Mauritius Institute of Professional Accountants

Anti-Money Laundering and Countering the Financing of Terrorism – Guidelines for Public Accountants, Professional Accountants and Member Firms in Mauritius

Issued pursuant to Section 19 (H) (a) of the Financial Intelligence and Anti Money Laundering Act 2002

May 2020

Table of Contents

ACRONYMS

AML/CFT	Anti-money Laundering/Countering the Financing of Terrorism and proliferation
CDD	Customer Due Diligence
DNFBP	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FI	Financial Institution
FIAMLA	Financial Intelligence and Anti-Money Laundering Act 2002
FIAML Regulations	Financial Intelligence and Anti-Money Laundering Regulations 2018
FIU	Financial Intelligence Unit
INR	Interpretive Note to Recommendation
MER	Mutual Evaluation Report
ML	Money Laundering
MIPA	Mauritius Institute of Professional Accountants
MLRO	Money Laundering Reporting Officer

NRA	National Risk Assessment
PEP	Politically Exposed Person
POCA	Prevention of Corruption Act 2002
POTA	Prevention of Terrorism Act 2002
R.	Recommendation
RBA	Risk-Based Approach
Rec	Recommendation
Reg	Regulation
SAR	Suspicious Activity Report
SRB	Self-Regulatory Body
STR	Suspicious Transaction Report
CSP	Company Service Providers
TCSP	Trust and Company Service Provider
TF	Terrorist Financing
UN Sanctions Act	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

UNSCR	United Nations Security Council Resolution

TERMINOLOGY USED IN THE GUIDELINES

You – refers to an accounting professional or a reporting person.

Shall/Must – refers to a specific requirement in legislation. You must comply unless there are statutory exemptions or defences.

Should – it is good practice in most situations, and these may not be the only means of complying with legislative requirements.

May – a non-exhaustive list of options to choose from to meet your obligations.

DISCLAIMER

This Guidance[1] is non-binding and does not overrule the purview of national authorities[2] including on their local assessment and categorisation of the accountancy profession based on the prevailing ML/TF risk situation and other contextual factors. It draws on the experiences of Mauritius and of the private sector to assist competent authorities and accountants to implement applicable FATF Recommendations effectively. Professional accountants should also consider their ethical obligations as set out under the Code of Ethics issued by the International Federation of Accountants (IFAC)[3]where relevant.

The Guidelines must be read in conjunction with the Financial Intelligence and Anti-Money Laundering Act 2002, Prevention of Corruption Act 2002, Prevention of Terrorism Act 2002, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Convention of the Suppression of the Financing of Terrorism Act and the Financial Intelligence and Anti-Money Laundering Regulations 2018.

This Guidance is not meant to apply to professional accountants in business, which includes professional accountants employed or engaged in an executive or non-executive capacity in such areas as commerce, industry, service, the public sector, education, the not-for-profit sector, regulatory bodies or professional bodies. Such accountants should refer to their professional code of conduct or other alternative sources of Guidance, on the appropriate action to take in relation to suspected illegal activity by their employer or a third party.

These Guidelines shall be subject to amendments by the MIPA. Stakeholders are urged to ensure that they consult the most up to date version.

[1] For the purposes of this exercise, the terms 'guidance' or 'guide' or 'guidelines' mean one and the same thing and the term will be used interchangeably throughout this document.
[2] National authorities should however take the Guidance into account when carrying out their supervisory functions.
[3] Handbook of the International Code of Ethics for Professional Accountants issued in 2018.

CHAPTER 1: OVERVIEW

1.1. Introduction

Accountants are key gatekeepers for the financial system, facilitating vital transactions that underpin the Mauritian economy. As such, they have a significant role to play in ensuring their services are not used to further a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activities.

Mauritius has established a strict and rigorous anti-money laundering (AML) and countering the financing of terrorism (CFT) measures through its comprehensive and sound legal, institutional, policy and supervisory frameworks to ensure that Mauritius is not a safe haven for money launderers and terrorist financiers.

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. Mauritius is committed to the fight against money laundering and terrorist financing and is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

This guidance is based on the laws and regulations as of May 2019. It covers the prevention of money laundering and the countering of terrorist financing. It is intended to be read by anyone who provides audit, accountancy, tax advisory and insolvency in Mauritius.

1.2. Background

Mauritius is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a regional inter-governmental body established to combat money laundering and terrorism financing in the eastern and southern African region. ESAAMLG members adopted a Memorandum of Understanding which established the Group and provided the basis that would enable them to forge the process of cooperation for implementing the Recommendations of the Financial Action Task Force. In February 2012, the FATF issued revised Recommendations which set out a number of new requirements compelling its members to implement in order to effectively combat money laundering and terrorism financing. Mauritius was assessed by ESAAMLG in relation to its anti-money laundering and counter-terrorist financing (AML/CFT) system, using the

FATF Assessment Methodology 2013. The assessment comprised a comprehensive review of the effectiveness of Mauritius' AML/CFT system and its level of compliance with the FATF Recommendations. The Mutual Evaluation Report (MER) was published in September 2018. The MER has identified the strengths and weaknesses of the systems and procedures in place in Mauritius for combating money laundering and terrorism financing and has made a number of recommendations to enable Mauritius improve its systems and procedures. In this respect, Mauritius has amended the FIAMLA, POCA, POTA and enacted the FIAML Regulations and UN Sanctions Act in order to meet the FATF requirements and improve its AML/CFT framework. As it currently stands, all statutes pertaining to AML/CFT apply to all Financial Institutions (FIs) and the Designated Non-Financial Businesses and Professions (DNFBPs)[4].

1.3. What is the purpose of this Guidance?

This guidance has been prepared to help accountants (including tax advisers and insolvency practitioners) comply with their obligations under Mauritius legislation to prevent, recognise and report money laundering and terrorism financing. Compliance with it will ensure compliance with the relevant legislation (including that related to counter terrorist financing) and professional requirements.

The Mauritius anti-money laundering and terrorism financing regime applies only to defined services carried out by designated businesses. This guidance assumes that many businesses will find it easier to apply certain AML/CFT processes and procedures to all of their services, but this is a decision for the business itself. It can be unnecessarily costly to apply anti-money laundering provisions to services that do not fall within the Mauritius AML regime.

1.4. Powers of the Regulatory Body

According to section 19H of the FIAMLA, a regulatory body shall have such powers as are necessary to enable it to effectively discharge its functions and may, in particular –

a) issue guidelines for the purposes of combating money laundering activities and the financing of terrorism and proliferation activities;

[4] DNFBPs include accounting and auditing professionals as a whole.

b) give directions to a member falling under its purview to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made, and guidelines issued under those Acts;

c) require a member falling under its purview to submit a report on corrective measures it is taking to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts, at such intervals as may be required by the regulatory body.

d) With respect to a member falling under its purview, the regulatory body may apply any or all of the following administrative sanctions – (i) issue a private warning; (ii) issue a public censure; (iii) impose such administrative penalty as may be prescribed by the regulatory body; (iv) ban, where the regulatory body has licensed or authorised the member to conduct his business or profession, from conducting his profession or business for a period not exceeding 5 years; and (v) revoke or cancel a licence, an approval or an authorisation, as the case may be.

1.5. Request of Information

As per section 19J of the FIAMLA, a regulatory body may require a member falling under its purview to furnish any information and produce any record or document within such time as it may determine. Failing to comply with such requirement may constitute an offence punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 2 years.

1.6. Onsite Inspections

Section 19K of the FIAMLA states that a regulatory body may at any time audit and inspect the books and records of a member falling under its purview in order to (i) verify that the member is compliant with the FIAMLA and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (UN Sanctions Act); and (ii) direct orally or in writing the member to produce documents or material that is relevant to inspection. Any person who intentionally obstructs and fails without any reasonable excuse to comply with any direction of the regulatory body shall commit an offence and be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years. Additionally, any person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal

of, any document, information stored on a computer or other device or other thing that the person knows or ought reasonably to have known is relevant to an onsite inspection or investigation, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

1.7. Who is this Guidance for?

1. A Professional Accountant;
2. Public Accountant;
3. And Member Firm under the Financial Reporting Act, who prepares for, or carries out, transactions for his client concerning the following activities:

i. buying and selling of real estate;
ii. managing of client money, securities or other assets;
iii. management of bank, savings or securities accounts;
iv. organisation of contributions for the creation, operation or management of legal persons such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed;
v. creating, operating or management of legal persons such as a company, a foundation, an association, a limited liability partnership or such other entity as may be prescribed, or legal arrangements, and buying and selling of business entities.

1.8. Compliance with Guidelines and Enforcement

According to section 10(3) of the FIAMLA a*ny institution to which, or person to whom, guidelines are issued under subsection (2) (ba) or (c) shall comply with those guidelines*. Furthermore, section 10(4) of the FIAMLA stipulates that *Where an institution or a person fails to comply with guidelines issued under subsection (3), the institution or person shall be liable to pay a penalty not exceeding 50,000 rupees for each day on which such breach occurs as from the date on which the breach is notified.*

CHAPTER 2: MONEY LAUNDERING AND THE FINANCING OF TERRORISM

2.1. What is Money Laundering?

Money laundering is the funnelling of cash or other funds generated from illegal activities through financial institutions or businesses to conceal or disguise the true ownership and source of the funds. Money laundering comes in varying forms and degrees and affects almost all countries. Under section 3 of the FIAMLA, the definition is broader as it puts a layer of obligation on members of a relevant profession and occupation to prevent its services from being used to commit money laundering and the financing of terrorism. It also captures the elements of conspiracy under section 4 of the FIAMLA.

Generally, the process of money laundering comprises three stages:

(a) Placement: the physical disposal of initial proceeds from illegal activities. Placement involves the introduction of illegal proceeds into the financial system or carrying of cash across borders.

(b) Layering: the process of generating a series or layers of financial transactions to separate these proceeds from their illegal source designed to obscure the audit trail.

(c) Integration: the process of the unnoticed reintroduction of the illegal proceeds into the economy. The purpose of integration is to allow the money launderers to use the funds through legitimate-appearing transactions without raising suspicion.

The three stages may occur as separate and distinct phases or may overlap.

The ability to launder the proceeds from criminal activities through the financial system is a key element to the success of criminal operations. Maintaining the integrity of the financial system depends on countering the money laundering activities and attracting and retaining legitimately earned funds.

2.2. What is Terrorism Financing?

Terrorist financing, as defined under section 2 of the UN Sanctions Act, means the financing of terrorist, terrorist acts and terrorist organisations. Sources of terrorism financing may be legitimate or illegitimate. Governments, large organisations as well as individuals often collect, provide and donate funds to terrorist groups, or the funds can be generated through revenue-generating

activities through legitimate businesses owned by terrorist organisations. Income may also be derived from unlawful activities such as smuggling, frauds, extortion and narcotics trafficking.

The methods used by terrorist organisations to obtain, move or conceal funds for their activities can be similar to those used by criminal organisations to launder their funds.

2.3. Proliferation Financing

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles). Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organizations or acting as representatives or middlemen.

