ATTORNEY GENERAL'S OFFICE

MAURITIUS

GUIDELINES ON THE MEASURES FOR THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM FOR LAW FIRMS/ FOREIGN LAW FIRMS/ JOINT LAW VENTURE/FOREIGN

LAWYERS AND INDIVIDUAL LAW PRACTITIONERS

(BARRISTERS/ATTORNEYS AND NOTARIES)

Amended August 2022

DISCLAIMER

These Guidelines are intended to provide assistance to legal professionals in meeting their obligations under the Financial Intelligence and Anti Money Laundering Act (FIAMLA), United Nations (Financial Prohibitions, Travel Ban and Arms Embargo) Sanctions Act 2019 (UN Sanctions Act) and the Financial Intelligence and Anti Money Laundering Regulations 2018 (FIAML Regulations).

These Guidelines have been issued by the AGO and the FIU pursuant to Section 19H (1) (a) of the Financial Intelligence and Anti-Money Laundering Act 2002. This Guide has been prepared and published for informational and educational purposes only and should not be construed as legal advice. The laws and regulations discussed in this Guide are complex and subject to frequent change. If you are unsure about your obligations in a given case, you should consider taking independent legal advice.

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.

Terminology used in the Guidelines

Legal Professional:	Refers to law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.
You:	Refers to a legal 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.

ACRONYMS

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
CDD	Customer Due Diligence
CO	Compliance Officer
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence Anti-Money Laundering Act
FIU	Financial Intelligence Unit
ML	Money Laundering
NRA	National Risk Assessment
PEP	Politically Exposed Person
PF	Proliferation Financing
STR	Suspicious Transaction Report
TF	Terrorism Financing
VA	Virtual Asset

Table of Contents

1. Introduction

Money laundering, terrorism and proliferation financing have far reaching consequences for a country's financial system and economy. With these crimes becoming increasingly cross border in nature, jurisdictions must equip themselves to protect the integrity of their financial systems and must also be prepared to deal with any abuses which are encountered. In order to achieve this, there are several building blocks that are required. The first is a sound and robust legal framework, which empowers institutions and lays down the obligations of all parties concerned. The second is an open and collaborative approach between AML/CFT supervisors and the reporting persons that they regulate. Additionally, there must be willingness on behalf of the sectors that are regulated to understand their obligations and to accept that they also have to contribute to the fight against ML and TF. Against this background, the FIU and the AGO, as AML/CFT regulators for this sector, firmly believe that one crucial way through which ML and TF can be curbed, is through the implementation of strong controls policies and procedures by legal professionals. These act as a line of defence in ensuring that the legal sector does not become a haven for criminals. The purpose of these guidelines is to assist the sector in establishing strong systems, understand their obligations under the law and becoming partners in the fight against ML and TF.

1.1 The Mauritian AML/CFT Legislative Framework

Mauritius has taken significant steps to ensure that it has a robust AML/CFT legal framework, which is aligned with international standards. The FIAMLA was enacted in 2002 and provided for several of the key requirements of a strong AML/CFT system. It has been amended to ensure that Mauritius meets its international obligations. Amongst others, the FIAMLA makes provision for an independent FIU, the obligation of filing suspicious transaction reports, CDD obligations as well as a framework for the AML/CFT supervision of Designated Non-Financial Businesses and Professions (DNFBPs).

In 2018, the FIAML Regulations 2018 were made and revoked the 2003 FIAML Regulations. The 2018 Regulations make extensive provision in relation to the measures, which must be put in place by reporting persons (which includes legal professionals) to ensure that they are complying with the requirements of the law and that they are taking the required steps to safeguard their businesses and/or legal practice from ML/TF abuses.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (henceforth referred to as the 'UN Sanctions Act') was also passed in May 2019. This act enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

Copies of the above legislations are available on the AGO's website: Home (govmu.org) and the FIU's website: FIU - Home (fiumauritius.org)

1.2 Application to the Legal Profession[1]

Legal professionals are key actors in the business and financial world, facilitating vital transactions that underpin the Mauritian economy. The FATF characterizes legal professionals as "Gatekeepers"[2] because they "protect the gates to the financial system," through which potential users must pass in order to succeed. The term includes professional experts who may, by the very nature of their work, provide financial expertise to launderers, including lawyers, accountants, tax advisers, and trust and service company providers (TCSP). The FATF has noted that gatekeepers are a common element in complex money laundering schemes. Gatekeepers' skills are important in creating legal structures that could be used to launder money and for their ability to manage and perform transactions efficiently to avoid detection.

Recommendation 22 of the FATF acknowledges the role that such gatekeepers can play by recommending that such individuals have AML/CFT responsibilities when engaged in certain activities. As such, they have a significant role to play in ensuring that their services are not used to further a criminal purpose. Legal professionals are therefore called to act with integrity and uphold the law. Money laundering and terrorist financing& proliferation are serious threats to society; endangering life, causing financial losses and fueling other criminal activities.

These guidelines aim to assist legal professionals to meet their obligations under the Mauritian AML/CFT regime.

[1] As already set out at the start of this document, the term 'Legal Professionals' refers to law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.
[2] FATF Methodology (2013) p 105.

As per the findings of the National Risk Assessment (2019) Public Report, the risk profile of clients, and the level of cash activity make the sector inherently vulnerable to money laundering. Legal professionals are involved in the vast majority of transactions in Mauritius and, therefore, can play a key role in detecting money laundering and financing of terrorism and proliferation schemes involving this industry. Given that they are in direct contact with clients, they generally know their clients better than the other parties in the transactions. Therefore, they are well placed to detect suspicious transaction/activity.

This document has been issued pursuant to section 19H (1) (a) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002. They are intended to assist legal professionals in complying with their obligations in relation to the prevention, detection and reporting of money laundering, financing of terrorism and proliferation. Through compliance with their obligations, legal professionals can ensure that their businesses and/or legal practices are not misused by money launderers or those financing terrorism or proliferation.

1.3 Businesses, Legal Practices and Individuals covered by the Guidelines

This guideline is addressed to the following:

- law firms/foreign law firms/joint law venture/foreign lawyers and
- individual law practitioners namely barristers/attorneys and notaries who are involved in the following activities, listed in Part 2 of the First Schedule of FIAMLA (as listed below):

A barrister, an attorney, a notary, a law firm, a foreign law firm, a joint law venture, a foreign lawyer under the Law Practitioners Act, […], who prepares for,[3] 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;

[3] Preparing or carrying out transactions for clients can include the drafting of legal documentation in the context of the creation of a corporation for example. It can also include but is not limited to the preparation of an act of sale of a company or real estate, making arrangements for a financial transaction to be conducted on behalf of a client, and preparing incorporation documentation.

(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;

(va) the business activities of virtual asset service providers and issuers of initial token offerings under the Virtual Asset and Initial Token Offering Services Act 2021; or

(vi) any activity specified in item (f);

f) a company service provider who prepares, or carries out, transactions for a client concerning the following activities –

(i) acting as a formation legal professional of a legal person with a view to assisting another person to incorporate, register or set up, as the case may be, a company, a foundation, a limited liability partnership or such other entity as may be prescribed;

(ii) acting, or causing another person to act, as a director, as a secretary, as a partner or in any other similar position, as the case may be, of a legal person such as a company, foundation, a limited liability partnership or such other entity as may be prescribed;

(iii) providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; or

(iv) acting, or causing another person to act, as a nominee shareholder for another person.

There will be circumstances where you give advice in relation to a listed activity (without necessarily then carrying out the activity). Generally, advice alone, in the absence of any actual listed activity, will not be captured. It is highlighted that the preparation of services/transactions would also result in the legal professional being captured.

It may be that in practice you expect to provide a mixture of advice and listed activities for a customer over a period of time. In those circumstances, you would need to conduct CDD to the required level *prior* to establishing a business relationship with the customer (and prior to providing any advice).

You also need to be aware of your obligations to report suspicious activities, which can include requests or enquiries about particular services you offer from potential new customers (regardless of whether you ultimately provide those services).

