AML/CFT Guidance

for the

Capital Market Sector

September, 2021

Table of Contents

PART 1 – OVERVIEW

Introduction

1.1 Purpose and Scope

The purpose of the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Guidelines for the Capital Market Sector is to provide guidance and assistance to supervised institutions within the Capital Market Sector in understanding their AML/CFT obligations under the legal and regulatory framework in force in the United Arab Emirates (UAE).

These Sectoral Guidelines supplement the Anti-Money Laundering and Combating the Financing Guidelines ('the Guidelines') for Financial Institutions and each section of the Sectoral Guidelines should be read in conjunction with the main Guidelines.

These Sectoral Guidelines set out the expectations of the Securities and Commodities Authority (SCA) regarding the factors that firms within the sector should take into account when identifying, assessing and mitigating the risk of money laundering (ML) and the financing of terrorism (TF).

Nothing in these Sectoral Guidelines is intended to limit or otherwise circumscribe additional or supplementary guidance, circulars, notifications, memoranda, communications, or other forms of guidance or feedback, whether direct or indirect, which may be published on occasion by the SCA or in respect of any specific supervised securities provider.

It should be noted that guidance on the subject of the United Nations Targeted Financial Sanctions (TFS) regime and the related Cabinet Decision No (74) of 2020 *Regarding Terrorism Lists Regulation and Implementation of UN Security Council Resolutions On the Suppression and Combating of Terrorism, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions* is outside of the scope of these Sectoral Guidelines.

1.2 Applicability

These Guidelines apply to all Financial Institutions licensed by SCA (FIs) which includes members of their boards of directors, management and employees, established and/or operating in the territory of the UAE under the jurisdiction of SCA, whether they establish or maintain a business relationship with a customer, or engage in any of the financial activities and/or transactions or the trade and/or business activities pursuant to Articles (2) of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

1.3 Legal Status

Article 44.11 of Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 *On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the crime-combatting measures."

As such, these Sectoral Guidelines do not constitute additional legislation or regulation, and are not intended to set legal, regulatory, or judicial precedent. They are intended rather to be read in conjunction with the relevant laws, cabinet decisions, regulations and regulatory rulings which are currently in force in the UAE and the respective Free Zones, and supervised institutions are reminded that the Sectoral Guidelines do not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between these Sectoral Guidelines and the legal or regulatory frameworks currently in force, the latter will prevail. Specifically, nothing in these Sectoral Guidelines should be interpreted as providing any explicit or implicit guarantee or assurance that the SCA or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

These Sectoral 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 firms within the Capital Market Sector in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, these Sectoral 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.

It is the SCA's intention to update or amend these Sectoral Guidelines from time to time, as and when it is deemed appropriate. Supervised firms are reminded that these Sectoral Guidelines are not the only source of guidance on the assessment and management of ML/TF risk and that other bodies, including international organizations such as FATF, MENAFATF and other FATF-style regional bodies (FSRBs), the Egmont Group and others also publish information that may be helpful in carrying out their statutory obligations. It is the sole responsibility of supervised institutions to keep appraised and updated at all times regarding the ML/TF risks to which they are exposed, and to maintain appropriate risk identification, assessment and mitigation programmes and to ensure their responsible officers, managers and employees are adequately informed and trained on the relevant policies, processes and procedures.

Unless specifically noted to the contrary, all references in the document to the term "financing of terrorism" also encompasses the financing of illegal organizations.

1.4 Overview of the Capital Market Sector

The global capital market has been quickly and continually evolving over the years. The capital market industry plays an important role in UAE and in the global economy and is one of the core industries through which natural and legal persons can access the financial system. Some of the features specific to the Capital Market Sector and which may make this sector vulnerable to abuse by criminals for ML/TF purposes are as follows:

The various roles that securities providers and other intermediaries play in transactions;

- The speed in executing transactions;
- The ability to transact via an intermediary which may provide a relative degree of anonymity;
- The number of large value transactions;
- The variety and complexity of financial instruments available;
- The high liquidity of certain securities products which can enable their easy conversion to cash;
- The international nature and global reach of the sector across a multitude of jurisdictions and financial markets;
- Difficulties in pricing some securities products due to their bespoke nature or complexity and the volatility of some products;
- Involvement of a multitude of securities providers and intermediaries on behalf of both buying and selling principals or agents, which may limit the ability of any one participant having full oversight of the transaction.