CHAPTER 3: ESTABLISHING A RISK-BASED APPROACH

3.1. Risk-Based Approach

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. It is an obligation for accountants to assess and understand their ML/TF risks pursuant to Section 17 of FIAMLA. Mauritius completed its NRA in August 2019. The ML risk for the accountancy sector was found to be Medium Low. It is highlighted that accountants should take into account the outcome of the National Risk Assessment[5] when applying CDD measures in relation to each customer.

The RBA to AML/CFT means that accountants should identify, assess and understand the Money Laundering and Terrorism Financing risks to which they are exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

For accountants, identifying ML/TF risks and maintaining an understanding of the ML/TF risks faced by the sector as well as specific to their services, client base, the jurisdictions in which they operate, the Delivery channels and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training. For supervisors, this will also require maintaining an understanding of the ML/TF risks specific to their area of supervision, and the degree to which AML/CFT measures can reasonably be expected to mitigate such risks.

The RBA is not a "zero failure" approach; there may be occasions where an accountancy practice has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks but is still used for ML or TF purposes in isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that accountants must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

3.2. Implementing a Risk-Based Approach to AML/CFT Obligations

The general principle of a RBA is that, where there are higher risks, enhanced measures should be taken to manage and mitigate those risks. The range, degree, frequency or intensity of preventive

[5] The public version of the NRA report may be accessed here:
https://www.mipa.mu/assets/upload/attachment/866273907_NRA%20Public%20Report%202019-compressed.pdf

measures and controls conducted should be stronger in higher risk scenarios. Accountants are required to apply each of the CDD measures under as below:

a) identification and verification of the client's identity;
b) identification and taking reasonable measures to verify the identity of the beneficial owner;
c) understanding the purpose and nature of the business relationship; and
d) on-going monitoring of the relationship.

However, where the ML/TF risk is assessed as lower, the degree, frequency and/or the intensity of the controls conducted will be relatively lighter. Where risk is assessed at a normal level, the standard AML/CFT controls should apply.

3.2.1 Consideration of the engagement in client relationships

Accountants are not obliged to avoid risk entirely. Even if the services they provide to their clients are considered vulnerable to the risks of ML/TF based on risk assessment, it does not mean that all accountants and all their clients or services pose a higher risk when taking into account the risk mitigating measures that have been put in place.

3.3. Guidance for Accountants on implementing a Risk-Based Approach

3.3.1 Risk Identification and Assessment

Accountants should take appropriate steps to identify and assess the risk firm-wide, given their particular client base, that they could be used for ML/TF. This is usually performed as part of the overall client engagement and acceptance processes. They should document those assessments, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to competent authorities and supervisors. The nature and extent of any assessment of ML/TF risks should be appropriate to the type of business, nature of clients and size of operations.

3.3.2 Factors to determine Risks

The risks the sector faces depend on variety of factors, namely:

a) country/geographic risk,
b) client risk and
c) transaction and delivery channel risk[6]

[6] Including products, transactions or delivery channels.

d) products and services provided

The risks and red flags listed in each category are not exhaustive but provide a starting point for accountants to use when designing their RBA.

When assessing risk, accountants should consider all the relevant risk factors before determining the level of overall risk and the appropriate level of mitigation to be applied. Such risk assessment may well be informed by findings of the NRA, the supra-national risk assessments, sectoral reports conducted by competent authorities on ML/TF risks that are inherent in accounting services/sector, risk reports in other jurisdictions where the accountant based in, and any other information which may be relevant to assess the risk level particular to their practice. For example, press articles and other widely available public information highlighting issues that may have arisen in particular jurisdictions. Accountants may well also draw references to FATF Guidance on indicators and risk factors. During the course of a client relationship, procedures for ongoing monitoring and review of the client's risk profile are also important.

Due to the nature of services that an accountant generally provides, automated transaction monitoring systems of the type used by financial institutions will not be appropriate for most accountants. There may be some scope to use artificial intelligence and analytical tools in an audit context to spot unusual transactions. The accountant's knowledge of the client and its business will develop throughout the duration of a longer term and interactive professional relationship (in some cases, such relationships may exist for short term clients as well, e.g. for property transactions).

However, although individual accountants are not expected to investigate their client's affairs, they may be well positioned to identify and detect changes in the type of work or the nature of the client's activities in the course of business relationship. Accountants will also need to consider the nature of the risks presented by short-term client relationships that may inherently, but not necessarily be low risk (e.g. one-off client relationship). Accountants should also be mindful of the subject matter of the professional services (the engagement) being sought by an existing or potential client and the related risks.

Identification of the ML/TF risks associated with certain clients or categories of clients, and certain types of work will allow accountants to determine and implement reasonable and proportionate measures and controls to mitigate such risks. The risks and appropriate measures will depend on the nature of the accountant's role and involvement. Circumstances may vary considerably

between professionals who represent clients on a single transaction and those involved in a long-term advisory relationship.

The amount and degree of ongoing monitoring and review will depend on the nature and frequency of the relationship, along with the comprehensive assessment of client/transactional risk. An accountant may also have to adjust the risk assessment of a particular client based upon information received from a designated competent authority, SRB or other credible sources (including a referring accountant).

The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential ML/TF may vary given the size, sophistication, nature and scope of services provided by the accountant and/or firm. These criteria, however, should be considered holistically and not in isolation. Accountants, based on their individual practices and reasonable judgements, will need to independently assess the weight to be given to each risk factor.

Although there is no universally accepted set of risk categories, the examples provided in this Guidelines are the most commonly identified risk categories. There is no single methodology to apply these risk categories, and the application of these risk categories is intended to provide a suggested framework for approaching the assessment and management of potential ML/TF risks. For smaller firms and sole practitioners, it is advisable to look at the services they offer (e.g. providing company management services may entail greater risk than other services).

A practical starting point for accounting firms (especially smaller firms) and accountants (especially sole practitioners) would be to take the following approach. Many of these elements are critical to satisfying other obligations owed to clients, such as fiduciary duties, and as part of their general regulatory obligations:

a) Client acceptance and know your client policies: identify the client (and its beneficial owners where appropriate) and the true "beneficiaries" of the transaction. Obtain an understanding of the source of funds and source of wealth[7] of the client.

[7] The source of funds and the source of wealth are relevant to determining a client's risk profile. The source of funds is the activity that generates the funs for a client (e.g. salary, trading revenues, or payments out of a trust), while the source of wealth describes the activities that have generated the total net worth of a client (e.g. ownership of a business, inheritance, or investments). While these may be the same for some clients, they may be partially or entirely different for other clients. For example, a PEP who receives a modest official salary, but who has substantial funds, without any apparent business interests or inheritance, might raise suspicions of bribery, corruption or misuse of position. Under the RBA, accountants should satisfy themselves that adequate information is available to assess a client's source

b) Engagement acceptance policies: Understand the nature of work. Accountants should know the exact nature of the service that they are providing and have an understanding of how that work could facilitate the movement or obscuring of the proceeds of crime. Where an accountant does not have requisite expertise, the accountant should not undertake the work.

c) Understand the commercial or personal rationale for the work: Accountants need to be reasonably satisfied that there is a commercial or personal rationale for the work undertaken. Accountants however are not obliged to objectively assess the commercial or personal rationale if it appears reasonable and genuine.

d) Be attentive to red flag indicators: exercise vigilance in identifying and then carefully reviewing aspects of the transaction if there are reasonable grounds to suspect that funds are the proceeds of a criminal activity or related to terrorist financing. These cases would trigger reporting obligations. Documenting the thought process by having an action plan may be a viable option to assist in interpreting/assessing red flags/ indicators of suspicion.

e) Then consider what action, if any, needs to be taken.

f) The outcomes of the above action (i.e. the comprehensive risk assessment of a particular client/transaction) will dictate the level and nature of the evidence/documentation collated under a firm's CDD/EDD procedures (including evidence of source of wealth or funds).

g) Accountants should adequately document and record steps taken under a) to e).

3.3.2.1 Country/Geographic Risk

a) A client may be higher risk when features of their business are connected to a higher risk country as regards:

i. the origin, or current location of the source of wealth or funds;

ii. where the services are provided;

iii. the client's country of incorporation or domicile;

iv. the location of the client's major operations;

v. the beneficial owner's country of domicile; or

of funds and source of wealth as legitimate with a degree of certainty that is proportionate to the risk profile of the client.

vi. target company's country of incorporation and location of major operations (for potential acquisitions).

b) There is no universally agreed definition of a higher risk country or geographic area but accountants should pay attention to those countries that are:

i. Countries/areas identified by credible sources [8]as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

ii. Countries identified by credible sources as having significant levels of organized crime, corruption, or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling.

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

iv. Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by FATF statements as having weak AML/CFT regimes, in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions.

v. Countries identified by credible sources to be uncooperative in providing beneficial ownership information to competent authorities, a determination of which may be established from reviewing FATF mutual evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards.

3.3.2.2. Client Risk

The levels of risks associated with the client base could include for example, (I) **prohibited clients** (i.e., clients that are prime candidates for prohibited transactions, a list of designated persons/ entities on any sanctions Lists such as the Un Sanctions List[9] , persons whose assets may have been frozen under section 45 of the Dangerous Drugs Act, (ii) clients considered as **high risk** (for example, Politically Exposed Persons), (iii) **medium risk** client, (iv) **low/standard risk** client.

[8] "Credible sources" refers to information that is produced by reputable and universally recognised international organisations and other bodies that make such information publicly and widely available. In addition to the FATF and FATF-style regional bodies, such sources may include, but are not limited to, supra-national or international bodies such as the International Monetary Fund, the World Bank and the Egmont Group of Financial Intelligence Units.

[9]https://www.mipa.mu/assets/upload/attachment/United_Nations_Security_Council_Consolidated_List_06.01.2020.pdf

The type of client may also pose ML/FT risks, e.g., individuals, listed companies, private companies, joint ventures, partnerships, etc. The following is a list of type of clients and the level of risks associated with them. Note that this is not a prescriptive list, nor does it imply that the risk is the same across all accounting sector, i.e., it may be low risk for one accountant and considered as high risk for another.

Identification of high-risk clients may be based on the following:

- The firm's client base includes industries or sectors where opportunities for ML/TF are particularly prevalent.
- The firm's clients include PEPs or persons closely associated with or related to PEPs, who are considered as higher risk clients.
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances (as evaluated taking into account all the circumstances of the client's representation).
- Clients where the structure or nature of the entity or relationship makes it difficult to identify in a timely manner the true beneficial owner or controlling interests or clients attempting to obscure understanding of their business, ownership or the nature of their transactions, such as unexplained use of shell and/or shelf companies, front company, legal entities with through nominee shares or bearer shares and unexplained use of informal arrangements such as family or close associates acting as nominee shareholders or directors.
- Client companies that operate a considerable part of their business in or have major subsidiaries in countries that may pose higher geographic risk.
- Clients that are cash (and/or cash equivalent) intensive businesses for example Money or Value Transfer Services (MVTS) businesses, Operators, Brokers, Casinos and Dealers in precious metals and stones.
- Non-profit or charitable organizations engaging in transactions for which there appears to be no logical economic purpose or where there appears to be no link between the stated
- Clients who appear to be acting on somebody else's instructions without disclosure.
- Clients who appear to actively and inexplicably avoid face-to-face meetings.
- Clients who have no address, or multiple addresses without legitimate reasons.