Legal professionals are not subject to AML/CFT obligations when ascertaining the legal position of their client, or in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. In principle, activities which are prescribed activities under part 2 of Schedule 1 of the FIAMLA which are related to the preparation or carrying out of financial transactions and the creation, operation and management of legal persons and arrangements are not subject to legal professional privilege.

The guidance would like to emphasize that if you are unsure about your obligations when it comes to your duty of confidentiality and claiming legal professional privilege over communications in a given situation, you should consider seeking independent legal advice and/or contact your relevant professional bodies.
The FIU has in August 2021 issued a focused Guidance on the prescribed activities for Individual Law Practitioners.

1.4 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) was established in 1989 by the G7countries. It is an inter-governmental body whose purpose is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, financing of terrorism and other related threats to the integrity of the international financial system.

As a member of the Eastern and Southern Africa Anti-Money Laundering Group, Mauritius has made the commitment to implement these standards into its domestic AML/CFT framework.

1.5 The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

The ESAAMLG was founded in 1999 and its main objective is to ensure that its Members comply with the FATF standards. Assessment for compliance with the FATF Recommendations is done through the Mutual Evaluation Process following which a Mutual Evaluation Report (MER) is prepared and posted on the ESAAMLG's website. The most recent MER of Mauritius can be accessed on the FIU Website[4].

1.6 Compliance with Guidelines and Enforcement

As the AML/CFT regulator for legal professionals, the FIU and AGO are mandated to ensure compliance by the professionals that they supervise with the FIAMLA, the UN Sanctions Act, and any regulations and guidelines issued under these Acts. Following legal amendments made in May 2019, the FIU and AGO have been further empowered, and provided with significant powers to enforce compliance by the sector.

1.7 Scope of the Powers of a 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;

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

[4] ESAAMLG Mutual Evaluation – Financial Intelligence Unit (FIU) (fiumauritius.org)

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.

In relation to legal professionals, the FIU is able to use all the powers provided in the FIAMLA, including the power to impose administrative sanctions. In addition to the administrative sanctions, the FIU may also refer any cases of non-compliance to the Attorney General for any other action that the latter may deem appropriate.

Any person who fails to comply with a direction issued shall 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.

It is noteworthy to highlight that a regulatory body may publish any of its decision or determination, or the decision of the Review Panel, or any other information the regulatory body may deem appropriate.

■ **Request for information**

As per sections 19FA and 19J of the FIAMLA, a regulatory body may require any member of a relevant business or profession and any member falling under its purview respectively 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.

■ **Onsite Inspections**

Section 19K of the FIAMLA states that a regulatory body may at any time-

i. audit and inspect the books and records of a member falling under its purview in order to 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.

■ **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, on conviction, punishable by 5000 rupees 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.

- **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. The FIU, as the AML/CFT supervisor for individual legal professionals may impose any or all of the relevant administrative sanctions in cases where non-compliance has been detected.

- **Compounding of offences**

The regulatory body may with the consent of the Director of Public Prosecutions (DPP) compound any offence committed under the FIAMLA and the UN Sanctions Act as per section 19P of the FIAMLA.

Where the DPP does not give his consent to compound the offence or the person does not agree to the compounding of the offence, the regulatory body may, with the consent of the DPP, refer the matter to the Police.

1.8 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.

2. Money Laundering and Financing of Terrorism and Proliferation

2.1 Money Laundering

Money laundering is the process intended to disguise the illegal origin of proceeds of crime in order to make them appear legitimate. If undertaken successfully, it allows criminals to maintain control over proceeds of criminal activities and, ultimately, provide a legitimate cover for these activities. The process is often carried out in three stages:

(1) Placement

This initial stage involves the introduction of criminally tainted money into the financial system. The launderer seeks to introduce illegal proceeds into the financial system by, for example breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (e.g. cheques etc.) that are then collected and deposited into accounts at another location.

(2) Layering

The layering stage is the dissociation of the dirty money from their source through a series of transactions to obscure the origins of the proceeds. These transactions may involve different entities such as companies and trusts as well as different financial assets such as shares, securities, properties or insurance products. It is the separation of benefits of drug trafficking or criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail. Illustratively, the launderer may engage in a series of conversions or movements of the funds to distance them from their source. (e.g. buying and selling of stocks, commodities or properties, buying precious metals or stones with cash, taking out and repaying a loan, use of gatekeepers and their services to buy and sell assets, etc.). The funds might even be channeled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti- money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services or use gatekeepers to carry out such transactions, thus giving them a legitimate appearance.

(3) Integration

The integration stage is the use of the funds in the legitimate economy through for instance, investment in real estate or luxury assets. Essentially, it is the provision of apparent legitimacy to benefits of drug trafficking or other illegal activities. If the layering process has been successful, the integration schemes thus place the laundered funds back into the economy so that they re- enter the financial system appearing as legitimate business funds. They can then be used for legitimate purchase of luxury goods, real estate and soon.

2.2 Financing of Terrorism

Financing of terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity for the financing of terrorism. Funds may also originate from personal donations, profits from businesses and charitable organizations but all the funds are actually used to finance terrorism. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism, it is possible to have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place. However, similar to money launderers, those financing terrorisms also move funds to conceal their source of those funds. The motive is to prevent leaving a trail of incriminating evidence.

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 programs 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.

3. Risk-Based Approach[5]

3.1 Adopting a risk-based approach

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. Based on the findings of its first national ML and TF risk assessment, which was completed in August 2019, the ML risk[6] associated with legal professionals was found to be Medium-High. The level of ML threat was rated Medium. Due to the nature of their work, barristers are frequently in contact with clients having criminal records, including persons with ML-related offences. Moreover, there have been cases where members of the legal profession have been assisting their clients in setting up complex legal structures and in providing nominee and directorship services. Alternatively, the diverse client-base profile of the sector domestic politically exposed persons, high-net worth individuals, non-resident clients, clients with foreign business and clients with criminal records or past administrative and/or supervisory actions against them, legal entities and clients obtained through introduced business) and the use of cash make the sector inherently vulnerable to money laundering.

It is an obligation for legal professionals to identify, assess and understand their ML/TF risks pursuant to section 17 of FIAMLA. It is highlighted that legal professionals should take into account the outcome of the National Risk Assessment[7] when applying CDD measures in relation to each customer.

---

[5] A risk-based approach must only be adopted by law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.

[6]For the purpose of assessing money laundering and terrorism financing risks, risk is defined as a function of threat, vulnerability and consequence.

- A threat is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities.
- Vulnerabilities comprise those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at vulnerabilities means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive forML or TF purposes.
- Consequence refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally.
-

