CORPORATE AND BUSINESS REGISTRATION DEPARTMENT (CBRD)

GUIDELINES ON THE MEASURES FOR THE PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM FOR COMPANY SERVICE PROVIDERS (CSPs)

Issued on 16th March 2020

CONTENTS

ACRONYMS

AML/CFT	-	ANTI-MONEY LAUNDERING / COMBATING THE FINANCING OF TERRORISM
CBRD	-	CORPORATE AND BUSINESS REGISTRATION DEPARTMENT
CDD	-	CLIENT DUE DILIGENCE
CSPs	-	COMPANY SERVICE PROVIDERS
DNFBPS	-	DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS
ESAAMLG	-	EASTERN AND SOUTHERN AFRICA ANTI-MONEY LAUNDERING
GROUP FATF	-	FINANCIAL ACTION TASK FORCE
FIU	-	FINANCIAL INTELLIGENCEUNIT
FIAMLA	-	FINANCIAL INTELLIGENCE AND ANTI- MONEY LAUNDERING ACT 2002
LP	-	LEGAL PERSONS
LA	-	LEGAL ARRANGEMENTS
ML	-	MONEYLAUNDERING
PEP	-	POLITICALLY EXPOSED PERSON
STR	-	SUSPICIOUS TRANSACTION REPORT
TCSP	-	TRUST AND COMPANY SERVICE PROVIDER
TF	-	TERRORISM FINANCING / FINANCING OF TERRORISM

1. INTRODUCTION

This document is being issued pursuant to section 10 (2) (ba) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002, as amended by the Anti-money Laundering and Counter Terrorism Financing and Proliferation (Miscellaneous Provisions) Act 2019. It is intended to assist Regulators of CSP to comply with their obligations in relation to the prevention, detection and reporting of money laundering, financing of terrorism and proliferation. In the process, the accounting and auditing profession will not be misused by money launderers or those involved in dubious transactions.

1.1 Purpose and Scope of the Guidelines

CSP in this guideline has the same definition as per the Companies Act and the FIAMLA. CSPs may become a preferred channel for criminals for hiding illicit gains. In view of the national overall rating ML vulnerability of Mauritius is medium high, the role of the CSPs is fundamental. The second factor influencing the overall national ML vulnerability rating is the overall sector. The National Risk Assessment Report highlights that amongst other DNFBPs, Company Service Providers have been rated as medium-high. 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 any suspicious transaction/activity.

This document has been issued pursuant to section 10(2)(ba) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002. They are intended to assist CSPs 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, the profession can safeguard that it is not misused by money launderers or those financing terrorism or proliferation.

1.2 Businesses and Individuals covered by the Guidelines

This guideline is addressed to the following:

CSPs under the definition of the companies Act

Company Service Providers

167A. Registration as company service provider

(1) No person shall provide any of the following services, as a business, unless he is registered as a company service provider with the Registrar –

(a) acting as a formation agent 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;

(b) acting, or causing for 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, a foundation, a limited liability partnership or such other entity as may be prescribed;

(c) 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

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

Definition under the FIAMLA:

" company service provider" –

(a) means a person, registered under section 164 or 167A of the Companies Act, who provides any of the services specified in section 167A of that Act; but does not include –

(i) a barrister, an attorney or a notary, or a law firm, foreign law firm, joint venture or foreign lawyer under the Law Practitioners Act;

(ii)a professional accountant, public accountant and member firm under the Financial Reporting Act; and

(iii) the holder of a management licence under section 77 of the Financial Services Act;

(b) Company secretaries

(c) Company representatives.

1.3 Compliance with Guidelines and Enforcement

The recent amendments to the FIAMLA, the CBRD - Corporate and Business Registration Department- is now the Supervisor for CSPs. These amendments have empowered the Registrar with a supervisory role for ensuring that AML/CFT measures are complied with

According to section 10(3) of the FIAMLA "any institution to which, or person to whom, guidelines are issued under subsection (2) (ba) or (c) shall comply with those guidelines".

Furthermore, section 10(4) of the FIAMLA stipulates that "Where an institution or a person fails to comply with guidelines issued under subsection (3), the institution or person shall be liable to pay a penalty not exceeding 50,000 rupees for each day on which such breach occurs as from the date on which the breach is notified or otherwise comes to the attention of the FIU (Financial Intelligence Unit) and such penalty may be recovered by the Director as if it were a civil debt".