1.4.1 ML/TF Typologies

The methods used by criminals for money laundering, the financing of terrorism and the financing of illegal organizations are continually evolving and becoming more sophisticated. In combatting these crimes it is essential that personnel within the Capital Market Sector are kept up to date on the most recent ML/TF trends and typologies.

There are numerous useful sources of research and information related to ML/FT typologies, including by the Supervisory Authorities, the FATF, MENAFATF and other FSRBs, the Egmont Group, 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.

Examples of some of the key ML/TF typologies with which entities should be familiar with are outlined in the main Guidelines. However, the following sections provides further information relating to the risks of cash based money laundering and trade based money laundering and terrorist financing (TBML) which the UAE is exposed to and of which the Capital Market Sector should be aware of.

1.4.2 Trade based money laundering

Trade based money laundering is the process of disguising the proceeds of crime or instruments of terrorist financing and moving money through the use of trade transactions to avoid financial transparency laws and regulations in an attempt to legitimise their illicit origins. It is one of the main methods by which criminals launder the proceeds of crime. TBML schemes often include a number of complex layers including cash, front companies, currency exchange and the purchase and shipment of goods with illicit proceeds.

Domestic and international trade, is especially vulnerable to misuse by criminals engaged in illegal operations. The special tax and administrative arrangements available to exporters and export service providers, while intended to boost legitimate trade, can create ML and TF vulnerabilities. TBML is easier to perpetrate when a series of systematic vulnerabilities exist in one place. In particular, FTZ represent an environment where this occurs through lack of transparency, trade data and systems integration. As a result FTZs may facilitate TBML and related illicit activity. The nature of the FTZ makes it more challenging to detect illicit activity and provides opportunities for misuse.

Trade can be inherently complex and complicated, reflecting the nature of interconnected supply chains around the world and Illegal transactions can easily be disguised as legal using TBML schemes that are very difficult to detect. A wide range of economic sectors have been identified as being vulnerable to TBML – both high-value, low volume sectors or products and

low-value, high volume sectors or products can be exploited by criminals to launder the proceeds of crime. Despite the diversity in sectors, the following common themes have been identified as conducive to TBML exploitation;

- Goods with wide pricing margins
- Goods with extended trade cycles (i.e. shipping across multiple jurisdictions)
- Goods which are difficult for customs authorities to examine.

Trading activity is primarily vulnerable to criminal exploitation, due to the large volume of trades conducted on a daily basis and the speed with which these trades often need to be executed. In practice this can be achieved by criminals through the misrepresentation of the price, quantity or quality of imports or exports which are outlined in further detail below.

1.4.3 Misrepresentation of the price of the good or service:

A criminal may misrepresent the price of the good or service in order to transfer additional value between the importer and exporter. By invoicing the good or service at a price below the fair market price, it is then possible for the exporter to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market. Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is in a position to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market.

1.4.4 Multiple invoicing of goods and services

Another technique used to launder funds involves issuing more than one invoice for the same trade transaction. By invoicing the same good or service more than once, a criminal is able to justify multiple payments for the same shipment of goods or delivery of services. Utilizing a number of different institutions to make these additional payments can further increase the level of complexity surrounding such transactions. In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there may be a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees.

1.4.5 Misrepresentation of the quantity of good or service

In addition to manipulating export and import prices, the quantity of goods being shipped or services being provided can be under or overstated. In extreme examples, an exporter may

not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with the so called "phantom shipment" are routinely processed. Entities which are part of the Capital Market Sector may unknowingly be involved in the provision of trade financing for these phantom shipments

1.4.6 Misrepresentation of quality or type of good or service

In addition to manipulating export and import prices, the quality or type of a good or service may be misrepresented. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, establishing the fair market value of these services can present additional valuation difficulties.

TBML techniques vary in complexity and are frequently used in combination with other ML techniques to further obscure the money trail. Given the dynamic nature of international trade, including the diversity of tradable goods and services, the involvement of multiple parties, and the speed of trade transactions, TBML remains a profound and significant risk to the UAE.