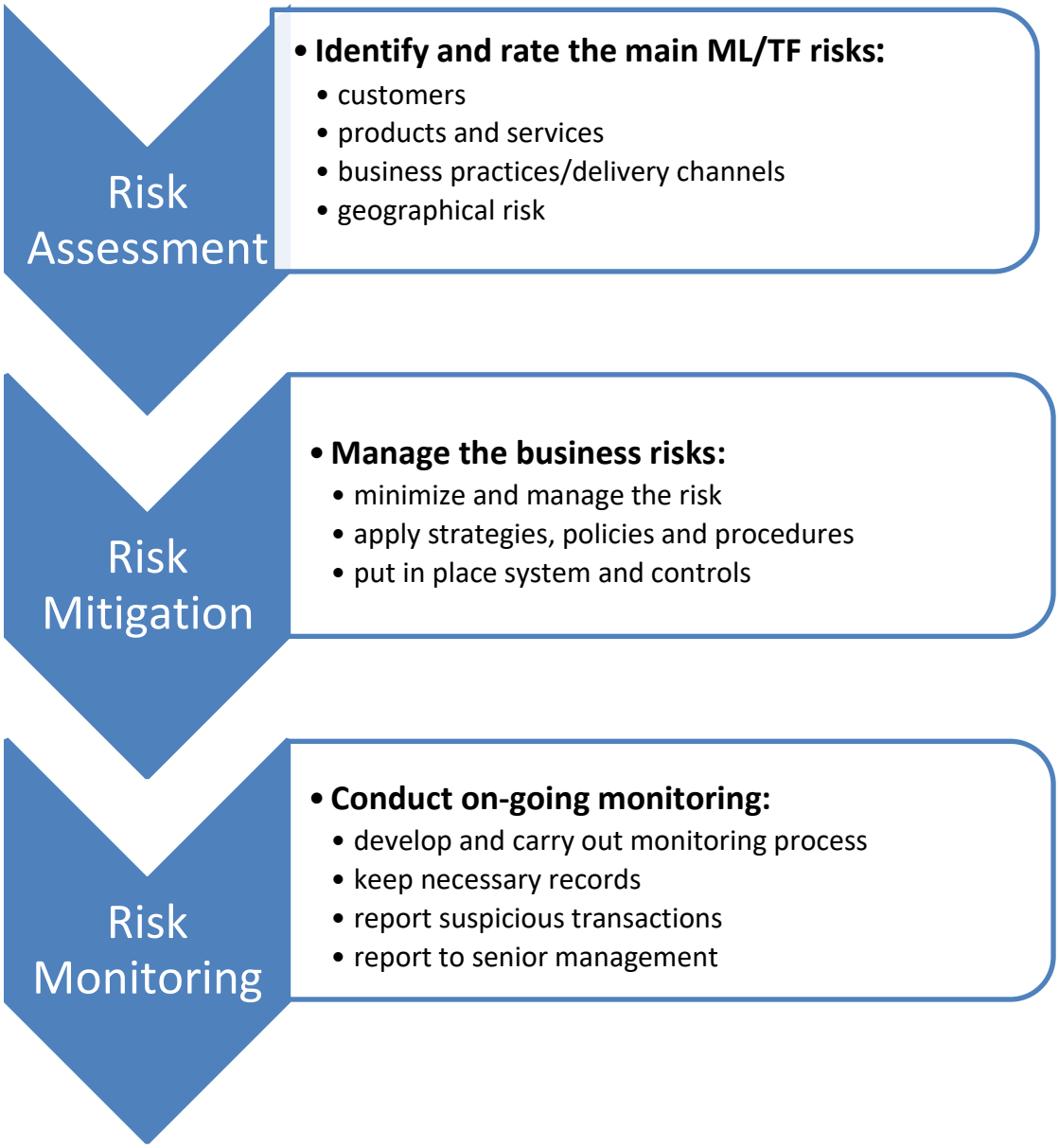
[7] The public version of the NRA report may be accessed here:
National Risk Assessment – Financial Intelligence Unit (FIU) (fiumauritius.org)

A risk-based approach also requires legal professionals to have systems and controls that are commensurate with the specific risks of money laundering and financing of terrorism facing them. Assessing this risk is, therefore, one of the most important steps in creating a robust anti-money laundering compliance program.

As money laundering risks increase, stronger controls are necessary. However, all categories of risk — whether low, medium or high — must be identified and mitigated by the application of controls, such as verification of customer identity, CDD policies, suspicious activity monitoring and checking list of people on whom sanctions have been applied or being applied. A risk-based approach should be flexible, effective and proportionate.

It is important to note that pursuant to section 3(2) of FIAMLA, legal professionals are required to take such measures that are necessary to ensure that their services are not being misused to commit a money laundering or the financing of terrorism offence. The penalty for such an offence is a fine not exceeding 10million rupees and penal servitude for a term not exceeding 20years. No legal professional can reasonably be expected to detect all wrongdoing by clients, including money laundering. However, if any legal professional develops systems and procedures to detect, monitor and report the riskier clients and transactions, he will reduce its chances of being misused by criminals.

There are three steps to establishing a risk-based approach: risk assessment, risk mitigation and risk monitoring. The following diagram depicts visually the three different steps in implementing a risk-based approach.


Risk Assessment
• Identify and rate the main ML/TF risks:
• customers
• products and services
• business practices/delivery channels
• geographical risk
Risk Mitigation
• Manage the business risks:
• minimize and manage the risk
• apply strategies, policies and procedures
• put in place system and controls
Risk Monitoring
• Conduct on-going monitoring:
• develop and carry out monitoring process
• keep necessary records
• report suspicious transactions
• report to senior management

3.1.1 Risk Assessment

Legal professionals can assess money laundering and terrorist financing risks by using various categories. The application of risk categories provides a strategy for managing potential risks by enabling legal professionals to subject each customer to reasonable and proportionate risk assessment.

3.1.1.1 Criteria to determine Risk

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

- The client base
- The services and products provided
- Geographic location
- Delivery channels and business practices

The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary from one legal professional to another, depending upon their respective circumstances. The categories however should be considered holistically and not in isolation.

In addition to the risk factors listed below a comprehensive list of ML/TF risk for legal professionals can be found in the FATF's Risk Based Guidance for Legal Professionals at: https://www.fatfgafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf

The risk categories may be broken down into different levels of risks and they also help to determine the rigidity of your policies and procedures.

(a) 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[5], persons whose assets may have

[5] These lists may be accessed on the FIU website here: https://www.fiumauritius.org/fiu/?page_id=1262

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.
The type of client may also pose ML/FT risks, e.g., individuals, listed companies, private companies, joint ventures, partnerships, etc. Each type of client is associated with a different level of risk, and it must not be assumed that the risk is the same across the legal sector, i.e., it may be low risk for one legal practitioner and considered as high risk for another.

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

- Unusual involvements of third parties;
- Making a purchase in the name of third party; for example, a friend, relative, business associate, or lawyer;
- Clients conducting their business relationship or requesting services in unusual or unconventional circumstances;
- Clients where the structure or nature of the entity or relationship makes it difficult to identify the true beneficial owner;
- Use of legal entities (corporations, LLCs or partnerships) that obscure the identity of the person who owns or controls them without a legitimate business explanation;
- Non face to face client;
- Politically exposed persons (PEPs);
- Clients that are cash intensive businesses;
- Persons whose assets have been frozen under section 45 of the Dangerous Drugs Act or whose assets have been temporarily or permanently confiscated under the Asset Recovery Act;
- Persons who appear on the UN Sanctions list or any domestic terrorist list pursuant to the UN Sanctions Act; and
- Clients with an affiliation to countries with high levels of corruption or having known associations with terrorist organizations.
- Unexplained use of virtual assets

(b) Product/Services Risk

An essential element of risk assessment is to review new and existing services that the legal practices 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 legal practice; and
- Services allowing levels of anonymity to the users.

Given the nature of services offered by legal practices, they may be exposed to transactions risks such as:

- Services where legal professionals, effectively acting as financial intermediaries, handle the receipt and transmission of funds through accounts they control in the act of facilitating a business transaction.
- Services that allow clients to deposit/transfer funds through the legal professional's trust account that are not tied to a transaction for which the legal professional is performing or carrying out activities specified in FIAMLA.
- Services where the client may request financial transactions to occur outside of the legal professional's trust account (the account held by the legal professional for the client).
- Services where legal professionals 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.
- Payments received from un-associated or unknown third parties and payments in cash where this would not be a typical method of payment.
- A proposal from any party to settle by way of virtual assets in full or in part.

- Transactions where it is readily apparent to the legal professional that there is inadequate consideration, especially where the client does not provide legitimate reasons for the amount of the consideration.

- The use of shell companies, companies with ownership through nominee shares or bearer shares and control through nominee and corporate directors without apparent legal, tax, business, economic or other legitimate reason.

- Situations where advice on the setting up of legal arrangements may be misused to obscure ownership or real economic purpose (including changes of name/corporate seat or on establishing complex group structures).

- Services that have deliberately provided, or depend upon, more anonymity in relation to the client's identity or regarding other participants, than is normal under the circumstances and in the experience of the legal professional.