2. MONEY LAUNDERING AND FINANCING OF TERRORISM

(i) 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:

(ii) 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.

(iii) 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 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.

(i) 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 or real estate.

(ii) 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 terrorism also move funds to conceal their source of those funds. The motive is to prevent leaving a trail of incriminating evidence.

(iii) 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. AML/CFT LEGISLATIVE FRAMEWORK

The Financial Action Task Force (FATF) was established in 1989 by the G7 countries. 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. The FATF standards are reflected in its 40 Recommendations issued in February 2012. These are universally recognized international standards for anti-money laundering and countering financing of terrorism (AML/CFT).

The new 40 Recommendations are available on the following website:
http://www.fatfgafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaundering
And currently the membership of the FATF includes 36 members and 8 Associate Members, including the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

3.1 ESAAMLG

ESAAMLG was founded in 1999 and its main objective is to ensure that its Members comply with the FATF standards. ESAAMLG was also admitted as an associate member of the FATF, in June 2010.
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.

In Mauritius' 2018 Mutual Evaluation Report, some deficiencies in the AML/CFT framework were identified and recommendations were made to the Government to address them. Subsequently, Parliament made appropriate legislative changes to improve our AML/CFT framework.

3.2 Mauritius AML/CFT Legislative Framework

The CBRD was designated as 'Regulatory Body' for CSPs through amendment to the FIAMLA. Also, the FIAMLA was amended so that those CSPs which fail to comply with Guidelines issued by the CBRD may be liable to a penalty not exceeding 50,000 rupees for each day such breach occurs. The CBRD may also apply administrative sanctions to CSPs when non-compliance with AML/CFT obligations is identified.

The latest amendments brought to the AML/CFT legislation were in 2019. Regulatory bodies, which include the CBRD, for the purpose of ensuring compliance with the guidelines, may require the CSPs to furnish such information to the FIU or produce such record or document that they may require. CSPs are also required to furnish such information or produce such record or document required under subsection 10(6) of the FIAMLA, to its regulatory body; namely the CBRD. In case of non-compliance, CSPs shall

commit an offence and shall, on conviction, be liable to a fine not exceeding 500,000 rupees and to imprisonment for a term not exceeding 5 years.

The main pieces of legislation that relate to terrorism financing are the Convention for the Suppression of the Financing of Terrorism Act 2003 and the Prevention of Terrorism (Special Measures) Regulations 2003. The Prevention of Terrorism Act 2002 deals with the acts of terrorism under the purview of the Commissioner of Police. It is also required (Section 14 of FIAMLA) that CSPs must report suspicious transactions, which include funds that may be linked to financing of terrorism to the FIU.

3.3 The Financial Intelligence Unit (FIU)

The Mauritius FIU was set up in August 2002 under the provisions of section 9 of the FIAMLA. It is the central agency in Mauritius responsible for the following:-
Receiving, requesting, analyzing and disseminating to the investigatory and supervisory authorities. –
- Disclosures of information regarding suspected proceeds of crime
- Alleged money laundering offences as well as the financing of any activities or transactions related to terrorism.
- FIU is responsible for receiving STR and other reports from CSPs and other reporting entities.

It was the first FIU to be set up in Africa and became member of the Egmont Group in July 2003. For general information on the FIU and the Egmont Group, please visit their websites: www.fiumauritius.org and www.egmontgroup.org

4. RISK BASED APPROACH TO AML/CFT

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. In particular, countries have a duty to require DNFBPs to identify, assess, and take effective action to mitigate their money laundering and terrorist financing risks.

Provisions already exist in FIAMLA for assessment and mitigation of risks for reporting entities. Under section 3(2) of FIAMLA, any CSP is required to take such measures that are necessary to ensure that its 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 2 million rupees and penal servitude for a term not exceeding 10 years.

The other measures mitigating the risks of money laundering and financing of terrorism are set out under section 17 and 10 (2) (ba) of the FIAMLA.

No CSP can reasonably be expected to detect all wrong doing by clients, including money laundering and terrorism financing. However, if any CSP develops systems and procedures to detect, monitor and report the riskier clients and transactions, it will reduce its possibilities of being misused by criminals.