1.5 TBML red flag indicators:

There are a number of red flag indicators which can be used to identify TBML activities. These include the following situations which securities providers should have regard to:

- Copy documents are used in situations where original documentation would be expected, without reasonable explanation.
- The customer is unable or reluctant to provide documentation to support the transaction.
- The majority of business activity is to or from a jurisdiction designated as "high risk" for money laundering activities.
- The method of payment appears inconsistent with the risk characteristics of the transaction.
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction.
- The transaction involves the use of front (or shell) companies.
- The transaction is highly structured, fragmented or complex involving multiple parties without apparent legitimate justification.
- The transaction is otherwise unusual.

- There are indications of collusion between the buyer and seller, for example the buyer and seller have the same address.
- The buyer's legal structure does not allow the identification of its owners, or it is represented by agents or third parties.

In situations where an entity provides trade finance services to a customer, there is an expectation that as part of the CDD process, the FI takes steps to understand its customers business. Example of the type of information which may be obtained by the institution includes information relating to;

- the countries with which the customer trades,
- the trading routes which are used,
- the goods which are traded,
- the parties with which the customer does business with,
- whether the customer uses agents or third parties and if so where these are based.

A due-diligence assessment of a corporate client at the time of onboarding may include information regarding expectations of volumes, values and trade flows as well as an understanding of the types of goods and services involved.

This information should assist in understanding the customer and allows institutions to periodically validate that the transaction flows are consistent with the business profile of the customer and help in the detection of unusual or suspicious transactions.

It should be noted that in certain cases, FIs may only have access to partial information about the transaction and the parties involved in the transaction. Furthermore, trade documentation can be very diverse. Therefore institutions should apply professional judgement to assess whether the documentation and information which they have received could give risk to a suspicion of ML/TF.

In situations which are deemed to be higher risk, FIs should conduct EDD. As part of this, FIs should consider whether performing more thorough due diligence checks on the transactions itself and on other parties to the transaction (including non-customers) would be appropriate.

1.6 Cash-based money laundering

The UAE is considered to be a cash-intensive economy and plays an important part in international trade which exposes the country to illicit cash movements. Cash remains a significant raw material for criminal groups and is used by choice as an anonymous financial instrument by a wide range of criminals, even in complex money laundering systems. It remains a key contributor to risk in all financial sectors as a result of a number of factors such as difficulty in tracing cash, anonymity of cash transactions, transferability of cash, prevalence of cash payments in illicit industries and the smuggling of cash across international borders.

In particular, often the nature of business within FTZs appear to be based on cash transactions with many businesses routinely accepting large volumes of cash for wholesale quantities of merchandise. Furthermore, the integration of cash into the financial system is often facilitated by the presence of financial institutions in the FTZs. Cash does not require financial institutions and presents particular ML/TF risks because of its portability, anonymity and lack of audit trail.

Many predicate offences, particularly those associate with organised criminal gangs, ML and TF, generate proceeds of crime primarily in the form of cash. Cash can also be used to obstruct any attempt to trace the movement of laundered proceeds through the regulated financial sector. Physical transportation of cash (i.e. bulk cash smuggling (BCS) and cash couriers) as a means of money laundering continues to be a problem in many countries worldwide. It is an issue that concerns both developing countries with cash based economies as well as countries with developed and sophisticated financial systems.

While the Capital Market Sector may not be predominately cash based and therefore considered to be less conducive to the initial placement of illegal funds that other financial entities where the payment underlying transactions is in cash, due diligence must nonetheless be exercised. The ability of cash to be placed into general transaction accounts and quickly moved between trading accounts may make the sector vulnerable to ML. This risk is then heightened when the transaction and trading accounts are held with different entities due to the limited visibility both firms have over the customers financial activity. For example cash can be placed into general accounts that are linked to trading accounts and through a series of transfers, made to look like the proceeds of securities and derivatives trading. Furthermore, it may be possible for criminals to approach individuals and offer them cash for their securities portfolio. Subsequently, these individuals could transfer their securities from their securities portfolio to the securities portfolio of the criminal. This would give criminals access to the financial system while avoiding AML/CFT obligations.