- Settlement of default judgments or alternative dispute resolutions is made in an atypical manner (e.g. if satisfaction of a settlement or judgment debt is made too readily).

(c) Country or Geographic Risk

There is no unique definition of what consists a high-risk country or geographic location. However, there are several factors, which can be considered when assessing whether a particular country or location presents higher risk. It is important to conduct such an assessment to ensure that legal professionals do not engage in transactions emanating from such countries or, if they do, that they have well-established controls and procedures to mitigate the associated risk.

When it comes to the legal profession, some countries will present more serious AML/CFT concerns than others, and the risk level will vary depending on any of the elements of a transaction, including[6]:

According to guidance provided by the FATF, factors that are generally agreed to place a country in a higher risk category include:

[6] https://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20for%20Legal professionals%20in%20Precious%20Metal%20and%20Stones.pdf

- Countries/areas identified by credible sources[7] as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.

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

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

- 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, and in relation to which financial institutions (as well as DNFBPs) should give special attention to business relationships and transactions. The link to FATF statements may be consulted here: https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)-

- 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

In line with FATF guidance, the following factors should be considered by legal professionals when making an assessment of the country/geographical risk in relation to a proposed transaction:

[7] "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.

(d) Business Practices/Delivery Channels

Legal practices should also consider the channels used to deliver their products or services. In today's economy and global market, many delivery channels do not bring the client into direct face-to-face contact with the reporting entity (for example, Internet, telephone or mail), and are accessible 24 hours a day, 7 days a week, from almost anywhere. The remoteness of some of these distribution channels can also be used to obscure the true identity of a client or beneficial owners and can therefore pose higher risks. The examination of business practices and delivery channels should also include conducting a risk assessment of any new technologies (e.g. Internet based services) that you are planning to implement. The risk assessment should be conducted prior to the new technology being implemented.

3.1.1.1.1 Risk relating to Virtual Assets

VAs due to their distinct features and characteristics, have a higher ML/TF/PF risk associated with them. By their very nature, VAs enable non-face-to-face business relationships and provide the ability to transact across borders rapidly. These not only could allow criminals to acquire, move and store assets digitally inside and often outside regulated financial systems, but also conceal the origin or destination of funds, beneficial owner and ultimate beneficial owner.

In addition, VA products or services may enable pseudo-anonymous and anonymous transactions which also pose higher ML/TF/PF risks, particularly if they inhibit customer due diligence measures.

Legal Professionals who are involved in VAs or provide services to clients involved in VA activities should therefore consider the salient vulnerabilities, apply a risk-based approach when establishing or continuing relationships with such customers, evaluate the ML/TF/PF risks of the business relationship, and assess whether those risks can be appropriately mitigated and managed

A list of indicators of suspicious VA activities is provided in Section 7.1

3.1.1.2 Risk Assessment Tool

A risk assessment tool at Annex 1 provides an example, for use by legal professionals, to facilitate the assessment of the above factors. However, a legal professional's risk assessment has to be appropriate for their specific business and/or legal practice needs, which means that it may have to be more detailed than the checklist provided. Legal professionals can customize the checklist or can use a different method or another tool.

Legal professionals should ensure that they have an appropriate tool to assess the risks involved in using virtual asset.

3.1.2 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, legal professionals must establish policies, controls and procedures to mitigate and manage the ML/TF risks that they have identified as part of their assessment.

As part of its internal controls, when the risk assessment determines that risks are higher for ML or TF, the reporting entity has to develop written risk mitigation strategies (policies and procedures designed to mitigate high risk) and apply them for high risk situations.

It is important that the risk mitigation strategies are developed by the legal professional for higher risk situations and that these mitigation strategies are documented. This allows the risk mitigation strategies to be shared with management and employees. Furthermore, the application of the mitigation strategies should be recorded to demonstrate that mitigation measures have been applied. Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based approach. Senior management should approve the risk mitigations strategies and ensure that they are reviewed every time the risk assessment is up to date.

Furthermore, section 41 of the UN Sanctions Act states that a reporting person shall implement internal controls and other procedures to enable it to effectively comply with their obligations under this Act. As such, when a legal professional designs his AML/CFT program, detailed in the previous section, he must also ensure that he incorporates policies and procedures to ensure that he is not engaging in any transactions with designated or listed parties. Each of the building blocks of his AML/CFT program must also take into account the obligations under the UN Sanctions Act and the legal professional must have systems which will allow him to screen customers against the lists of designated or listed parties maintained by the NSS on its website. Additionally, any legal professional already registered with the FIU will also receive any changes to these lists as soon as these are made.

The development of a robust AML/CFT program is thus a crucial component of risk mitigation.

Risk mitigation strategies that can be applied have been identified at Annex 1.a.

3.1.3 Risk Monitoring

In addition to risk assessment and risk mitigation activities, a risk-based approach also requires legal professionals 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 legal professional'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.

4. Internal Controls

4.1 AML/CFT Program

An AML/CFT program is required to identify, mitigate and manage the risk of the products or services being offered by the legal professional that could facilitate money laundering or terrorism financing. Through an AML/CFT program, the legal professional is able to set out how it is going to implement its AML/CFT obligations.

As previously mentioned, AML/CFT programs should be risk-based. This means that legal professionals must develop their own program, tailored to their situation to mitigate money laundering and terrorism financing risks. This approach recognizes that not all aspects of an institution' business and/or legal practice 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.

It is highlighted that the AML/CFT program should be proportionate to the size, risk and nature of the legal professional's practice. It will also depend on the type of services offered and their level of complexity. It is acknowledged that in Mauritius, a significant number of barristers, attorneys and notaries are sole practitioners. Those who are in these types of arrangements, and who are captured by the AML/CFT framework because they perform any of the listed activities in Part 2 of the First Schedule of the FIAMLA, must therefore design an AML/CFT program which is a reflection of their activities, and of the risks that are associated with these activities. It is important to note that while

the regulator may have different expectations from each reporting person, this is not based on the size of the outfit exclusively. As mentioned in these guidelines, it is the level of risk which will primarily drive the expectations of the regulators. A sole practitioner (who is captured by the AML/CFT regulatory framework) may, from the regulator's perspective be more high risk than a law firm, depending on the type of clients, services offered and location of the clients and/or services.

Although not exhaustive, the list below provides the basics of an AML/CFT program:

- Appointment of key officers
- Policies and Procedures
- Training
- Audit and Review

As mentioned at the start of this chapter, having an AML/CFT program enables the legal professional to have a clear approach on how it is going to fulfill its AML/CFT obligations. These obligations are the following and are discussed in detail at Chapter 5 and 6 of these guidelines.

- Customer Due Diligence (CDD)
- Record Keeping
- Enhanced Due Diligence (EDD)
- Politically Exposed Persons (PEPs)
- Ongoing Monitoring
- Suspicious Transaction Reporting
- Training
- Terrorism Financing Obligations

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

4.1.1 Appointment of Key Officers

Subject to the size and nature of their business and/or legal practice, legal professionals, are required to appoint both a compliance officer and a Money Laundering Reporting Officer (MLRO) as part of their internal procedures and controls.

4.1.1.1 The Compliance Officer

The Compliance Officer (CO), who must be part of senior management is responsible for ensuring that the legal professional is complying with its AML/CFT obligations.

The legal professional must ensure that the CO:

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

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

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

(d) is fully aware of his or her obligations and those of the legal professional; 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 there under, are being met and that the legal professional is 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 legal professional considers 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.

4.1.1.2 The Money Laundering Reporting Officer

In accordance with Regulation 26(1) of FIAML Regulations 2018, legal professional 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 a sufficiently senior employee 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 the process of reporting any suspicion that they may have internally, to the MLRO. Records must be kept by the agent of both internal and external disclosures.

Where, due to its size or the nature of its business, legal professional 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 agent with the FIU directly.