- Clients who have funds that are obviously and inexplicably disproportionate to their circumstances (e.g. their age, income, occupation or wealth).
- Clients who insist, without adequate justification or explanation, that transactions be effected exclusively or mainly through the use of virtual assets for the purpose of preserving their anonymity.
- The relationship between employee numbers/structure and nature of the business is divergent from the industry norm (e.g. the turnover of a company is unreasonably high considering the number of employees and assets used compared to similar businesses).

3.3.2.3 Transaction and Delivery Channel Risks

Services which may be provided by accountants and which (in some circumstances) risk being used to assist money launderers may include:

- Use of pooled client accounts or safe custody of client money or assets without justification.
- In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting as trustees of such a trust.
- Services where accountants may in practice represent or assure the client's standing, reputation and credibility to third parties, without a commensurate knowledge of the client's affairs.
- Services that are capable of concealing beneficial ownership from competent authorities.
- Non-cash wire transfers through the use of many inter-company transfers within the group to disguise the audit trail.
- Services that rely heavily on new technologies (e.g. in relation to initial coin offerings or virtual assets) that may have inherent vulnerabilities to exploitation by criminals, especially those not regulated for AML/CFT.
- Transfer of real estate or other high value goods or assets between parties in a time period that is unusually short for similar transactions with no apparent legal, tax, business, economic or other legitimate reason.
- Transactions using unusual means of payment (e.g. precious metals or stones).

- Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.
- Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner) with no apparent legal, tax, business, economic or other legitimate reason.
- Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment.
- Existence of suspicions regarding fraudulent transactions, or transactions that are improperly accounted for. These might include:

i. Over or under invoicing of goods/services.

ii. Multiple invoicing of the same goods/services.

iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading).

iv. Multiple trading of goods/services.

In relation to the areas of risk identified above, accountants may also consider the examples of fraud risk factors listed in International Standard of Auditing 240: The auditor's responsibilities relating to fraud in an audit of financial statements (ISA 240). Even where the accountant is not performing an audit, ISA 240 and ISA 315 provide helpful lists of additional red flags.

3.3.2.4 Products and Services Provided

An essential element of risk assessment is to review new and existing services that Accountants offer to determine how they may be used to launder money or finance terrorism. For instance, some services can be used to conceal the ownership or the source of property, such as:

- Services in relation to complex transactions/ enabling significant volumes of transactions to occur rapidly;
- Services allowing customer to engage in transactions with minimal oversight by the institution; and
- Services allowing levels of anonymity to the users.

3.3.2.5 Variables that may Impact on a RBA and risk

- While all accountants should follow robust standards of due diligence in order to avoid regulator arbitrage, due regard should be accorded to differences in practices, size, scale and expertise amongst accountants, as well as the nature of the clients they serve. As a result, consideration should be given to these factors when creating a RBA.
- Consideration should also be given to the resources that can be reasonably allocated to implement and manage an appropriately developed RBA. For example, a sole practitioner would not be expected to devote an equivalent level of resources as a large firm; rather, the sole practitioner would be expected to develop appropriate systems and controls and a RBA proportionate to the scope and nature of the practitioner's practice and its clients. Small firms serving predominantly locally based and low risk clients cannot generally be expected to devote a significant amount of senior personnel's time to conducting risk assessments. In such cases, it may be more reasonable for sole practitioners to rely on publicly available records and information supplied by a client for a risk assessment than it would be for a large firm having a diverse client base with different risk profiles. However, where the source is a public registry, or the client, there is always potential risk in the correctness of the information. Sole practitioners and small firms may be regarded by criminals as more of a target for money launderers than large firms.

3.3.2.6 Documentation of Risk Assessments

- Accountants must always understand their ML/TF risks (for clients, countries or geographic areas, services, transactions or delivery channels). They should document those assessments in order to be able to demonstrate their basis and exercise due professional care and use compelling good judgement.
- Accountants may fail to satisfy their AML/CFT obligations, for example by relying completely on a checklist risk assessment where there are other clear indicators of potential illicit activity. Completing risk assessments in a time efficient yet comprehensive manner has become more important.
- Each of these risks could be assessed using indicators such as low risk, medium risk and/or high risk. A short explanation of the reasons for each attribution should be included and an overall assessment of risk determined. An action plan (if required) should then be outlined to accompany the assessment and dated. In assessing the risk profile of the client at this

stage, reference must be made to the relevant targeted financial sanctions lists to confirm neither the client nor the beneficial owner is designated and included in any of them.

- A risk assessment of this kind should not only be carried out for each specific client and service on an individual basis, but also to assess and document the risks on a firm-wide basis, and to keep risk assessment up-to-date through monitoring of the client relationship. The written risk assessment should be widely shared throughout the firm not only those that have AML/CFT functions.

3.3.2.7 Risk Assessment Tool

A risk assessment tool at Annex 1 provides an example, for use by accountants, to facilitate the assessment of the above factors.

However, an accountant's risk assessment has to be appropriate for their specific business needs which means that it may have to be more detailed than the checklist provided. Accountants can customise the checklist or can use a different method or another tool.

3.4. Risk Mitigation

The second component of a risk-based approach is risk mitigation. Risk mitigation is about implementing measures to limit the potential money laundering and terrorist financing risks the reporting entity has identified while staying within its risk tolerance level. Pursuant to Section 17A of FIAMLA, accountants must establish policies, controls and procedures to mitigate and manage the ML/TF risks that they have identified as part of their assessment.

Accountants should have policies, controls and procedures that enable them to effectively manage and mitigate the risks that they have identified (or that have been identified by the country). They should monitor the implementation of those controls and enhance or improve them if they find the controls to be weak or ineffective. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether

higher or lower) should be consistent with national requirements and with guidance from competent authorities and supervisors. Measures and controls may include:

a) General training on ML/TF methods and risks relevant to accountants
b) Targeted training for awareness by the accountants providing specified activities to higher risk clients or to accountants undertaking higher risk work.
c) Increased or more appropriately targeted CDD or enhanced CDD for higher risk clients/situations that concentrate on providing a better understanding about the potential

source of risk and obtaining the necessary information to make informed decisions about how to proceed (if the transaction/ business relationship can be proceeded with). This could include training on when and how to ascertain, evidence and record source of wealth and beneficial ownership information if required.

d) Periodic review of the services offered by the accountant, and the periodic evaluation of the AML/CFT framework applicable to the accountant and the accountant's own AML/CFT procedures, to determine whether the ML/TF risk has increased.

e) Reviewing client relationships from time to time to determine whether the ML/TF risk has increased.

The development of a robust AML/CFT program is thus a crucial component of risk mitigation. Annex 1A provides a list of risk mitigation measures that may be appropriate for situations that you have determined to be high risk.

3.5. Risk Monitoring

In addition to risk assessment and risk mitigation activities, a risk-based approach also requires accountants/ accountancy firms to take measures to conduct on-going monitoring of financial transactions when there is a business relationship. The level of monitoring should be adapted according the ML/TF risks as outlined in the entity's risk assessment. The purpose of on-going monitoring activities is to help detect suspicious transactions. The accountant's policies, controls and procedures have to determine what kind of monitoring is done for particular high-risk situations, including how to detect suspicious transactions. The policies, controls and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

3.6. AML/CFT Program

An AML/CFT program is required to identify, mitigate and manage the risk of the products or services being offered by accountants that could facilitate money laundering or terrorism financing. As previously mentioned, AML/CFT programs should be risk-based. This means that accountants must develop their own program, tailored to their situation to mitigate money laundering and terrorism financing risks. This approach recognises that not all aspects of an institution' business present the same level of risks. The reporting person is in the best position to

assess the risk of its clients, products and services and to allocate resources to counter the identified high-risk areas.

The basics of an AML/CFT program consist of the following elements:

- Internal policies, procedures and controls;
- Nomination of a compliance officer and Money Laundering Reporting Officer (MLRO) at the management level;
- On-going Employment Screening and Training Program; and
- Independent Audit function to test the AML/CFT program.

3.6.1. Internal policies, procedures and controls

The law mandates that every reporting person, pursuant to section 17A of the FIAMLA, shall-

i. Establish policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the reporting person;

ii. Monitor the implementation, review and update the policies, controls and procedures

iii. Maintain a record in writing of-

- the policies, controls and procedures
- any changes to the policies, controls and procedures
- the steps taken to communicate those policies, controls and procedures internally; and

iv. establish policies, controls and procedures that are proportionate to the size and nature of the business of a reporting person which must be approved by the senior management.

Annex 2 provides a template to assist dealers in the development of internal policies, procedures and controls.

Strong leadership and engagement by senior management and the Board of Directors (or equivalent body) in AML/CFT is an important aspect of the application of the RBA. Senior management must create a culture of compliance, ensuring that staff adhere to the firm's policies, procedures and processes designed to limit and control risks.

The nature and extent of the AML/CFT controls, as well as meeting national legal requirements, need to be proportionate to the risk involved in the services being offered. In addition to other

compliance internal controls, the nature and extent of AML/CFT controls will encompass a number of aspects, such as:

a) designating an individual or individuals, at management level responsible for managing AML/CFT compliance;
b) designing policies and procedures that focus resources on the firm's higher-risk, services, products, clients and geographic locations in which their clients/they operate, and include risk-based CDD policies, procedures and processes;
c) ensuring that adequate controls are in place before new services are offered; and
d) ensuring adequate controls for accepting higher risk clients or providing higher risk services, such as management approval.

These policies and procedures should be implemented across the firm include:

a) performing a regular review of the firm's policies and procedures to ensure that they remain fit for purpose;
b) performing a regular compliance review to check that staff are properly implementing the firm's policies and procedures;
c) providing senior management with a regular report of compliance initiatives, identifying compliance deficiencies, corrective action taken, and STRs filed;
d) planning for changes in management, staff or firm structure so that there is compliance continuity;
e) focusing on meeting all regulatory record-keeping and reporting requirements, recommendations for AML/CFT compliance and providing for timely updates in response to changes in regulations;
f) enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;
g) incorporating AML/CFT compliance into job descriptions and performance evaluations of appropriate personnel;
h) providing for appropriate training to be given to all relevant staff;
i) having appropriate risk management systems to determine whether a client, potential client, or beneficial owner is a PEP or a person subject to applicable financial sanctions;

j) providing for adequate controls for higher risk clients and services, as necessary (e.g. additional due diligence, evidencing the source of wealth and funds of a client and escalation to senior management, or additional review and/or consultation);

k) providing increased focus on the accountant/accounting firm's operations (e.g. services, clients and geographic locations) that are more vulnerable to abuse for ML/TF;

l) providing for periodic review of the risk assessment and management processes, taking into account the environment within which the accountant/accounting firm operates and the services it provides; and

m) providing for an AML/CFT compliance function and review programme, as appropriate, given the scale of the organisation and the nature of the accountant's practice.