There is evidence that depository institutions and securities intermediaries that permit the use of cash for the purchase of securities products can be used to place illicit assets in the securities industry, as well as integrate and layer the assets through securities trading and redemptions. The following, were identified as suspicious indicators involving the use of cash:

- The customer refuses to identify a legitimate source for the funds or provides the securities firm with information that is false, misleading, or substantially incorrect;
- The customer makes many small cash deposits that are eventually used to purchase a particular securities product which is sold or redeemed shortly thereafter;
- The customer deposits a large amount of small-denomination currency to fund the account or make securities purchases;
- The customer operates with amounts and denominations of currencies that do not fit their profile or their usual commercial activity
- There are many incoming cash deposits into a customer's account from third parties that coincide with or are close in time to outgoing cheques or wire transfers to other third parties; and

- The customer has accounts primarily used for deposits and other accounts primarily used for outgoing payments.

PART 2 - Identification and Assessment of ML/TF Risks

Both the AML-CFT Law and the AML-CFT Decision provide for a risk based approach with respect to the identification and assessment of ML/TF risks.

FIs are obliged to assess and understand the ML/TF risks to which they are exposed and how they may be affected by those risks. Specifically, the AML-CFT Law provides that they shall:

"….continuously assess, document and update such assessment based on the various risk factors established in the Implementing Regulation of this Decree-Law and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority upon request.

Furthermore, the AML-CFT Decision charges entities with:

"….documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request.

2.1 Risk Based Approach

A risk based approach (RBA) is central to the effective implementation of the AML/CFT legislation. This means that firms 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. Assessing this risk is therefore one of the most important steps in creating a good AML/CFT compliance programme and will enable firms to focus their resources where the risks are higher.

For FIs, this requires an understanding of the ML/TF risk faced by the sector, knowledge of the specific products and services, customer base, whether a customer is operating on its own behalf or on behalf of an underlying customer, jurisdiction in which they operate together with the effectiveness of risk controls put in place. The RBA to customer due diligence by FIs can vary depending on a number of factors such as the securities product involved in a transaction, custodial relationships, contractual obligations, and the customer.

Entities within the Capital Market Sector which are subject to supervision by SCA provide a range of products and services including exchanges (ADX-DFM), securities and commodities brokerage, securities consultation and analysis, portfolio and investment management, fund service business, and depository services, ….etc. Regardless of the role, an FI must continually tailor its own RBA to assessing and managing ML/TF risk as different business models and practices may pose different ML/TF risks.

FIs must understand how their business practices may be exposed to ML/TF risks both directly (eg. through transactions executed by customers) and indirectly (eg, risks associated with the

underlying customers or risks associated with the possibility that an intermediary or other entity on which the FI relies to perform a task fails to do so.)

The AML-CFT Law and AML-CFT Decision require firms to apply a risk-based approach when applying AML/CFT compliance measures.

2.2 Assessing Business-wide risks

An important first step in applying a RBA is to identify, assess and understand the ML/TF risks by way of 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 enterprise as a whole, determining how these risks are effectively mitigated through internal policies procedures and controls and establishing the residual ML/TF risk and any gaps in controls that should be addressed.

A business risk assessment should consist of the following steps:

- Identifying ML and TF risks relevant to a firm's business
- Assessing the identified ML and TF risks in order to understand how to effectively mitigate those risks.

FIs should ensure that their business wide risk assessment is documented and tailored to their business profile and takes into account the factors and risk specific to the institution's business. A generic risk assessment that has not been adapted to the specific needs and business model of the firm is not demonstrative of the risk based approach.

The risk assessment should enable the FI to understand how and to what extent it is vulnerable to ML/TF..

2.3 Risk Factors

As part of the business-wide ML/TF risk assessment, a proper identification of risk factors is crucial to the effective assessment of ML/TF risk. Examples of risk factors specific to the Capital Market Sector which may be taken into account by FIs when conducting the ML/TF business risk assessment are provided in the sections below. While there is no complete set of circumstances which may be considered to be of higher risk, the examples provided in this document are the most commonly identified within the Capital Market Sector.

It should be noted that the presence of isolated risk factors does not necessarily move a business relationship into a higher or lower risk category and institutions should take a holistic view of the risk associated with any situation. FIs must thoroughly review all risk factors

relevant to their business, including how certain factors interact with each other and have an amplifying effect.

In line with the ever evolving nature of ML/TF risks and in order to ensure that firms implement a model for conducting the ML/TF business risk assessment that is appropriate to the nature and size of their business, firms should continuously update the risk factors in order to reflect new and emerging ML/TF risks and typologies.