4.1.2 Policies and Procedures

Legal professionals should have in place adequate policies, controls and procedures (PCPs) that promote high ethical and professional standards and prevent their business and/or legal practice from being misused by criminals. PCPs should clearly document the steps which the legal profession intends to follow in the implementation of each element of its AML/CFT Program. The legal professional must, for example, have policies on employee screening and procedures detailing how it will meet the expectation set out in its policy.

These policies, procedures and internal controls should be efficiently introduced and maintained and each legal professional should be aware of his responsibilities. All these PCPs must be widely publicized across the legal professional's business and/or legal practice and all its employees must be made aware of their role and existence. They should also be easily accessible across the business and/or legal practice.

4.1.3 Employment Screening and Training

4.1.3.1 Employment Screening

Legal professionals 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).

4.1.3.2 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 programmes for the directors, officers and employees of the legal professional, 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; and

(ii) 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 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 business and/or legal practice;
- 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.

Lastly, legal professionals must keep a record of all anti-money laundering and combating the financing of terrorism training delivered to their employees.

4.1.4 Auditing the AML/CFT Program

Putting in place an AML/CFT Program is not sufficient; the program must be monitored and evaluated. Legal professionals should assess their anti-money laundering and combating the financing of terrorism programs at a minimum every year 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.

Pursuant to Regulation 22(1)(d) of the Financial Intelligence and Anti-Money Regulations 2018, a Reporting person should also carry out an independent audit review. The independent audit review 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 practices the review can be conducted by the sole practitioner directly. Guidance can also be sought from professional bodies who could assist members with their audit.

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 independent audit review should be conducted at least every two years.

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.

5. Preventive Measures[8]

5.1 Customer Due Diligence: Identification and Verification Procedures

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

In line with section 17C of FIAMLA, legal professionals 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. The legal professional must keep all CDD information collected up to date. 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.

Timing of CDD

Identification and verification measures need to be carried out:

- When establishing a business relationship with a customer;
- When dealing with a one-off customer or counterparty and the transaction concerned is equal to or above 500,000 rupees whether conducted as a single transaction or several transactions that appear to be linked;
- Where there is a suspicion of money laundering or financing of terrorism; and

[8] These measures must only be adopted by law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.

- Where there are doubts concerning the veracity of previous customer/counterparty identification information.

5.1.1 Natural Persons (i.e. Individuals)

(a) Face to Face transactions

Regulation 4 of the FIAML Regulations requires that the legal professional 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.

Data to be collected	**Verification Methods**
1. Full legal and any other names, including, marital name, former legal name or alias 2. Date of birth 3. Gender 4. Place of birth 5. Nationality	▪ Current Valid National Identity Card ▪ Current Valid Passport ▪ Current valid driving licence- where the Legal Professional is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence. In each case, the document must incorporate a photographic evidence of identity. Where the legal person with which the natural person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary

6. Current residential address. (PO Box addresses are not acceptable) 7. Permanent residential address (if different to current residential address)	Any of the identity sources listed below: ▪ a recent utility bill issued to the individual by name; ▪ a recent bank or credit card statement; or ▪ a recent reference or letter of introduction from (i) a legal professional that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or (iii) a branch or subsidiary of a group headquartered in a well-regulated overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards. 'Recent' means within the last three months.
8. Any public position held and, where appropriate, nature of employment (including selfemployment) and name of employer	A letter or other written confirmation of the individual's status from the public body in question and or any enhanced CDD; a letter or other written confirmation of employment.
9. Government issued personal identification number or other government issued unique identifier	The relevant government document.

(b) 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, legal professionals 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 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 legal professional believes in good faith to be acceptable to it for the purposes of certifying.

5.1.2 Legal Persons and Legal Arrangements

Legal persons refer to any entities other than natural persons that can establish a permanent customer relationship with a reporting entity including a legal professional or otherwise own property.
In Mauritius, a legal person includes a company, a foundation, an association and a limited liability partnership. Legal arrangements, on the other hand, refers to express trusts or other similar legal arrangements. Examples of other similar arrangements (for AML/CFT purposes) include fiduciary.

Regulations 5, 6 and 7 of the FIAML Regulations 2018 lay down specific requirements where an applicant is a legal person or a legal arrangement.

(a) Legal persons (For example: Companies)

Legal professionals must, in relation companies, understand and document the nature of the company's business as well as the ownership and control structure. The following documents must be obtained to identify and verify the customer's identify:

i. The name, legal form and proof of existence of the company;
ii. Powers that regulate and bind the customer;
iii. The names of persons having senior management positions; and
iv. The address of the registered office or principal place of business.

Identification and Verification Methods for Legal Persons

Person to be identified	**Data to be identified**	**Verification Methods**
Underlying persons who are individuals.	As per the requirements for natural person Legal Professionals should collect identification data in relation to the following: 1.Directors 2.Beneficial Owner(s) 3.Significant Shareholders and 4.Authorised signatories. In the absence of an authorised signatory, the identity of the relevant person who is the senior managing officials. Senior managing official means an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer or who has the capacity to affect significantly the financial standing of a client.	▪ As per the requirements for natural person ▪ Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. ▪ However, where the legal person is high risk, or where a high-risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
1. Private companies 2. Partnerships 3. Sociétés 4. Foundations 5. Other legal persons	▪ Legal status of body ▪ Legal name of body ▪ Any trading names ▪ Nature of business ▪ Date and country of incorporation/registration ▪ Official identification number (for e.g., company number) ▪ Registered office address ▪ Mailing address (if different) ▪ Principal place of business / operations (if different) ▪ Any other data which the legal professional considers to be reasonably necessary for the purpose of establishing the true identity of the legal person	▪ Certificate of incorporation (or other appropriate certificate of registration or licensing); ▪ Memorandum and Articles of Association (or equivalent); ▪ Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; ▪ Latest audited financial statements or equivalent; ▪ Annual report or equivalent; ▪ Personal visit to principal place of business; ▪ Partnership deed or equivalent; ▪ Charter of Foundation; ▪ Acte de société; ▪ Certificate of good standing from a relevant national body; ▪ Reputable and satisfactory third-party date such as a business information service ▪ Any other source of information that to verify that the document submitted is genuine.

Where identification information relating to a legal person is not available from a public source, a legal professional will be dependent on the information that is provided by the legal person. Legal professionals should accordingly treat such information with care and in any event in accordance with the legal person's risk assessment.

Settlor

A legal professional 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

A legal professional 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 a legal professional is satisfied that it knows who the beneficiaries are. This does not require a legal professional to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the legal professional 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), a legal professional 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, a legal professional 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, a legal professional 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, a legal professional 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), a legal professional 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), a legal professional 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, a legal professional should satisfy itself that it has sufficient information to identify the individual beneficial owner.

Individual and Corporate Trustee

Where a legal professional is not itself acting as trustee, it is necessary for a legal professional 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, a legal professional should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A legal professional 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 website of the body that regulates the trustee and of the regulated trustee itself).

Identification and Verification Methods for Legal Arrangements

Person/ arrangement to be identified	Data to be identified	Verification Methods
Underlying persons who are individuals.	As per the requirements for natural person	▪ As per the requirements for natural person
Underlying principals who are legal persons	As per the requirements for legal persons above In circumstances where an applicant for business which is a legal arrangement acts or purports to act on behalf of a legal person, then identification and verification must take place not just in respect of that legal person, but also in respect of that legal person's underlying principals.	▪ As per the requirements for legal persons above
Legal arrangement	1. Legal status of arrangement (including date of establishment) 2. Legal name of arrangement (if applicable) 3. Trading or other given name(s) of arrangement (if applicable) 4. Nature of business 5. Any official registration or identifying number (if applicable) 6. Registered office address (if applicable) 7. Mailing address (if different) 8. Principal place of business/ operations (if different) 9. Any other data which the legal professional considers to be reasonably necessary for the purposes of establishing the true identity of the legal arrangement.	Trust deed or equivalent instrument ▪ Official certificate of registration (if ▪ applicable) Where the above proves insufficient, ▪ any other document or other source of information on which it is reasonable to place reliance in all the circumstances.