Depending on the size of the firm, the types of services provided, the risk profile of clients and the overall assessed ML/TF risk, it may be possible to simplify internal procedures. For example, for sole practitioners, providing limited services to low risk clients, client acceptance may be reserved to the sole owners/proprietors taking into account their business and client knowledge and experience. The involvement of the sole owner/proprietor may also be required in detecting and assessing possible suspicious activities. For larger firms, serving a diverse client base and providing multiple services across geographical locations, more sophisticated procedures are likely to be necessary.

3.6.2. Appointment of Compliance Officer and Money Laundering Reporting Officer

The compliance officer (CO), who must be part of senior management is responsible for ensuring that the Accountant is complying with its AML/CFT obligations.

The Accountant must ensure that the CO:

(a) has timely and unrestricted access to the records of the Accountant;

(b) has sufficient resources to perform his or her duties;

(c) has the full co-operation of the Accountant's staff;

(d) is fully aware of his or her obligations and those of the Accountant; and

(e) reports directly to, and has regular contact with, the Board (where applicable) so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and the Regulations issued thereunder, are being met and that the legal professional s taking sufficiently robust measures to protect itself against the potential risk of being used for ML

and TF. Where there is no Board, the CO must report directly to the business owner or to any other senior officer appointed by the owner.

In accordance with Regulation 22(3) of the FIAML Regulations 2018, the functions of the CO include:

(a) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the legal professional where applicable and senior management;

(b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

(c) regular reporting, including reporting of non-compliance, to the Board where applicable and senior management; and

(d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("MLRO") and CO, provided the Accountant/ Accountancy firm consider this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

In accordance with Regulations 26(1) of FIAML Regulations 2018, Accountants shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism. The MLRO must be sufficiently senior within the organization and must have the technical skills required to make an assessment of internal reports prior to determining whether an STR should be filed with the FIU. There should be clear reporting lines internally, to ensure that all employees including directors or partners, know what the process is to report any suspicion that they may have internally to the MLRO. Records must be kept by the accountant of both internal and external disclosures. Where due to its size or the nature of its business an Accountant cannot appoint an MLRO, it must nevertheless have documented policies and procedures in place to ensure that it is complying with the FIAMLA and the 2018 Regulations. In these instances, the STR is filed by the Accountant with the FIU directly.

3.6.3 Employment Screening and Training

3.6.3.1. Employment Screening

Accountants are required, under Regulation 22(1) (b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees. In light of the above, significance may be given to:

- Obtaining and confirming proper references at the time of recruitment;
- Requesting information from the member of staff with regard to any regulatory action taken against him; and
- Requesting information from the member of staff pertaining to any criminal convictions and the provision of a check of his criminal record (for instance, requiring a Certificate of Character).

3.6.3.2. Employee Training

Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against money laundering and terrorism financing should be in place to include ongoing training programme for the directors, officers and employees accountants/accountancy firms, to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to:

i. assist them in recognizing transactions and actions that may be linked to money laundering or terrorism financing;
ii. and instruct them in the procedures to be followed where any links have been identified under subparagraph (i).

A training program should be designed to train the appropriate personnel on a regular basis. A successful training program not only should meet the standards set out in laws (i.e. FIAMLA Act 2002) but should also satisfy internal policies and procedures in place. For the purpose of this "Guidelines", training includes not only formal training courses, but also communications that serves to educate and inform employees such as e-mails, newsletters, periodic team meetings and anything else that facilitates sharing of information. Topics to be taught in the training program vary according to target audience and services being offered but several basic matters should be factored into the program:

- Policies and Procedures in place to prevent money laundering and financing of terrorism for instance identification, record-keeping, the recognition and reporting of suspicious transactions;

- Legal Requirements under relevant AML/CFT legislations and the statutory obligations under these laws;
- Understanding ML/TF risk of the sector and of their firm;
- Penalties for anti-money laundering violations;
- How to react when facing a suspicious client or transaction;
- Duties and accountabilities of employees; and
- New developments together with information on current money laundering and financing of terrorism techniques, methods and trends.

Firms should provide targeted training for increased awareness by the accountant providing specified activities to higher-risk clients and to accountants undertaking higher- risk work. Case studies (both fact-based and hypotheticals) are a good way of bringing the regulations to life and making them more comprehensible. Training should also be targeted towards the role that the individual performs in the AML/CFT process. This could include false documentation training for those undertaking identification and verification duties, or training regarding red flags for those undertaking client/transactional risk assessment.

Lastly, it would be advisable for firms to keep a record of all anti-money laundering and combating the financing of terrorism training delivered to their employees.

3.6.4 Auditing AML/CFT Program

Putting in place an AML/CFT Program is not sufficient; the program must be monitored and evaluated. The Accountant/ Accountancy Firm should assess their anti-money laundering and combating the financing of terrorism programs at a minimum every two years to ensure their effectiveness and to look for new risk factors. The audit program should address issues such as (i) the adequacy of its ML/TF risk assessment, (ii) the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements, (iii) the adequacy of its risk-based approach in relation to the services offered clients and geographic locations, (iv) the training adequacy, including its comprehensiveness, accuracy of materials, training schedule, (v) compliance with applicable laws, (vi) the system's ability to identify unusual activity, (vii) the adequacy of recordkeeping and (viii) the review of its Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others. The audit can be conducted by an internal or external auditor. If the reporting entity

does not have an auditor, it can conduct a self-review. The self-review should be conducted by an individual who is independent of the compliance-monitoring functions and should not be conducted by the compliance officer. This could be an employee or an outside consultant. For sole practitioners, the review can be conducted by the sole practitioner directly. The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements. The results of the audit should be documented and presented either to the Board of Directors (if applicable) or to senior management. The recommended changes should be implemented no later than a month following the completion of the audit.

CHAPTER 4: PREVENTIVE MEASURES

4.1. Customer Due Diligence (CDD)

Both the FIAMLA and the FIAML Regulations make provision for CDD and KYC obligations and these apply to Accountants as well.

In line with section 17C of FIAMLA, Accountants need to **identify** and **verify** the true identity of the customer that they are conducting a transaction with. The identity of a customer must be established and verified using independent source documents, data or information. All CDD information collected must be kept up to date by the legal professional. Additionally, CDD information must be verified against independent and reliable sources.

In case of corporate bodies, the company's ultimate beneficial owner must be ascertained (see further below for more information on beneficial ownership) by obtaining information on their identity on the basis of documents, data or information obtained from a reliable and independent source and verifying the accuracy of the information obtained. The beneficial owner is the natural person who owns or controls the legal person or legal arrangement.

4.1.1 CDD Requirements

According to section 17C of the FIAMLA, a reporting person shall undertake CDD measures to-establish a business relationship with a customer;

- establish a business relationship with a customer;
- a transaction in an amount equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
- a domestic or cross-border wire transfer
- doubts exist the veracity or adequacy of previously obtained customer identification information.
- there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

The CDD requirements have to be in accordance with the findings of the National Risk Assessment[10] pursuant to section 19D of the FIAMLA.

[10] The public version of the NRA report may be accessed here: https://www.mipa.mu/assets/upload/attachment/866273907_NRA%20Public%20Report%202019-compressed.pdf

Accountants should design CDD procedures to enable them to establish with reasonable certainty the true identity of each client and, with an appropriate degree of confidence, know the types of business and transactions the client is likely to undertake. Accountants should have procedures to:

1. Identify the client and verify that client's identity using reliable, independent source documents, data or information.
2. Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, such that accountants are satisfied that they know who the beneficial owner is. This should include accountants' understanding of the ownership and control structure of the client.
3. Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.
4. Conduct ongoing due diligence on the business relationship. Ongoing due diligence ensures that the documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher-risk categories of clients. Undertaking appropriate CDD may also facilitate the accurate filing of suspicious transaction reports (STRs) to the financial intelligence unit (FIU), or to respond to requests for information from an FIU and the law enforcement agencies.

   In accordance with the national AML/CFT framework, accountants should design a 'standard' level of CDD for normal risk clients and a reduced or simplified CDD process for low risk clients. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF or where specific higher-risk scenarios apply. Enhanced due diligence should be applied to those clients that are assessed as high risk. These activities may be carried out in conjunction with firms' normal client acceptance procedures and should take account of any specific jurisdictional requirements for CDD.

4.2. Customer-natural person (Face to Face transactions)

Regulation 4 of the FIAML Regulations requires that the reporting person shall obtain from and verify a customer who is a natural person the following information-

- **a.** the full legal and any other names, including, marital name, former legal name or alias;
- **b.** the date and place of birth;
- **c.** the nationality;

d. the current and permanent address; and

e. such other information as may be specified by a relevant supervisory authority or regulatory body.

4.2.1. Customer Natural Persons (Non-Face to Face Transactions)

It is most vital that the procedures adopted to verify identity of clients for non-face-to-face transaction is at least as robust as those for face-to-face verification. Accordingly, in accepting transactions from non-face-to-face clients, Accountants should apply uniformly effective customer identification procedures as for those mentioned above and other specific and appropriate measures to mitigate the higher risk posed by non-face-to-face verification of clients. In addition, for non-residents requiring services from abroad, details such as true name, current permanent address, mailing address, telephone and fax number, date and place of birth, nationality, occupation and name of employer (if self-employed, the nature of the self- employment), signature/signatures, authority to obtain any data provided. Documents required are namely: the National Identity Card, current valid passports, and current valid driving licences, armed forces identity card where applicable. Documents provided should be duly certified as a true copy by a lawyer, accountant or other professional person who clearly adds to the copy (by means of a stamp or otherwise) his name, address and profession to aid tracing of the certifier if necessary and which the accountant believes in good faith to be acceptable to it for the purposes of certifying.

Customer-Legal persons (for example Companies) or Legal Arrangement (for example Trusts)

According to regulation 5 of the FIAML Regulations, where the customer is a legal person or legal entity, the reporting person shall

a. with respect to the customer, understand and document –
    i. the nature of his business
    ii. his ownership and control structure
b. identify the customer and verify his identity by obtaining the following information –
    i. name, legal form and proof of existence;
    ii. powers that regulate and bind the customer;
    iii. names of the relevant persons having a senior management position in the legal person or arrangement; and

iv. the address of the registered office and, if different, a principal place of business

Legal Arrangements

In the case of trusts, an accountant should have policies and procedures in place to identify the following and verify their identity using reliable, independent source documents, data or information (provided that an accountant's policies should enable it to disregard source documents, data or information which are perceived to be unreliable):

i. the settlor;

ii. the protector;

iii. the trustee(s), where the accountant is not acting as trustee;

iv. the beneficiaries or class of beneficiaries; and

v. any other natural person actually exercising effective control over the trust.

Settlor

An accountant establishing on behalf of a client or administering a trust, company or other legal entity or otherwise acting as or providing a trustee or director of a trust, company or other legal entity should have policies and procedures in place (using a RBA) to identify the source of funds in the trust, company or other legal entity.

It may be more difficult (if not impossible) for older trusts to identify the source of funds, where contemporaneous evidence may no longer be available. Evidence of source of funds may include reliable independent source documents, data or information, share transfer forms, bank statements, deeds of gift or letter of wishes.

Beneficiaries

An accountant should have policies and procedures in place, adopting a RBA to enable it to form a reasonable belief that it knows the true identity of the beneficiaries of the trust, and taking reasonable measures to verify the identity of the beneficiaries, such that an accountant is satisfied that it knows who the beneficiaries are. This does not require an accountant to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the accountant should at least identify and verify the identity of beneficiaries who have current fixed

rights to distributions of income or capital or who actually receive distributions from the trust (e.g. a life tenant).