2.3.1 Customer Risk

The customer risk factors relates to the 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.

The following factors may contribute to increasing the risk associated with the customer:

The customer's behaviour, for example:

- The rationale for the investment lacks an obvious economic purpose.
- The customer makes investments that are inconsistent with the customer's overall financial situation.
- A request to repurchase or redeem a long-term investment by the customer shortly after the initial investment or before the payout date in the absence of any clear rationale, in particular in circumstances where this results in financial loss or payment of high transaction fees.
- A request for a repeated purchase and sale of shares or units within a short period of time without any obvious rationale.
- A reluctance to provide CDD information on the customer and the beneficial owner;
- frequent changes to CDD information or payment details.
- the customer transfers funds in excess of those required for the investment and asks for the surplus to be reimbursed.
- the circumstances in which the customer makes use of the 'cooling-off' period give rise to suspicion.
- using multiple accounts without previous notification, especially when these accounts are held in multiple or high-risk jurisdictions.
- the customer wishes to structure the relationship in such a way that multiple parties are used in different jurisdictions, particularly where these jurisdictions are associated with higher ML/TF risk.
- The customer suddenly changes the settlement location with any explanation, for example by changing the customer's country of residence.

The customer's nature, for example:

- The customer is a company, a trust or other legal arrangements having a structure or functions similar to trusts, established in a jurisdiction associated with higher ML/TF risk (firms should pay particular attention to those jurisdictions that do not comply effectively with international tax and information sharing transparency standards).
- the customer is an investment vehicle that carries out little or no due diligence on its own clients.
- The customer is a highly liquid open-ended fund with the possibility of frequent subscriptions and redemptions.
- the customer is an unregulated third party investment vehicle.
- the customer's ownership and control structure is opaque.
- the customer or the beneficial owner is a PEP or holds another prominent position that might enable them to abuse their position for private gain.
- the customer is a non-regulated nominee company with unknown shareholders.

The customer's business for example:

- The customer's funds are derived from business in sectors that are associated with a higher risk of financial crime.

2.3.2 Product, Services and Transaction Risk

When assessing the inherent ML/FT risks associated with product, service, and transaction types, an FI should take stock of its lines of business, products and services that are more vulnerable to ML/FT abuse. An FI may offer a range of products and services to customers which may involve executing transactions for a customer by processing an order to transact or clear trades, handling the movement of funds or securities for the customer and settling a customer's transactions and liabilities. Transactions may be conducted by way of a regulated exchange or other market or between parties directly. The provision of products and services used within this sector can involve multiple parties such as the fund manager, advisors (including financial advisors), depository, custodians and brokers.

The following factors may contribute to increasing risk:

- Transactions that are unusually large in the context of knowledge and profile of the customer.
- The purchase of securities using physical cash.
- Settlement arrangements that appear irregular or are non-standard.
- Third party payments are possible, in particular where this is unexpected.
- The product or service is structured in a way that may present difficulties identification of the customers or inherently favour anonymity.

- The product or service is used for subscriptions that are quickly followed by redemption possibilities, with limited intervention by the investment manager.
- It is possible to subscribe to the fund and quickly redeem the investment without the incurrence of significant costs by the investor.
- Regular payment of fees, commissions and costs to source and investigate transactions, but no transactions are executed.
- Transactions involving securities used for currency conversion that appear unusual or have no obvious business or economic purpose.
- The fund is designed for a limited number of individuals for example a private fund or single investor fund.
- The subscription involves accounts or third parties in multiple jurisdictions, in particular where these jurisdictions are associated with higher ML/TF risk.

2.3.3 Delivery channel-related risk factors

Different delivery channels for the acquisition and management of customers and business relationships, as well as for the delivery of products and services, entail different types and levels of ML/TF risk. A risk assessment should include the risks associated with the different types of delivery channels which facilitate the delivery of securities products and services. Typically, securities products and services are distributed directly to the customers or through an intermediary.

The following may contribute to increasing risk:

- Complexity in the chain of reception and transmission of orders.
- Complexity in the distribution channels which limit the funds oversight of its business relationships and ability to monitor transactions for example the fund uses a large number of sub-distributors for distribution across a number of jurisdictions.
- Complexity in the distribution chain of investment products.
- The trading venue has members or participants or a distributor is located in jurisdictions associated with higher ML/TF risk.