Legal professionals must seek and obtain assurances from the trustee/s (or controlling individual/s) that all of the data requested by the legal professional under the above process has been provided, and that the individual(s) will notify the legal professional in the event of any subsequent changes.

Where identification information relating to a legal arrangement is not available from a public source, a legal professional will be dependent on the information that is provided by the legal arrangement (usually through its controlling individuals, such as trustees). Legal professionals should accordingly treat such information with care and in any event in accordance with the legal arrangement risk assessment.

5.1.3 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, Legal professionals 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,[9] 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, legal professionals 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.

[9] An example could be an individual in the context of organized crime where an individual who does not have an ownership stake in the company but exercises control through influence.

5.1.4 Individuals acting on Behalf of Applicants for Business and Customers

There might be cases where customers (particularly those which are legal persons) will have one or more individuals authorised to act on their behalf in dealing with legal professionals.

Legal professionals must have in place appropriate policies, procedures and controls to ensure that they are able to identify and verify the identity of all persons purporting to act on behalf of customers, and to confirm the authority of such persons to act. Legal professionals must, in the case of individuals acting on behalf of customers, obtain identification data and verify that data, in line with guidelines provided above.

Where the legal professional is unable to determine whether the customer is acting for a third party or not, it shall make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit.

5.1.5 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, legal professionals must also ensure that the requirements of Regulation 21 of the FIAML Regulations are fulfilled and that –

i. the necessary information required is obtained immediately;
ii. he is satisfied 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. he is satisfied 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. he shall not rely on a third party based in a high-risk country.

5.1.6 Inability to Establish Customer Identity

Where the legal professional cannot obtain all the information required to establish the identity of the customer to its full satisfaction, he shall not commence the business relation or perform the transaction and shall file a suspicious transaction report with the FIU.

In accordance with Regulation 9(3) of the FIAML, 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—

(a) this is essential not to interrupt the normal conduct of business;

(b) the verification of identity occurs as soon as reasonably practicable; and

(c) the money laundering and terrorism financing risks are effectively managed by the reporting person.

Moreover, if during the course of its business activities, the legal professional has doubts about the veracity or adequacy of previously obtained client identification data, he must identify and verify the identity of the customer and beneficial owner before conducting any further.

5.2 Record Keeping

All legal professionals are required to keep records of all the transactions in which they are involved and of all customers. The following records must be kept:

a) Records relating to the identification of customers and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as business correspondence for at least 7years after the business relationship has ended.

b) Records concerning transactions, both domestic and international shall be kept for a period of 7 years after the completion of the transaction; and

c) Copies of all STRs filed with the FIU shall also be kept for a period of at least 7 years from the date the report was made.

5.3 Enhanced Due Diligence (EDD)

Regulation 12 of the FIAML Regulations 2018 provides that legal professionals shall implement internal controls and other procedures to combat money laundering and financing of terrorism, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.

Where the ML/TF risks are identified to be higher, legal professionals shall take EDD measures to mitigate and manage those risks.

The EDD measures that may apply for higher risk relationships should include:

(a) requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship and the source of fund/wealth;

(c) obtaining information on the intended or performed transactions;

(d) obtaining the approval of senior management to commence or continue the business relationship;

(e) conducting close monitoring of the business relationship; and

(f) any other measures the legal professional may undertake with relation to a high-risk relationship.

Where a legal professional is unable to perform the required Enhanced CDD requirements, the latter shall terminate the business relationship and file a suspicious transaction report under section 14 of the FIAMLA.

See below for EDD measures to applicable to politically exposed persons (PEPs)

5.4 Simplified Due Diligence

In general, legal professionals should apply the full range of CDD measures. However, simplified CDD measures can be implemented in cases where lower risks have been identified. The simplified CDD measures have to be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

Where a legal professional determines that there is a low level of risk, he shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment of his supervisory authority or regulatory body, whichever is most recently issued. Importantly, simplified CDD shall not apply where, a legal professional knows, suspects, or has reasonable grounds for knowing or suspecting that a customer is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer is being carried out on behalf of another person engaged in money laundering or terrorist financing. The possibility of applying simplified CDD is not an exemption for CDD measures. It only allows for the application of reduced measures.

The ultimate decision rests with the legal professional and there may be instances, depending on the level of risk and all the known circumstances (a high-risk relationship e.g. PEP will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these simplified measures. Under all circumstances, legal professionals must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if simplified CDD measures are adopted. Legal professionals are required to keep the risk assessment and level of CDD requirements under review and the level of risk of the CDD measures should be consistent with the risk of the relationship. Where simplified CDD measures are adopted, legal professionals should apply a risk-based approach to determine whether to adopt the simplified CDD measures in a given situation and/or continue with the simplified measures, although these customers' accounts are still subject to transaction monitoring obligations.

5.5 Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic and international organisations, as well as the close relatives and associates of such persons. Pursuant to the FIAML Regulations 2018, PEPs have been classified as “domestic PEPs,” “foreign PEPs” and “international organization PEPs” in the FIAML Regulations.

5.5.1 Types of PEPs

(a) Domestic PEPs

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.

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

(b) Foreign PEPs

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

(c) International Organization PEPs

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.

(d) Close Associates and Family members

As provided by regulation 15(5) FIAML Regulations, in addition to the primary PEPs listed above, a PEP also includes close associates and family members.

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.

5.5.2 PEPs and Due Diligence Measures

Business relationships with PEPs pose a greater than normal money laundering risk to legal professionals, 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, legal professionals are required to have a clear policy in relation to transactions involving such persons. Legal professionals 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, legal professionals shall apply all the above measures to family members or close associates of all types of PEP.

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.

5.6 Ongoing Monitoring

Legal professionals have the obligation of filing STRs with the FIU pursuant to section 14 of FIAMLA. The ability to file an STR of good quality is heavily reliant on the robustness of the systems put in place by the legal professional. In fact, legal professionals 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. As part of the monitoring of transactions, legal professionals must examine the background and purpose of each transaction especially where these are complex, unusually large or conducted in unusual patterns. Equally, they must pay attention to transactions that do not seem to have an apparent economic or lawful purpose.

5.6.1 Reporting Suspicious Transactions

Pursuant to Section 14 of FIAMLA, legal professionals are obliged to file suspicious transaction reports (STRs) as soon as they become aware of a suspicious transaction. An STR must be filed not later than 5 working days after the suspicion arose. Failure to report an STR or failure to reasonably become aware of a suspicious transaction are both offences under the FIAMLA. The FIU has an approved form for the filing of STRs. A copy of the form is available on the website of the FIU on the link below:
STR_FORM_FINAL_VERSION.pdf (fiumauritius.org)

Information on the manner in which a STR shall be reported is contained in the FIU's Guidance Note No. 3 which is also available on the FIU's website.

5.6.2 Suspicious Transaction

Under the FIAMLA, a suspicious transaction is one which gives rise to a reasonable suspicion that it may involve -

(a) the laundering of money or the proceeds of any crime; or
(b) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment whether or not the funds represent the proceeds of crime

Additionally, suspicious transactions:

(c) are made in circumstances of unusual or unjustified complexity;

(d) Appear to have no economic justification or lawful objective;

(e) Are made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made; or

(f) Gives rise to suspicion for any other reason.

A transaction includes:

(a) 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; and

(b) a proposed transaction or an attempted transaction.

For further details on how to identify and report a suspicious transaction, please refer to the FIU current Guidance Note No 3, mentioned above. The offence for failing to report an STR is set out under section 14 of the FIAMLA. The penalty is a fine not exceeding one million rupees and imprisonment for a term not exceeding 5 years.

5.6.3 Request for Information by the FIU

Under section 13(2) (a) and 13(2)(b) of FIAMLA, the Director of the FIU may request additional information from legal professionals 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 from legal professionals, whenever the FIU becomes aware of information that may give rise to reasonable suspicion of ML/TF offences, or it has received a request from 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 legal professionals to inform it if a person has been their client, or has acted on behalf of their client; or whether a client of the legal professional has acted for a person.