Where the beneficiaries of the trust have no fixed rights to capital and income (e.g. discretionary beneficiaries), an accountant should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

Corporate settlors and beneficiaries

In certain cases, the settlor, beneficiary, protector or other person exercising effective control over the trust may be a company or other legal entity. In such a case, an accountant should have policies and procedures in place to enable it to identify (where appropriate) the beneficial owner or controlling person in relation to the entity.

In the case of a settlor that is a legal entity, an accountant should satisfy itself that it has sufficient information to understand the purpose behind the formation of the trust by the entity. For example, a company may establish a trust for the benefit of its employees or a legal entity may act as nominee for an individual settlor or on the instructions of an individual who has provided funds to the legal entity for this purpose. In the case of a legal entity acting as nominee for an individual settlor or on the instructions of an individual, an accountant should take steps to satisfy itself as to the economic settlor of the trust (i.e. the person who has provided funds to the legal entity to enable it to settle funds into the trust) and the controlling persons in relation to the legal entity at the time the assets were settled into trust. If the corporate settlor retains powers over the trust (e.g. a power of revocation), an accountant should satisfy itself that it knows the current beneficial owners and controlling persons of the corporate settlor and understands the reason for the change in ownership or control.

In the case of a beneficiary that is an entity (e.g. a charitable trust or company), an accountant should satisfy itself that it understands the reason behind the use of an entity as a beneficiary. If there is an individual beneficial owner of the entity, an accountant should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate Trustee

Where an accountant is not itself acting as trustee, it is necessary for an accountant to obtain information to enable it to identify and verify the identity of the trustee (s) and, where the trustee is a corporate trustee, identify the corporate entity, obtain information on the identity of the beneficial owners of the trustee, and take reasonable measures to verify their identity.

Where the trustee is a listed entity (or an entity forming part of a listed group) or an entity established and regulated to carry on trust business in a jurisdiction identified by credible sources as having appropriate AML/CFT laws, regulations and other measures, an accountant should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. An accountant can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body that regulates the trustee and of the regulated trustee itself).

4.2.2. Establishing and Verifying Beneficial Ownership

Section 17E(3) of the FIAMLA defines a 'beneficial owner' as a natural person:

i. Who ultimately owns or controls a customer;

ii. On whose behalf a transaction is being conducted;

iii. Includes those natural persons who exercise ultimate control over a legal person or arrangement; and

iv. Such other persons as may be prescribed.

In line with Regulation 6 of the FIAML Regulations, Accountants must identify and take reasonable measures to verify the identity of the beneficial owners. This should be done by obtaining the following information:

a. The identity of the natural persons having an ultimate controlling ownership interest in the company;

b. In the event the requirements of paragraph (a) cannot be fully satisfied, or where no natural person has control through ownership interests, the identity of the natural person who exercises control through other means; and

c. Where no natural person has been identified in (a) or (b), the identity of the natural person holding a senior management position.

When gathering the above data, Accountants must document the process as well as any difficulties encountered during. Further enquiries may be made for verification such as verifying with the Registrar of companies, that the company continues to exist and has not been, or is not in the process of being, dissolved, struck off, wound up or terminated, by conducting in cases of doubt a visit to the place of business of the company, to verify that the company exists for a legitimate trading or economic purpose.

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

A more difficult situation arises where there is a beneficial owner who is not the immediate client (e.g. in the case of companies and other entities). In such a scenario reasonable steps must be taken so that the accountant is satisfied about the identity of the beneficial owner and takes reasonable measures to verify the beneficial owner's identity. This likely requires taking steps to understand the ownership and control of a separate legal entity that is the client and may include conducting public searches as well as by seeking information directly from the client.

4.3. Third Party Reliance

In order to rely on another regulated/supervised/monitored person to perform CDD measures in accordance with section 17D of the FIAMLA you must also consider the implications of regulation 21 of the FIAML Regulations and-

i. obtain immediately the necessary information required;
ii. take steps to satisfy himself that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;
iii. satisfy himself that the party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing and has measures in place for

compliance with CDD and record keeping requirements in line with the FIAMLA and FIAML Regulations; and

iv. not rely on a third party based in a high-risk country.

A reporting person may rely on a third party that is part of the same financial group where-

i. the group applies CDD and record keeping requirements and programs against ML and TF in accordance with the FIAMLA and FIAML Regulations;

ii. the implementation of those CDD, record keeping and programs against MLF and TF is supervised at a group level by a competent authority; and

iii. any higher risk country is adequately mitigated by the group's policies to combat ML and TF.

You should note that you remain liable for any non-compliance with CDD requirements when you rely on a third party (section 17D (2) of the FIAMLA). For this reason, you should ask what CDD enquiries the third party has undertaken to ensure that there is compliance with the laws & Regulations and the risk-based approach. This is particularly important when relying on a person outside Mauritius. You should ensure that the CDD information provided to you is up to date.

Mitigating measures

A reporting person with respect to business relationships or transactions involving a high-risk country shall-

i. apply enhanced CDD measures; and

ii. apply proportionate mitigating measures including-

- the application of additional elements of enhanced due diligence;
- the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and
- the limitation of business relationships or transactions with natural persons or legal entities from the countries identified as high-risk countries.

Factors to consider when identifying a high-risk country

Regulation 24 of the FIAML Regulations lists the factors to which due consideration shall be given in identifying a high risk country. These are-

i. Strategic deficiencies in the AML/CFT legal and institutional framework in particular in relation to-

- criminalization of money laundering and terrorism financing
- measures relating to CDD
- requirements relating to record-keeping
- requirements to report suspicious transactions
- the availability and accurate and timely information of the beneficial ownership of legal persons and arrangements to competent authorities

ii. powers and procedures of the third country's competent authorities for the purposes of combating ML and TF with effective, proportionate and dissuasive sanctions;

iii. country's practice in cooperation and exchange of information with overseas competent authorities;

iv. effectiveness of the third country's system in addressing ML and TF risks;

v. to have regard to relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing ML and combating TF; and

apply Enhanced Due Diligence proportionate to the risks, to business relationships and transactions with natural and legal persons to countries identified as high risk by the FATF[11].

4.4. Inability to complete CDD measures

Where a reporting person is unable to comply with the relevant CDD measures under the FIAML Regulations, the following action shall be taken pursuant to Regulation 13 of the FIAML Regulations. Therefore, the reporting person-

i. must not open the account;

ii. must not commence the business relationship;

iii. must not perform a transaction;

iv. shall terminate the business relationship; and

v. shall file a suspicious transaction report.

[11] http://www.fatf-gafi.org/countries/#high-risk

4.5. Record-Keeping

Record keeping and quality assurance are important for supervisors to carry out risk-based approach to AML/CFT supervision on their members. Supervisors should be able to easily retrieve information while complying with the data protection rules. Having a proper and effective record keeping system ensures that the money trail is documented and allows competent authorities to have access to records that can be used as evidence in ML/TF cases.

To reflect the above, section 17F of the FIAMLA requires that a reporting person-

i. shall maintain all books and records with respect to his customers and transactions; and

ii. shall ensure that such records and books are kept for such time as specified.

The time limit to maintain such domestic and international records is 7 years after the business relationship has ended and/or after the completion of the transaction, as stipulated in section 17F (2)(b) of the FIAMLA.

The books and records shall include-

i. all records obtained through CDD measures-
   - account files;
   - business correspondence;
   - copies of all documents evidencing the identity of customers and beneficial owners;
   - records and the results of any analysis undertaken should be in accordance with the FIAMLA;

ii. records of both domestic and international transactions that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders; and

iii. copies of all suspicious transaction reports made to the FIU.

4.6. Simplified CDD

A reporting person may apply simplified CDD measures pursuant to Regulation 11 of the FIAML Regulations where-

i. lower risks have been identified;

ii. are in accordance with any guidelines issued by the MIPA; and

iii. is consistent with the NRA findings and/or any risk assessment findings of the regulatory/supervisory body, whichever is most recently issued.

It is not appropriate to apply Simplified Due Diligence measures where a reporting person-

i. knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing; or

ii. that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing. However, the low risk identified by the reporting person should be consistent with the findings of the National Risk Assessment[12] in order to comply with regulation 11 (2) of the FIAML Regulations; and

iii. apply CDD measures as prescribed and specified by a supervisory authority.

Example of Simplified CDD Measures

- Limiting the extent, type or timing of CDD measures
- Obtaining fewer elements of client identification data
- Altering the type of verification carried out on client's identity
- Simplifying the verification carried out on client's identity
- Inferring the purpose and nature of the transactions or business relationship establishing based on the type of transaction carried out or the relationship established
- Verifying the identity of the client and the beneficial owner after the establishment of the business relationship
- Reducing the frequency of client identification updates in the case of a business relationship
- Reducing the degree and extent of ongoing monitoring and scrutiny of transactions

4.7. Enhanced Due Diligence (EDD)

According to Regulation 12 of the FIAML Regulations, a reporting person must, in addition to performing the basic CDD measures, perform enhanced CDD measures in the following situations-

i. where a higher risk of money laundering or terrorist financing has been identified;

ii. where through supervisory guidance, a high risk of money laundering or terrorist financing has been identified;

iii. where a customer or an applicant for business is from a high risk third country;

[12] The public version of the NRA report may be accessed here: https://www.mipa.mu/assets/upload/attachment/866273907_NRA%20Public%20Report%202019-compressed.pdf

iv. in relation to correspondent banking relationships;
v. the customer is a PEP;
vi. where a reporting person discovers that a customer has provided false or stolen identification documentation or information and the reporting person proposes to continue to deal with that customer; and
vii. in the event of any unusual or suspicious activity.

Enhanced CDD measures include but not limited to-

i. obtaining additional information on the customer through:
   - occupation
   - volume of assets
   - information available through public databases
   - internet
ii. updating more regularly the identification data of the customer and the beneficial owner;
iii. obtaining additional information on the intended nature of the business relationship;
iv. obtaining information on the source of funds or source of wealth of the customer;
v. obtaining information on the reasons for intended or performed transactions;
vi. obtaining the approval of senior management to commence or continue the business relationship;
vii. conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination;
viii. requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards;
ix. where a reporting person determines that the beneficiary who is a legal person or legal arrangement presents a higher risk, the reporting person shall take enhanced due diligence measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout; and
x. where the beneficiary of a life insurance policy is identified as a relevant risk factor when determining whether enhanced CDD measures are required.

In any event, if the reporting person is unable to perform Enhanced CDD where it is required under the law, he shall terminate the business relationship and shall file a suspicious transaction report under section 14 of the FIAMLA.

4.8. Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) have been a focus of the FATF as there are concerns that PEPs have used their political position to corruptly enrich themselves. You should take a risk-based and proportionate approach to identifying PEPs and then apply EDD measures and treat business with PEPs on a case by case basis.

PEPs have been classified as "domestic PEPs," "foreign peps" and "international organization PEPs" in the FIAML Regulations. A domestic PEP means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

Foreign PEPs have the same definition as above insofar as they are entrusted with prominent public function by a foreign country.

