliance officer are delegated to a manager or staff member who also has other responsibilities, FIs should undertake their best efforts to ensure that the

designated AML/CFT compliance officer does not have day-to-day responsibility for sales and/or customer business relationship management.

- When an adequate separation of responsibilities is not possible due to the small size of an FI's organisation, FIs should take the necessary steps to ensure that operational and AML/CFT policies and procedures (particularly those pertaining to CDD, the identification and reporting of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and Sanctions Lists) are clearly formulated, documented, and adhered to during the establishment and ongoing monitoring of business relationships and the carrying out of transactions.

- In such cases, FIs should ensure that they clearly document the rationale for any policy and/or procedural exceptions they make, along with any additional AML/CFT risk mitigation measures they implement, and that these records are properly retained in accordance with the statutory record-keeping requirements. FIs should also consider referring to any significant policy or procedural exceptions, along with their rationale, associated additional AML/CFT risk mitigation measures, and senior management comments, to the CBO/CMA as appropriate.

- FIs that are unable to ensure a clear and effective separation of AML/CFT responsibilities from those related to the day-to-day management of their businesses, including but not limited to sales and customer business relationship management functions, due to the small size of their organisation should also consider taking additional measures to enhance the application of their independent audit controls. Examples of such measures include but are not limited to:

  - Incorporating the audit of policies, procedures (particularly those pertaining to CDD, the identification of Suspicious Transactions, and the monitoring and updating of required High Risk Country CDD measures, and Local and International Sanctions Lists), and records related to exceptions made to them, as part of their audit plans and/or their service-level agreements with their external providers of independent audit services;
  - Increasing the frequency of independent audits and random audit inspections;

- Applying stricter criteria with regard to the review of past transactions, such as increasing the number of transactions reviewed for a given time period, reducing size threshold limits for transactions to be reviewed, or taking other reasonable measures in this regard.

3.5 Record Keeping

Article 44 AML/CFT Law, Article 35, 36 CBO Instructions, Article 25 Decision No. E/80/2021, Article 27 Decision E/81/2021

3.5.1 Obligation to retain records

Adequate record keeping is critically important to the preservation of the audit trail which in turn can assist with any investigation into ML and TF. Effective record keeping also allows the FI to demonstrate to the CBO/CMA the steps which they have taken to comply with their AML/CFT obligations under the AML/CFT Law and Supervisory Instructions. FIs are obliged to maintain detailed records, documents, data and statistics for all transactions, all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, as well as a variety of record types and documents associated with their ML/TF risk assessment and mitigation measures, as specified in the relevant provisions of the AML/CFT Law and Supervisory Instructions.

FIs are required to maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions, and to make the records available to the competent authorities immediately upon request. The records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

The statutory retention period for all records is at least 10 years in the following circumstances:

- After the termination of the business relationship

- Completion of an occasional transaction (in respect of a customer with whom there is no established business relationship)

FIs should note that in situations where it is deemed necessary by competent authorities, FIs may be required to retain records for a longer period of time.

3.5.2 Records which must be retained

The AML/CFT Law and Supervisory Instructions oblige FIs to retain the following categories of records:

- All records of transactions: This category relates to operational and statistical records, documents and information concerning all transactions executed or processed by the FI (including attempted transactions) whether domestic or international in nature.
- Copies of transaction reports which were filed with the Centre and related documentation
- Risk Assessment reports and underlying information
- CDD Records: This category relates to records, documents, and information about customers, their due diligence, and the investigation and analysis of their activities, and can be further divided into sub-categories such as records pertaining to:
  - Customer Information, including account files and business correspondence, and results of any analysis undertaken
  - Reliance on Third Parties to Undertake CDD
  - Ongoing Monitoring of Business Relationships
  - Suspicious Transaction Reports (STRs)

Further guidance in respect of these categories of records is provided below:

I. Records of Transactions

FIs are obliged to retain the operational and statistical records, documents and information concerning all transactions executed or processed by the FI whether domestic or international in nature, and irrespective of the type of customer and whether or not a Business Relationship is maintained, for a minimum period of 10 years. Some examples of the type of records, documents and information which must be retained include but are not limited to:

- Customer credit or debit advices, and transaction orders or applications (including those for cash deposits or withdrawals, currency exchange transactions);
- Credit-related documentation, including loan or guarantee applications, agreements, amendments and supporting documents, disbursement or repayment records, collateral pledges, letter of credit documentation, promissory notes;
- Deal tickets, trade blotters and ledgers, settlement and dividend payment records related to foreign exchange, securities dealing or investing transactions;
- Escrow or fiduciary account transaction records;
- Insurance policy premiums, pay-outs, and related transaction records and documents;
- Money transfer records, including book transfers orders, and domestic and cross-border wire transfer orders, and their related originator and beneficiary records;
- Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates, and other information.

In addition to the above, FIs should compile notes on any particularly large or unusual transactions, and keep these notes as part of their records.

II. Customer Information

FIs are required to retain all customer records and documents obtained through the performance of CDD measures in relation to Business Relationships, including customers, Beneficial Owners, beneficiaries, or other controlling persons. Examples of such records include but are not limited to:

- Customer account information and files;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls);

- Copies of personal identification documents, CDD (including EDD and SDD) forms, profiles and supporting documentation, and results of due diligence background searches, queries and investigations;
- Customer risk assessment and classification records.

III. Reliance on third parties to undertake CDD

FIs should ensure, when placing reliance on third parties to undertake CDD, that copies of all the necessary documentation collected can be obtained upon request and without delay and that the third parties comply with the record-keeping provisions of the AML/CFT Law and Supervisory Instructions.

IV. Ongoing Monitoring

FIs should retain all records obtained through the ongoing monitoring conducted by the FI, including the monitoring of transactions. Examples of such records include, but are not limited to:

- Transaction review, analysis, and investigation files, with their related correspondence;
- Customer correspondence (including email and fax correspondence), call reports or meeting minutes (including where applicable recordings, transcripts or logs of telephone or videophone calls) related to those transactions or their analysis and investigation;
- CDD records, documents, profiles or information gathered in the course of reviewing, analysing or investigating transactions, as well as transaction-related supporting documentation, including the results of background searches on customers, Beneficial Owners, beneficiaries, controlling persons, or counterparties to transactions;
- Transaction handling decisions, including approval or rejection records, together with related analysis and correspondence.

V. Suspicious Transaction Reports (STRs)

- FIs are required to retain all records and documents pertaining to STRs and the results of all analysis or investigations performed. Such records

relate to both internal STRs and those filed with the Centre and include but are not limited to:

- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence;
- CDD and Business Relationship monitoring records, documents and information obtained in the course of analysing or investigating potentially suspicious transactions, and all internal or external correspondence or communication records associated with them;
- STRs (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records (including the rationale for reporting or not reporting), and all related correspondence;
- Competent authority request for information, correspondent bank requests for assistance, and their related investigation files and correspondence;
- All documentation and information used as part of any internal assessment into a customer following on from the filing of an STR.
- Notes concerning feedback provided by the Centre with respect to reported STRs, as well as notes or records pertaining to any other actions taken by, or required by, the Centre

VI. Business Risk Assessment

FIs should retain each business risk assessment that it conducts which includes any amendments made to the risk assessment as part of an FI's review and monitoring process and any relevant underlying information.

Other records which should be retained by the FI:

Minutes of Senior Management Meetings

FIs should retain all records of discussion and decisions made at senior management level in relation to:

- How the requirements of the AML/CFT Law and Supervisory Instructions

were implemented

- How the Board/senior management has assessed the effectiveness of and compliance with systems and controls
- Any AML/CFT issues that arise on an ongoing basis

Training Records

FIs should retain records of all AML/CFT training provided to staff during any given year. Information should include:

- The dates on which AML/CFT training was provided to staff
- Attendance log of who received the AML/CFT training
- The nature and content of the AML/CFT training provided
- Results of the assessment and examination during the training session to measure employees understanding of the training provided