If legal professionals fail 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. Furthermore, the falsification, concealment, destruction or disposal of any document or material which is likely to be relevant to a request under Section 13(2), (3) or (6) also consists of an offence under the FIAMLA.

5.6.4 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.

5.6.5 Tipping Off

After making a suspicious transaction report to the FIU, section 16 (1) of FIAMLA prevents legal professionals 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 years.

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 legal professional should immediately file an STR with the FIU.

5.6.6 Registration with the FIU

Also, in line with section 14C of the FIAMLA, the legal professional must register with the FIU, within such time, form and manner as may be prescribed. The Financial Intelligence and Anti Money Laundering (Registration of Reporting Persons) Regulations 2019 were made on 5th November 2019 to this effect. All legal professionals who fall within the purview of the FIAMLA must register with the FIU in accordance with the time frames which shall be specified by the FIU.

5.7 Cash Prohibition

Moreover, legal professionals 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.

6. Terrorist Financing Offences

6.1 Introduction

Terrorist organizations require funds to plan and carry out attacks, train militants, pay their operatives and promote their ideologies. The Convention for the Suppression of the Financing of Terrorism Act and the Prevention of Terrorism Act criminalize the financing of the terrorism in Mauritius. Additionally, the UN Sanctions Act provides the legal framework for implementing targeted financial sanctions imposed by the United Nations Security Council.

6.2 Extension of Obligations

According to section 19H & K of the FIAMLA, a legal professional[10] falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act. Legal professionals should be aware that once a person has been designated domestically or listed by the UN, it is an offence to deal with the funds or other assets of such a person. It is also an offence to make funds or other assets available to a designated party or listed party. As soon as there is a designation or a listing, two prohibitions prevail under the UN Sanctions Act:

- A prohibition to deal with the funds or other assets of the designated or listed party under section 23; and
- A prohibition to make available funds or other assets to the designated or listed party under section 24.

The prohibitions to apply to all persons.

Under the UN Sanctions Act, there are also several reporting obligations which apply to legal professionals. These are set out below.

[10] As explained previously, this refers to law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.

6.3 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 or other assets
    - where the funds or other assets were intended to be sent.

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.

The NSS has made available forms for reporting under Section 23(4) and Section 25(2) of the UN Sanctions Act. These forms can be accessed under the "Guidelines" tab of the NSS website:
Index (govmu.org)

Additionally, the forms are also accessible on the FIU website:

FIU - Targeted Financial Sanctions (fiumauritius.org)

Contact details for the National Sanctions Secretariat:

National Sanctions Secretariat
Prime Minister's Office (Home Affairs)
Fourth floor
New Government Centre
Port Louis

Phone Number: (+230) 201 1264 / 201 1366
Fax: (+230) 211 9272
Email: nssec@govmu.org

6.4 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 legal professional should be submitted to the FIU in accordance with section 14 of the FIAMLA.
For more information about how to file STRs, please refer to Section 4.1.8 of this guideline.

7. ML/TF Indicators for Legal professionals[11]

There are a number of situations, which may give rise to a suspicion that a transaction may involve money laundering. The list of situations given below is meant to assist law firms and legal professionals to detect/identify suspicious or unusual transactions in the conduct of their operations and business activities. It is not a prescriptive list of all possible transactions linked to money laundering or terrorism financing. Nor does it imply that the transactions listed below are necessarily linked to such activities. The role of legal professionals is to be familiar with these indicators, and exercise sound judgment based on their knowledge and where they identify any "suspicious or unusual transactions", know the proper action to take.

The client is overly secret or evasive about:

- who the client is
- who the beneficial owner is
- where the money is coming from
- why they are doing this transaction this way or what the big picture is.

<u>The client:</u>

- is using any legal professional or intermediary without good reason
- is actively avoiding personal contact without good reason
- is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution
- holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved.

[11] As defined under these guidelines.

- provides false or counterfeited documentation
- is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact.
- is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals
- is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities.
- shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries and suspicious transaction reports – that is – asks repeated questions on the procedures for applying the ordinary standards.

<u>The parties:</u>

- The parties or their representatives (and, where applicable, the real owners or intermediary companies in the chain of ownership of legal entities), are native to, resident in or incorporated in a high-risk country
- The parties to the transaction are connected without an apparent business reason.
- The ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason for the transaction.
- There are multiple appearances of the same parties in transactions over a short period of time.
- The age of the executing parties is unusual for the transaction, especially if they are under legal age, or the executing parties are incapacitated, and there is no logical explanation for their involvement.
- There are attempts to disguise the real owner or parties to the transaction.
- The person actually directing the operation is not one of the formal parties to the transaction or their representative.
- The natural person acting as a director or representative does not appear a suitable representative.
- The transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.

- The client or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation.

The source of funds is unusual:

- third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation
- funds received from or sent to a foreign country when there is no apparent connection between the country and the client
- funds received from or sent to high-risk countries.
- The client is using multiple bank accounts or foreign accounts without good reason.
- Private expenditure is funded by a company, business or government.
- Selecting the method of payment has been deferred to a date very close to the time of notarization, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation.
- An unusually short repayment period has been set without logical explanation.
- Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.
- The asset is purchased with cash and then rapidly used as collateral for a loan.
- There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested which are not appropriate for the common practice used for the ordered transaction.
- Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.
- The collateral being provided for the transaction is currently located in a high-risk country.
- There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.
- There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.
- The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation.

- There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (e.g. volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.
- Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons.

The choice of lawyer

- Instruction of a legal professional at a distance from the client or transaction without legitimate or economic reason.
- Instruction of a legal professional without experience in a particular specialty or without experience in providing services in complicated or especially large transactions.
- The client is prepared to pay substantially higher fees than usual, without legitimate reason.
- The client has changed advisor a number of times in a short space of time or engaged multiple legal advisers without legitimate reason.
- The type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting.
- The required service was refused by another professional or the relationship with another professional was terminated.

Nature of the retainer

The transaction is unusual, e.g.:

- the transactions are unusual because of their size, nature, frequency, or manner of execution
- there are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional
- a non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body.

The client:

- is involved in transactions which do not correspond to his normal professional or business activities
- shows he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested
- wishes to establish or take over a legal person or entity with a dubious description of the aim, or a description of the aim which is not related to his normal professional or commercial activities or his other activities, or with a description of the aim for which a license is required, while the customer does not have the intention to obtain such a licence
- frequently changes legal structures and/or managers of legal persons
- asks for short-cuts or unexplained speed in completing a transaction
- appears very disinterested in the outcome of the retainer
- requires introduction to financial institutions to help secure banking facilities
- Creation of complicated ownership structures when there is no legitimate or economic reason.
- Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason.
- Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short period of time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation.
- There is an absence of documentation to support the client's story, previous transactions, or company activities.
- There are several elements in common between a number of transactions in a short period of time without logical explanations.
- Back to back property transactions, with rapidly increasing value or purchase price.
- Abandoned transactions with no concern for the fee level or after receipt of funds.
- There are unexplained changes in instructions, especially at the last minute.
- The retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services. ▪ There is a lack of sensible commercial/financial/tax or legal reason for the transaction.
- There is increased complexity in the transaction or the structures used for the transaction which results in higher taxes and fees than apparently necessary.

- A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation.
- Investment in immovable property, in the absence of any links with the place where the property is located and/ or of any financial advantage from the investment.
- Litigation is settled too easily or quickly, with little/no involvement by the legal professional retained.
- Requests for payments to third parties without substantiating reason or corresponding transaction.