An "international organization PEP" means a person who is or has been entrusted with a prominent function by an international organization and included members of senior management or individuals who have been entrusted with equivalent functions including directors, deputy directors and members of the board or equivalent functions and such other person or category of person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

4.9.1 Examples on who may be a PEP

- Heads of state
- Heads of government
- Ministers and deputy or assistant ministers
- Members of parliament or similar legislative bodies
- Members of governing bodies of political parties
- Members of supreme courts, or any judicial body whose decisions are not subject to further

appeal, except in exceptional circumstances

- members of courts of auditors or of the boards of central banks
- ambassadors, charges d' affaires and high-ranking officers in the armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board of equivalent function of an international organization

In addition to the primary PEPs listed above, a PEP also includes (regulation 15(5) FIAML Regulations)-

i. close associates mean-
   - an individual who is closely connected to a PEP, either socially or professionally; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

ii. family members mean-
   - an individual who is related to a PEP either directly through consanguinity, or through marriage or similar forms of partnership; and
   - any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

4.9.2 How to identify a PEP?

You are not required to conduct extensive investigations to establish whether a person is a PEP. You can use information that is in your possession or publicly known. Many practices use subscriber services that can run checks against the PEPs databases which they maintain. If your practice regularly encounters PEPs, you should consider a subscription as otherwise it is easy to 'miss' PEPs in your client database including at the ultimate beneficial ownership level.

To assess your PEP risk profile, you must take into account your risk assessment, the level of risk of money laundering or terrorist financing inherent in your business and the extent to which that risk would be increased by a business relationship with a PEP. If the risk of you acquiring a PEP as a client is low, you may simply wish to ask clients whether they fall within any of the PEP categories. Where they say no, you may reasonably assume the individual is not a PEP unless

anything else within the retainer, or that you otherwise become aware of, makes you suspect they may be a PEP. Where you have a higher risk of having PEPs as clients or you have reason to suspect that a person may actually be a PEP contrary to earlier information, you should consider conducting some form of electronic verification. You may find that a web-based search engine will be sufficient for these purposes, or you may decide that it is more appropriate to conduct electronic checks through a reputable international electronic verification provider. The range of PEPs is wide and constantly changing, so electronic verification will not give you 100 per cent certainty.

You should remain alert to situations suggesting the client is a PEP. Such situations include-

i. receiving funds in the retainer from a government account;
ii. correspondence on official letterhead from the client or a related person;
iii. general conversation with the client or person related to the retainer linking the person to a PEP; and
iv. news reports which come to your attention suggesting your client is actually a PEP or linked to one.

4.9.3. Enhanced Monitoring and Supervision of PEPS

Business relationships with PEPs pose a greater than normal money laundering risk to Accountants, by virtue of the possibility for them to have benefitted from proceeds of corruption, as well as the potential for them (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

As such, Accountants are required to have a clear policy in relation to transactions involving such persons. Accountants must therefore establish appropriate risk management systems to determine whether the customer or beneficial owner is a PEP. Regulation 12 of the FIAML Regulations prescribe that when dealing with domestic or international organization PEPs, the following EDD measures must be applied in addition to the normal CDD measures applicable under the Regulations:

(a) reasonable measures must be taken to determine whether a customer or the beneficial owner is a PEP; and

(b) in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP, adopt the measures listed below:

- obtain senior management approval before establishing or continuing, for existing customers, such business relationships;
- take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- conduct enhanced ongoing monitoring on that relationship

Additionally, Accountants shall apply all the above measures to family members or close associates of all types of PEP.

It is a requirement that Senior Management approves the dealing with a PEP. Senior management may be-

i. the head of a practice group;
ii. another partner who is not involved with the particular file;
iii. the partner supervising the particular file;
iv. the nominated officer or, if different, the officer responsible for compliance under the FIAML Regulations; and
v. the managing partner.

In any case, it is required that you advise those responsible for monitoring risk assessment that a business relationship with a PEP has begun, to help their overall monitoring of the practice's risk profile and compliance.

Relevant factors that will influence the extent and nature of CDD include the particular circumstances of a PEP, the PEP's role in a particular government/ government agency, whether the PEP has access to official funds, the PEP’s home country, the type of work the PEP is instructing the accountant to perform or carry out (i.e. the services that are being asked for), whether the PEP is domestically based or international, particularly having regard to the services asked for, and the scrutiny to which the PEP is under in the PEP’s home country.

The nature of the risk should be considered in light of all relevant circumstances, such as:

a) The nature of the relationship between the client and the PEP. If the client is a trust, company or legal entity, even if the PEP is not a natural person exercising effective control

or the PEP is merely a discretionary beneficiary who has not received any distributions, the PEP may nonetheless affect the risk assessment.

b) The nature of the client (e.g. where it is a public listed company or regulated entity which is subject to and regulated for a full range of AML/CFT requirements consistent with FATF recommendations, the fact that it is subject to reporting obligations will be a relevant factor, albeit this should not automatically qualify the client for simplified CDD).

Life Insurance Policies

At the time of payout in relation to life insurance policies, a reporting person should take reasonable measures to determine whether the beneficiaries or the beneficial owner of the beneficiary are PEPS. Where higher risks are identified, the reporting person shall-

i. inform senior management before the payout of the policy proceeds;
ii. conduct enhanced scrutiny on the whole business relationship with the policy holder; and
iii. consider making a suspicious transaction report.

4.9. Ongoing CDD & Monitoring

Pursuant to regulation 9 of the FIAML Regulations, a reporting person shall verify the identity of the customer and beneficial owner-

i. before or during the course of establishing a business relationship or conducting transactions for occasional customers; and
ii. where doubts exist about the veracity or adequacy of previously obtained customer identification information, the reporting person shall identify and verify the identity of the customer and beneficial owner before the customer may conduct any further business.

By virtue of regulation 9(3) of the FIAML Regulations, a reporting person may be allowed by the relevant supervisory authority or regulatory body to complete the verification of the identity of the customer and beneficial owner after the establishment of the business relationship, provided that-

i. this is essential not to interrupt the normal conduct of business;
ii. the verification of identity occurs as soon as reasonably practicable;
iii. the money laundering and terrorism financing risks are effectively managed by the reporting person; and

iv. the reporting person shall adopt and implement risk management procedures concerning the conditions under which a customer may utilise prior to verification.

4.10.1. CDD on existing customers

According to section 17E of the FIAMLA, a reporting person shall apply CDD requirements to customers and beneficial owners-

- with which a business relationship has already commenced by having regard to the following factors-
  i. the basis of materiality and risk depending on the type and nature of the customer;
  ii. the business relationship;
  iii. products or transactions;
  iv. previous CDD measures; and
  v. adequacy of information obtained.

And as per Regulation 10 of the FIAML Regulations, a reporting person shall apply CDD measures to existing customers when-

i. there is indication that the identity of the customer or the beneficial owner has changed;
ii. any transactions which are not reasonably consistent with his knowledge of the customer;
iii. any change in the purpose or intended nature of his relationship with the customer; and
iv. any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

Accountants are not expected to scrutinise every transaction that goes through their clients' books and some accounting services are provided only on a one-off basis, without a continuing relationship with the client and without the accountant having access to client's books and/or bank records. However, many of the professional services provided by accountants put them in a relatively good position to encounter and recognise suspicious activities (or transactions) carried out by their clients through their inside knowledge of, and access, to the client's records and management processes and operations, as well as through close working relationships with senior managers and owners. The continued administration and management of the legal persons and arrangements (e.g. account reporting, asset disbursements and corporate filings) would also enable the relevant accountants to develop a better understanding of the activities of their clients.

Accountants need to be alert for events or situations which are indicative of a reason to be suspicious of ML/TF, employing their professional experience and judgement in the forming of suspicions where appropriate. An advantage in carrying out this function is the professional scepticism which is a defining characteristic of many professional accountancy functions and relationships.

4.10.2 On-going Monitoring

Ongoing monitoring of the business relationship should be carried out on a risk related basis, to ensure that accountants are aware of any changes in the client's identity and risk profile established at client acceptance. This requires an appropriate level of scrutiny of activity during the relationship, including enquiry into source of funds where necessary, to judge consistency with expected behaviour based on accumulated CDD information.

Accountants should also consider reassessing CDD on an engagement/assignment basis for each client. Well-known, reputable, long-standing clients may suddenly request a new type of service that is not in line with the previous relationship between the client and accountant. Such an assignment may suggest a greater level of risk.

4.10. Suspicious Transaction Reporting & Monitoring

Section 14 of the FIAMLA imposes a legal obligation on Accountants/Accountancy Firms to-

i. as soon as practicable; and
ii. but no later than 15 working days from the day the reporting person became aware of the suspicious transaction;

-to make a report of such transaction to the FIU.

The FIU is also obligated by law to provide feedback to the reporting person and relevant supervisory authorities following an STR under section 14(1A) of the FIAMLA.

Lodging of reports of suspicious transaction

The procedure to lodge a report of suspicious transactions is laid down under section 15 of the FIAMLA. It stipulates that-

i. every report shall be lodged with the FIU;
ii. the report shall be in such a form as approved by the FIU;

iii. the report shall include-

- the identification of the party or parties to the transaction
  - the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion
  - the business relationship of the suspect to the bank, financial institution, cash dealer or member of a relevant profession or occupation
  - where the suspect is an insider, whether the suspect is still affiliated with the bank financial institution, cash dealer, or member of a relevant profession or occupation
  - any voluntary statement as to the origin, source or destination of the proceeds
  - the impact of the suspicious activity on the financial soundness of the reporting institution or person
  - the names of all the officers, employees or agents dealing with the transaction

iv. no report of a suspicious transaction shall be required to be disclosed or be admissible as evidence in any court proceedings.

As explained, the CDD process allows the Accountant to build a profile of the customer both in terms of risk and also in terms of activities. This further enables Accountants to detect any suspicious or unusual activities such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business. In fact, Accountants are required to scrutinize transactions undertaken throughout the course of a business relationship, including where necessary the source of funds to ensure that the transactions are consistent with his knowledge of the customer.

MIPA may provide information to accountants, which can inform their approach for identifying suspicious activity or transactions, as part of a RBA. Accountant should also periodically assess the adequacy of their system for identifying and reporting suspicious activity or transactions. As such, Accountants should review CDD if they have a suspicion of ML/TF.

Information on the manner in which a STR shall be reported and on how to identify and report a suspicious transaction is contained in the FIU's Guidance Note No. 3 which is also available on the FIU's website.

A list of ML/TF sector specific indicators for accountants can be found at Annex 3.

4.11.1. Request for Info from FIU

Under Section 13(2) (a) and 13(2)(b) of FIAMLA, the Director of the FIU may request additional information from Accountants who submitted the suspicious transaction report or from any other reporting person which is, or appears to be, involved in the transaction. Also, pursuant to Section 13(3) of the FIAMLA, the Director of the FIU can request information Accountants, whenever the FIU becomes aware of information that may give rise to reasonable suspicion of ML/TF offences, or it has received a request form investigatory /supervisory /overseas FIU/government agencies. The information sought for under the above sections shall, as soon as practicable but not later than 15 days, be furnished to the FIU. Also, in line with section 13(6) of the FIAMLA, the FIU may order Accountants to inform it if a person has been their client, or has acted on behalf of their client; or whether a client of the Accountant has acted for a person. If the Accountant fails to supply any information requested by the FIU under section 13(2), 13(3) or 13(6) of FIAMLA, they commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years as provided for in section 19 and 32A of the FIAMLA.