2.3.4 Country or geographical risk factors

A firm should consider geographic ML/TF risk factors both from domestic and cross border sources.

The following factors may contribute to increasing risk:

- The investor or their custodian is based in a jurisdiction associated with higher ML/TF risk. Companies should periodically check the web page of the National AML/CFT Committee for updates on high-risk countries.
- The funds have been generated in jurisdictions associated with higher ML/TF risk.
- The customer requests their investment be redeemed to an account in an institution located in a jurisdiction associated with higher ML/TF risk.

2.4 Risk Assessment Methodology and Documentation

A well-documented assessment of the identified inherent risk factors is fundamental to the adoption and effective application of reasonable and proportionate ML/FT risk-mitigation measures. Thus, the result of such an ML/TF business risk assessment allows for a systematic categorisation and prioritization of inherent and residual ML/FT risks, which in turn allows FIs to determine the types and appropriate levels of AML/CFT resources needed for mitigation purposes. An effective ML/TF business risk assessment is not necessarily a complex one. The principle of a risk-based approach means that FIs risk assessments should be commensurate with the nature and size of their businesses. Those 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.

FIs are obliged to document their risk assessment operations and keep their ML/TF business risk assessment up-to-date on an ongoing basis.

PART 3 - Mitigation of ML/TF Risks

Commonly referred to as the three lines of defence, the basic elements that must be addressed in an AML/ CFT program are

- A system of internal policies, procedures and controls, including an ongoing employee training program (first line of defence);
- A designated compliance function with a compliance officer or money laundering reporting officer (second line of defence); and
- An independent audit function to test the overall effectiveness of the AML program (third line of defence).

In setting up these three lines of defence, FIs can take into account their business nature, size and complexity

Following an assessment of the inherent ML/TF risks in their businesses, FIs are obliged to take the necessary measures to manage and mitigate the ML/TF risks to which they are exposed.

The internal policies, controls and procedures which entities should have in place to prevent, detect and deter ML/TF risks can be broadly categorised as those related to:

- The identification and assessment of ML/TF risks
- Customer due diligence (CDD), including Enhanced Due Diligence (EDD) and Simplified Due Diligence (SDD)
- Customer and transaction monitoring and the reporting of suspicious transactions
- AML/CFT governance including staffing and training, senior management responsibilities and the independent auditing of risk mitigation measures
- Record-keeping requirements.
- Procedures to deal with transactions originating or ending in high-risk countries, as identified by the National AML/CFT Committee as well as by FATF and/or MENAFATF.
- Screening, reporting and actions to be taken upon finding a match or a potential match to names listed on the UNSC and Dometic TFS lists disseminated by the Executive Office of the Committee for Goods and Materials subject to Import and Export Control (EO-TFS)

Guidance in relation to each of these categories is provided for in detail in the main Guidelines.

3.1 The FI's customer

As part of their role, and in addition to conducting transactions and/or maintaining accounts for customers directly, it may be the case that FIs engage with other FIs and intermediaries

who have their own underlying customers. Therefore, particular consideration should be given to the CDD obligations which such entities should take.

When determining the type and extent of CDD measures to apply, an FI should be clear as to whether the customer is acting on its own behalf or as an intermediary on behalf of its underlying customers. In relation to investment funds for example, the CDD measures which are taken will depend on how the ultimate customer comes to the fund. The investment fund may be required to treat an underlying investor as its customer or the intermediary as its customer depending on factors such as how the investment fund is sold, with whom the business relationship is established or who is registered in the fund's share/units register.

Where an intermediary is treated as the investment fund's customer, the investment fund may not have visibility on the intermediary's underlying customers. Risk sensitive measures should be taken to identify and verify the identity of the natural persons, if any, who ultimately own and control the customer, or on whose behalf the transaction is being conducted, for example by asking the prospective investor to declare when they first applied to join the fund, whether they are investing on their own behalf or whether they are an intermediary investing on someone else's behalf.

FIs should also obtain from the intermediary, information about the intermediary's AML/CFT controls, including information relating to the intermediary's risk assessment of its underlying customer base and its implementation of risk mitigation measures.