7.1 VA related Indicators

The existence of a single red flag indicator does not necessarily indicate criminal activity, and often it is the presence of multiple indicators in a transaction with no logical business explanation that raises suspicion of potential criminal activity. However, the presence of such indicators should raise further monitoring, examination, and reporting. The following sections contains a non-exhaustive list of potential red flags indicators of suspicious VA/VASP activities and has been categorised under six themes, namely;

1) Anonymity
2) Transactions
3) Transaction Patterns
4) Senders or Recipients
5) Source of Funds or Wealth
6) Geography

1. Anonymity

The various technological features of VAs increase anonymity and even though the mere presence of this feature does not automatically suggest an illicit transaction, it does nevertheless add hurdles to the detection of criminal activity by Regulators and Law Enforcement Agencies (“LEAs”). The below non-exhaustive red flag indicators demonstrate how criminals can make use of technological features associated with VAs that increase anonymity.

- Customers prepared to pay additional transaction fees for one or more types of VAs with technological features providing higher anonymity.
- Customers entering the digital platforms of VASPs and ITOs using an Internet protocol (IP) address that allows anonymous communication such as the Onion router, I2P or IP associated with a darknet.
- Receiving funds from or sending funds to VASPs and ITOs with weak or non-existent CDD or Know Your Customer (“KYC”) requirements.
- The use of decentralised/un-hosted, hardware or paper wallets to transport VAs across borders. Decentralised VA systems are particularly vulnerable to anonymity risks compared to a centralised system where some risks are mitigated.

- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Abnormal volume of VAs cashed out at exchanges from P2P (Peer-to-Peer) platform associated wallets with no logical business explanation.

2. Transaction

While VAs are still not widely used by the public, their use has caught on among criminals. The use of VAs for money laundering purposes first emerged over a decade ago, but VAs are becoming increasingly mainstream for criminal activity more broadly. The second non-exhaustive list of indicators demonstrate how red flags traditionally associated with transactions involving more conventional means of payment, remain relevant in detecting potential illicit VA-related activities.

- Structuring of VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions – in short succession, such as within a 24-hour period, in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which are particularly common in ransomware cases related to VAs or to a newly created or to a previously inactive account.
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; orthere is non-existent or weak AML/CFT regulation.

3. Transaction patterns

Similar to the above section, the non-exhaustive list of indicators below illustrates how the misuse of VAs for ML/TF purposes could be identified through irregular, unusual or uncommon patterns of transactions.

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.
- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit on the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after.
- A new user attempts to trade the entire balance of VAs or withdraws the VAs and attempts to send the entire balance off the platform.
- Making frequent transfers of large amounts in a certain period of time (e.g., a day, a week, a month, etc.) to the same VA account by more than one person; or from the same IP address by one or more persons.
- Conducting VA-fiat currency exchange at a potential loss.

4. Senders or Recipients

The non-exhaustive indicators listed below relates to the profile and unusual behaviour of either the sender or the recipient of the illicit transactions including irregularities observed during account creation and CDD process.

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
- Sender/recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.
- A customer provides identification or account credentials shared by another account.
- A customer is known via publicly available information to law enforcement due to previous criminal association..
- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.
- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.

5. Source of Funds or Wealth

The misuse of VAs is often related to criminal activities such as illicit trafficking in narcotics, and psychotropic substances, fraud, theft, and extortion. Below are common red flags related to the source of funds or wealth linked to such criminal activities:

- Transacting with VA addresses that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- VA transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
- Deposits into a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an ITO where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.

6. Geography

This last set of non-exhaustive red flag indicators stress on how criminals, when moving their illicit funds, can take advantage of the varying stages of implementation across jurisdictions.

- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- Customer making use of VASPs located in a high-risk jurisdiction having inadequate AML/CFT regulations.
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

Annex 1. Risk Assessment Form for Legal Professionals[12]

Name of Legal Professional: _____

The *Financial Intelligence Anti-Money Laundering Act* requires legal professionals (to conduct a risk assessment of their exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist in meeting these obligations. This form is presented as an example only. Legal Professionals may choose to conduct their 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 and/or legal practice.

The results of this risk assessment should be communicated to all legal professionals engaged in prescribed activities 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.

[12] Refers to law firms/foreign law firms/joint law venture/foreign lawyers and individual law practitioners (barristers/attorneys and notaries) who perform any of the activities listed in Part 2 of the First Schedule of FIAMLA.

Risk Assessment

Higher risk clients and situations	Yes Higher Risk	No Moderate risk	Suggested Control Measures
■ **Clients**			
Are your clients foreigners?			■ Determine if individuals are politically exposed persons.[13] ■ 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 real estate 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 owns or controls the funds or property)?			■ Obtain name of natural person(s) behind company, trust or other legal arrangements.[14] ■ 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.

[13] 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.

[14] For further information on how to comply with your beneficial ownership obligations please consult the Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism for Legal Professionals.

Do your clients that engage in activities that are consistent with the indicators identified for Suspicious Transactions? (See Guidance Note on AML/CFT Guidance on Suspicious Transaction Reports for suspicious transactions indicators and the indicators listed in this guideline).			■ Consider filing a Suspicious Transaction Report (STR). ■ Obtain additional information on source of funds or source of wealth.

Link to the Guidance note: Annexure III (fiumauritius.org)			
■ **Products, services and transactions**			
Do you undertake high value transactions?			■ Pay special attention for unusual transaction and ML/TF indicators. ■ Obtain additional information on source of funds or source of wealth.
Do you sell gold bars or loose diamonds?			■ Pay special attention for unusual transaction and ML/TF indicators. ■ Obtain additional information on source of funds or source of wealth.
■ **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: FIU - Home (fiumauritius.org) United Nations: United Nations Security Council Consolidated List | United Nations Security Council			■ 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? Research and Analysis (imolin.org) Corporate Tax Haven Index 2021 (taxjustice.net)			■ 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 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: Documents - Financial Action Task Force (FATF) (fatf-gafi.org)			■ 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 organizations 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? View 2020 results (taxjustice.net)			■ 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.
Are any of your clients or the source funds originate from a high level of financial secrecy? https://www.financialsecrecyindex.com /introduction/fsi-2018-results			■ 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 rupees 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
Do you have clients that are referred to you by a third party (such as a lawyer, accountant or other real estate legal professional)?			■ 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.
Do you have short-term or part-time employees?			■ Include AML/CFT obligations in job descriptions and performance reviews. ■ Deliver comprehensive AML/CFT training for all employees
Other risk factors: (list any additional factors)			

Signature of the Legal professional ***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. Ask for an additional piece of identification to confirm the identity.
3. Obtain name of natural person(s) behind company, trust or other legal arrangement.
4. Monitor if client conducts additional real estate transactions.
5. Obtain information on source of funds or source of wealth of the client.
6. Deliver more frequent employee training.
7. Monitor AML/CFT legislative and regulatory changes.
8. Include AML/CFT obligations in job descriptions and performance reviews.
9. Set limits to cash transaction amounts (less than the 500,000 rupees prohibition).
10. Request bank drafts instead of accepting large amounts of cash.
11. Conduct transaction only in person.
12. Obtain appropriate additional information to understand the client's business or circumstances.
13. Conduct transaction only in person.
14. 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).
15. Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship.
16. Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained.
17. Obtaining information on the reasons for intended or performed transactions.
18. 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.
19. Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

Annex 2: Template for AML/CFT Policies and Procedures

Address | City Postal Code| Telephone

Email

NAME OF ENTITY

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

---

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/legal professionals will identify suspicious transactions (should refer to ML/TF indicators)
- Who is your Money Laundering Reporting Officer?
- How employees/legal professionals 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/legal professionals on:
  - How to identify a suspicious transaction? ○ What are the AML/CTF obligations?
  - How to implement your policies and procedures?

Terrorist Financing Obligations (Section 25 (1) of the UN Sanctions Act 2019)

- 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

CONTACT DETAILS

Attorney General's Office

Renganaden Seeneevassen Building

Port-Louis

Republic of Mauritius
Telephone: (230) 203-4740
Fax: (230) 212-6742
Email: lawfirm.ago@govmu.org

Financial Intelligence Unit
Compliance Division

10th Floor SICOM Tower
Ebene Cybercity
Republic of Mauritius
Telephone: (230) 454 1423
Fax: (230) 466 2431

Email: compliance@fiumauritius.org