4.11.2. Protection of Information

Confidentiality is a key success factor for the operations of an FIU. In this context, the FIU has put in place a proper Program Level Security and a System Level Security policies and procedures. Under the Program Level Security (based on protection afforded under the law), and in line with section 30(1) of the FIAMLA, the Director, every officer of the FIU, the Chairperson and members of the Board shall take an oath of confidentiality before they begin to perform their duties. They should maintain during and after their relationship with the FIU, the confidentiality of any matter relating to the relevant enactments. Section 30(2) of the FIAMLA further provides that no information from which an individual or body can be identified and which is acquired by the FIU in the course of carrying out its functions shall be disclosed except where disclosure appears to the FIU to be necessary to enable it to carry out its functions, or in the interests of the prevention or detection of crime, or in connection with the discharge of any international obligation to which Mauritius is subject. More so, in view of preserving the confidentiality of information disseminated, at the time of disclosure of intelligence to recipients, the FIU imposes terms and conditions on the usage of such intelligence in line with section 30(2A) of FIAMLA. Any breach

of this section shall be punishable by a fine not exceeding Rs1 million and to imprisonment for a term not exceeding 3 years. Additionally, under the Program Level Security, the FIU has adopted clear policies on recruitment and termination of employment of staff.

On the System Level Security side, the FIU has adopted proper policies to safeguard its environmental and physical security by implementing policy documentation, encryption of electronic communication, restricting access and use of CCTV cameras, alarm systems among others. Furthermore, for ongoing monitoring and "break the glass" purposes, the FIU Mauritius has mandatory security policy, document tracking system, back ups and disaster recovery.

4.11.3 Tipping Off

After making a suspicious transaction report to the FIU, Section 16 (1) of FIAMLA prevents Accountants from informing anyone, including the customer, about the contents of a suspicious transaction report or even discloses to him that he/she has made such a report or information has been supplied to the FIU pursuant to the request made under section 13(2), 13(3) or 13 (6) of FIAMLA. It shall amount to an offence under the Act punishable by a fine not exceeding five million rupees and to imprisonment for a term not exceeding 10 year. Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and on-going monitoring, and should not give rise to tipping off. If the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead the Accountant should immediately file an STR with the FIU.

CHAPTER 5: CASH PROHIBITION OBLIGATIONS

Moreover, Accountants/Accountancy Firms shall not make or accept any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency pursuant to section 5 of FIAMLA. Under FIAMLA, "cash" means money in notes or coins of Mauritius or in any other currency; and it includes any cheque which is neither crossed nor made payable to order whether in Mauritian currency or in any other currency. As far as transaction is concerned, it includes opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise.

CHAPTER 6: TERRORIST FINANCING OFFENCES

6.1 Introduction

Terrorist organisations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The UN Sanctions Act criminalises the provision of monetary support for terrorist purposes by implementing the United Nations Security Council Resolutions on targeted sanctions including financial sanctions, arms embargo and travel ban.

6.2 Extension of Obligations

According to section 19H & K of the FIAMLA, a member falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act as well. The prohibition to deal with funds or other assets of a designated party[13]or listed party[14] applies to all persons (including reporting persons which also encapsulate accounting firms & accounting professionals) as per section 23 of the UN Sanctions Act.

In addition, section 24 of the UN Sanctions Act prohibits any person on making funds or other assets available to a designated party or listed party.

Reporting Obligations

Where any person holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party, he/she shall immediately notify (section 23(4) UN Sanctions Act) the National Sanctions Secretariat of-

i. details of the funds or other assets against which action was taken against;
ii. the name and address of the designated party or listed party; and
iii. details of any attempted transaction involving the funds or other assets, including-

- the name and address of the sender
- the name and address of the intended recipient
- the purpose of the attempted transaction
- the origin of the funds and other assets
- where the funds or other assets were intended to be sent

[13] A designated party means any party designated by the National Sanctions Committee under section 9 of the UN Sanctions Act.
[14] A listed party means any party listed by or under the authority of the United Nations Security Council.

The reporting obligations continue under section 25 of the UN Sanctions Act which says that a reporting person shall immediately verify whether the details of the designated or listed party match with the particulars of any customer and if so, identify whether the customer owns any funds or other assets in Mauritius. A report has to be submitted to the National Sanctions Secretariat regardless of whether any funds or other assets were identified by the reporting person.

Reporting of suspicious information

Pursuant to section 39 of the UN Sanctions Act, any information related to a designated party or listed party which is known to the reporting person should be submitted to the FIU in accordance with section 14 of the FIAMLA.

CHAPTER 7: ADDRESSING NON-COMPLIANCE

According to section 19H of the FIAMLA, a regulatory body shall have such powers as are necessary to enable it to effectively discharge its functions and may, in particular –

a) issue guidelines for the purposes of combating money laundering activities and the financing of terrorism and proliferation activities;

b) give directions to a member falling under its purview to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts;

c) require a member falling under its purview to submit a report on corrective measures it is taking to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts, at such intervals as may be required by the regulatory body.

d) With respect to a member falling under its purview, the regulatory body may apply any or all of the following administrative sanctions –

i. issue a private warning;

ii. issue a public censure;

iii. impose such administrative penalty as may be prescribed by the regulatory body;

iv. ban, where the regulatory body has licensed or authorised the member to conduct his business or profession, from conducting his profession or business for a period not exceeding 5 years; and

v. revoke or cancel a licence, an approval or an authorisation, as the case may be.

7.1. Directions by Regulatory Body

By virtue of section 19L of the FIAMLA, a regulatory body may give written directions to its member where he has reasonable cause to believe that a member who falls under its purview has failed or is failing to comply with the requirements under the FIAMLA and the UN Sanctions Act or is engaging in money laundering and the financing of terrorism and proliferation activities.

The regulatory body may take any of these actions-

i. remove or take steps to remove any specified employee from office;

ii. ask the member falling under its purview to refrain from doing a specified act;

iii. ensure that a specified employee does not take part in his management or conduct except as permitted by the regulatory body;

iv. appoint a specified person to a specified office for a period specified in the direction;

v. implement corrective measures and reports on the implementation of the corrective measures; and

vi. revoke a direction and notify accordingly its member.

Non-compliance with the direction of a regulatory body is punishable by Rs 5000 per day under section 19M of the FIAMLA. In addition, a person who knowingly hinders or prevents compliance with a direction may be liable to a fine not exceeding one million rupees and a term of imprisonment not exceeding 5 years.

7.2. Administrative sanctions

Where a regulatory body has reasonable cause to believe that a member falling under its purview has contravened the FIAMLA and/or the UN Sanctions Act, it is empowered to impose administrative sanctions under section 19N of the FIAMLA. Details of the Administrative Sanctions can be found at section 19H(1)(d) FIAMLA.

7.3. Review Panel

Section 19Q of the FIAMLA caters for the establishment of a Review Panel which will be responsible to review a decision of a regulatory body to impose an administrative sanction under section 19N of the same Act. Under section 19S of the FIAMLA, a member who is aggrieved by the decision of the regulatory body, may within 21 days of the decision of the regulatory body, make an application to the Review Panel for a review of that decision. Finally, the avenue for a judicial review of the determination of the Review Panel to the Supreme Court is made possible under section 19X of the FIAMLA.

GLOSSARY OF TERMINOLOGY

Beneficial Owner

Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Competent Authorities

Competent authorities refers to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements. SRBs are not to be regarded as competent authorities.

Designated Non-Financial Businesses and Professions (DNFBPs)

Designated non-financial businesses and professions means:

a) Casinos (which also includes internet and ship-based casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:

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

Express Trust

Express trust refers to a trust clearly created by the settlor, usually in the form of a document e.g. a written deed of trust. They are to be contrasted with trusts which come into being through the operation of the law and which do not result from the clear intent or decision of a settlor to create a trust or similar legal arrangements (e.g. constructive trust).'

FATF Recommendations

Refers to the FATF Forty Recommendations.

Legal Person

Legal person refers to any entities other than natural persons that can establish a permanent client relationship with an accountant or otherwise own property. This can include bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

Legal Professional

In this Guidance, the term *"Legal professional"* refers to legal professionals, civil law notaries, common law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs)

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. *Domestic PEPs* are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Red Flags

Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A *"red flag"* may be used as a shorthand for any indicator of risk which puts an investigating accountant on notice that further checks or other appropriate safeguarding actions will be required.

ANNEX 1. RISK ASSESSMENT FORM FOR ACCOUNTANTS/ ACCOUNTING FIRMS

Name of Accountant or Accounting firm:_____

The *Financial Intelligence Anti-Money Laundering Act* requires Professional Accountants, Public Accountants and Member Firms who carry activities under First Schedule Part II (e) of the FIAMLA to conduct a risk assessment of your exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist you in meeting these obligations. This form is presented as an example only. You may choose to conduct your risk assessment using a different approach.

Instructions: When you answer yes to one of the questions, this situation or client is considered higher risk and a control measures to reduce the risk should be applied. For each higher risk client or situation, a suggested control measure is proposed. You can adapt the control measures to correspond to your business (see Annex A for a list of control measures).

The results of this risk assessment should be communicated to all Professional and Public Accountants and employees in your business/firm that deal with clients. The training should include a review of what is considered higher risk and the corresponding control measures. The date of the training should be documented. You should review your risk assessment every two years.

Risk Assessment

Higher risk clients and situations	**Yes** Higher risk	**No** Moderate risk	**Suggested Control Measures**
Clients			
Are your clients foreigner?			• Determine if individuals are politically exposed persons.[15] • Obtain additional information on source of funds or source of wealth.
Do you have clients who are politically exposed persons?			• Obtain senior management approval to conduct the transaction. • Obtain additional information on source of funds or source of wealth. • Conduct enhanced on-going monitoring any future accountancy transactions.
Is your client a company, trust, foundation, partnership or other structure that makes it difficult to determine who is the beneficial owner (the natural person who			• Obtain name of natural person(s) behind company, trust or other legal arrangements.

[15] Pursuant to FIAMLA, you are required to ascertain whether all clients and beneficial owners are politically exposed persons. The mitigation measure is suggested here for emphasis.

owns or controls the funds or property)?			• Obtain additional information on organizational structure. • Obtain additional information on source of funds or source of wealth.
Are your clients intermediaries (i.e. lawyers and accountants acting on behalf of clients)?			• Obtain name of person(s) on whose behalf the transaction is being conducted. • Verify that the intermediary has the necessary documentation to act on behalf of the client. • Obtain additional information on source of funds or source of wealth.
Has one of your clients been named in the media as being involved with criminal organizations or having committed a crime?			• File Suspicious Transaction Report (STR). • Obtain additional information on source of funds or source of wealth.
Do you have a client that is purchasing a property that is not within his or her means based on his stated occupation or income?			• Obtain additional information on source of funds or source of wealth.
Do your clients that engage in activities that are consistent with the indicators identified for Suspicious Transactions? (See			• Consider filing a Suspicious Transaction Report (STR).

Guidance Note on AML/CFT Guidance on Suspicious Transaction Reports for suspicious transactions indicators and the indicators listed in Chapter 5 of this guideline).			• Obtain additional information on source of funds or source of wealth.
Products, services and transactions			
Do you undertake high value transactions? (over 50 millions rupees)?			• Pay special attention for unusual transaction and ML/TF indicators. • Obtain additional information on source of funds or source of wealth.
Are you involved in the creation of complex legal structures where the persons owning or controlling the entity cannot be immediately identified?			• Obtain name of person(s) behind corporation, trust or legal arrangement. • Obtain additional information on organizational structure. • Obtain additional information on source of funds or source of wealth.
Are you involved in the buying and selling of real estate?			• Confirm source of funds

			• Pay special attention for unusual transaction and ML/TF indicators.
Are you involved in the management of client money, securities or other assets?			• Confirm source of funds • Pay special attention for unusual transaction and ML/TF indicators.
Are you involved in the management of bank, savings or securities accounts?			• Confirm source of funds • Pay special attention for unusual transaction and ML/TF indicators
Are you involved in the organisation of contributions for the creation operation or management of companies?			• Obtain name of person(s) behind corporation, trust or legal arrangement. • Obtain additional information on source of funds or source of wealth. • Pay special attention for unusual transaction and ML/TF indicators.
Are you involved in the creating, operating or management of legal persons or arrangements, and buying and selling of business entities?			• Obtain name of person(s) behind corporation, trust or legal arrangement. • Pay special attention for unusual transaction and ML/TF indicators.

Geographic Risk			
Are any of your clients or the source funds originate from countries subject to sanctions, embargoes or similar measures issued by Mauritius or International Organizations such as the United Nations ("UN"). Mauritius https://www.mipa.mu/assets/upload/attachment/United_Nations_Security_Council_Consolidated_List_06.01.2020.pdf United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list			• Obtain senior management approval to proceed with the transaction. • Ask for additional information, piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
Do any of your clients or the source funds originate from foreign jurisdictions known for high levels of financial secrecy or jurisdictions with low tax rates? http://www.imolin.org/imolin/finhaeng.html#Map.%20%20Major%20Financial%20Havens			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.

https://www.financialsecrecyindex.com/en/			
• Do any of your clients or the source funds originate from foreign jurisdictions identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement? FATF: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
• Do any of your clients or the source funds originate from jurisdictions identified by credible sources (for example international organisations such as the UN, credible news reports) as providing funding or support for terrorist activities			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.

• Do any of your clients or the source funds originate from countries identified by credible sources as having significant levels of corruption, or other criminal activity? http://www.transparency.org/news/feature/corruption_perceptions_index_2016			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
Delivery channel and business practices			
Do you accept cash?			• Confirm source of funds • Set limits to cash transaction amounts recognizing the 500,000 rupee cash prohibition outlined in the FIAMLA. • Request bank drafts instead of accepting large amounts of cash.
Do you conduct transactions where you do not meet the client?			• Deliver comprehensive AML/CFT training to your employees specifically focused on client due diligence requirements

			• Ask for an additional piece of identification to confirm the identity. • Confirm the beneficial owner (the natural person who owns or controls the funds or property) • Confirm that any intermediary has the necessary documentation to act on behalf of the client. • Conduct periodic review of records to ensure that client due diligence requirements are adequately implemented
Do you have clients that are referred to you by a third party (such as a lawyer or real estate agent or other accountant)?			• Conduct client due diligence measures directly. • Conduct periodic review of records to ensure that client due diligence requirements are respected by third party if you rely on them for due diligence measures.
Other risk factors: (list any additional factors)			

_____ _____

Signature of Accountant ***Date***

Date of employee training: _____

Annex 1.A - Examples of Risk Control Measures

1. Obtain senior management or compliance officer approval to proceed with the transaction.
2. Obtaining additional information on the client (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of client and beneficial owner
3. Obtain name of natural person(s) behind company, trust or other legal arrangement.
4. Deliver more frequent employee training.
5. Monitor AML/CFT legislative and regulatory changes.
6. Include AML/CFT obligations in job descriptions and performance reviews.
7. Set limits to cash transaction amounts (less than the 500,000 rupees prohibition).
8. Request bank drafts instead of accepting large amounts of cash.
9. Conduct transaction only in person.
10. Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the client risk profile (provided that the internal policies of accountants should enable them to disregard source documents, data or information, which is perceived to be unreliable)
11. Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship
12. Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained
13. Obtaining information on the reasons for intended or performed transactions
14. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
15. Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards
16. Increasing awareness of higher risk clients and transactions, across all departments with a business relationship with the client, including the possibility of enhanced briefing of

engagement teams responsible for the client.

17. Enhanced CDD may also include lowering the threshold of ownership, to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Annex 2: Template for AML/CFT Policies and Procedures

Address | City Postal Code| Telephone

Email

Risk Assessment and Risk mitigation (Section 17 of the Financial intelligence Anti-Money Laundering Act (FIAMLA))

Describe how you will comply with your risk assessment and risk mitigation obligations including:

- Identifying what clients and situations you have identified as higher risk (copy of the risk assessment should be attached)
- What mitigation and control measures you will be implementing to reduce the risk
- How you will document the risk of any new product or services
- How often you will update the risk assessment

See How to conduct a risk assessment in the accounting sector for additional guidance (Please refer to Annex 1).

Customer due diligence (CDD): (section 17C of the FIAMLA)

Describe how you will comply with CDD requirements including:

- When will you identify the buyer and seller of a transaction?
- What information will you collect when you identify a natural person?
- What information will you collect when you identify a legal persons and legal arrangements?
- What identification documents are acceptable?
- Only original documents will be acceptable
- How will you identify clients that are not physically present?

- What will you do if you cannot complete customer due diligence measures?

Record Keeping (Section 17F of FIAMLA)

Describe how you will comply with record keeping requirements including:

- How long will you retain records related to transactions?
- What records will you retain?
- Where will records be retained?
- How will you ensure that information can be provided in a timely manner to the Financial Intelligence Unit, the police and other competent authorities?
- If you are using a third party to conduct customer due diligence measures:
    - How you will ensure that they are properly identifying clients?
    - How you will gain access to information in a timely fashion?

Enhanced due diligence (Regulation 12 of the Financial Intelligence Anti-Money Laundering Regulations (FIAMLR))

Describe how you will comply with enhanced due diligence requirements including:

- How you will apply enhanced due diligence measures to:
    - Persons or transactions involving a country identified as higher risk by FATF
    - Persons or transactions involving higher risk countries for ML, TF, corruption or subject to international ML/TF
    - Any other situation representing a higher risk of ML/TF based on your risk assessment
- What enhanced due diligence measures will be applied in those circumstances?

Politically Exposed Persons (Regulation 15 of the FIAMLR)

Describe how you will comply with enhanced due diligence requirements related to politically exposed persons including:

- What is a politically exposed person?
- How you will identify politically exposed persons?
- How you will seek approval from senior management?
- How you will take adequate measures to establish source of wealth and source of funds?
- How you will conduct enhanced ongoing monitoring?

Ongoing monitoring (Section 3 (e) of the FIAMLR)

Describe how you will comply with ongoing monitoring requirements including:

- How you will conduct ongoing monitoring for:
  - Business relationships (typically after 2 transactions)
  - Complex and unusual transactions
  - Unusual patterns of transactions which have no economic or lawful purpose?
- How you will record the findings?

Suspicious transaction reporting (Section 15 of the FIAMLA)

Describe how you will comply with suspicious transaction reporting requirements including:

- What is a suspicious transaction?
- How you and your employees/agents will identify suspicious transactions (should refer to ML/TF indicators)
- Who is your Money Laundering Reporting Officer?
- How employees/agents should raise suspicions to the reporting officer?
- Specify that you cannot communicate that an STR has been filed with the FIU

Training (Regulation 22 (1) (c) of the FIAMLR)

Describe how you will comply with training requirements including:

- How you will screen employees to ensure high standards before hiring
- How you will train employees/agents on:
    - How to identify a suspicious transaction?
    - What are the AML/CTF obligations?
    - How to implement your policies and procedures?

Terrorist Financing Obligations (Regulation 22 (1) (c) of the FIAMLR)

- Describe how you will comply with training requirements including:
    - How you will screen against UN Sanctions List?
    - How you will report to the National Sanctions Secretariat?
    - How you will report to the FIU?

Policies and procedures (Section 22 (1) (c) of the FIAMLR)

Describe the following regarding your policies and procedures:

- How you will communicate the policies and procedures to employees and staff as well as branches and subsidiaries
- How you will reflect changes to AML/CTF legislative and regulatory requirements
- How often you will update your policies and procedures

ANNEX 3 – ML/TF INDICATORS – ACCOUNTING SECTOR

Accountants are in a position to discover money laundering and terrorist financing because of their expertise and involvement in the execution and facilitation of a wide variety of financial transactions such as the creation of companies formation or the management of their financial matters, involvement in tax matters, wire transfers, etc. In many of these transactions, the value and the complexity of the transactions are high.

- Client appears to be living beyond his or her means.
- Client has cheques inconsistent with sales (i.e., unusual payments from unlikely sources).
- Client has a history of changing bookkeepers or accountants yearly.
- Client is uncertain about location of company records.
- Client performs activities that are irrelevant to his or her normal activities or profession and cannot provide a reasonable explanation.
- Accountant does not meet client face-to-face.
- Client provides instructions or funds outside of their personal or business sector profile.
- Client starts or develops an enterprise with unexpected profile or early profits.
- Client does not wish to obtain necessary governmental approvals/filings, etc.
- Client offers to pay extraordinary fees for services which would not ordinarily warrant such a premium.
- Company carries non-existent or satisfied debt that is continually shown as current on financial statements.
- Company has no employees, which is unusual for the type of business.
- Company is paying unusual consultant fees to offshore companies.
- Company records reflect sales at less than cost, thus putting the company into a loss position, but the company continues without reasonable explanation of the continued loss.
- Company shareholder loans are not consistent with business activity.
- Examination of source company documents shows misstatements of business activity that cannot be readily traced through the company books.
- Company makes large payments to subsidiaries not within the normal course of business.

- Company invoiced by organizations located in a country with weak AML/CFT regime or a tax haven.
- Company acquires large personal and consumer assets (i.e., boats, luxury automobiles, personal residences and cottages) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice of that particular industry.
- Company uses many different firms of auditors and advisers for connected companies and businesses.
- Legal structure of client has been altered numerous times (name changes, transfer of ownership, change of corporate seat).
- Management of the corporate client appears to be acting according to instructions of unknown or inappropriate person(s).
- Frequent or unexplained changes in the corporate client's professional adviser(s) or members of management.
- The number of employees or organizational structure is out of keeping with the size or nature of the business (for instance the turnover of a company is unreasonably high considering the number of employees and assets used).
- Company receives large international payments when there is no business rationale.