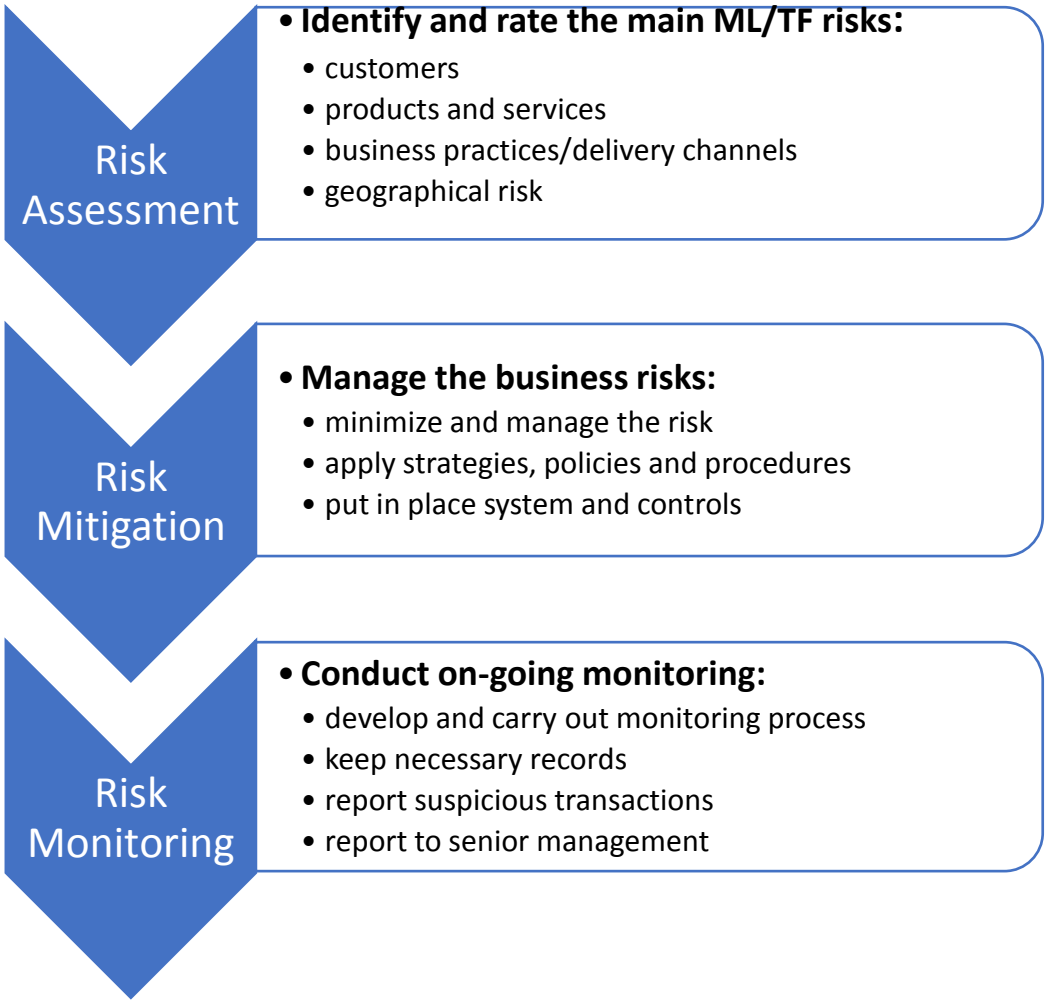
A risk-based approach also requires CSPs to have systems and controls that are commensurate with the specific risks of money laundering and financing of terrorism facing them. Assessing this risk is, therefore,

one of the most important steps in creating a good anti-money laundering compliance program. As money laundering risks increase, stronger controls are necessary.

4.1 Risk-Based Approach for CSPs

In the context of CSPs, the risk of money laundering or financing of terrorism is defined as the risk of the professional services being used directly or indirectly by criminals to channel illicit money. In accordance with AML/CFT laws and revised FATF Recommendations of 2012, CSPs should be responsible for assessing their exposure to the risk of money laundering and financing of terrorism. The purpose of establishing a risk-based approach is to make sure that anti money laundering and financing of terrorism measures applied by CSPs are proportionate to the identified risk.

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.



The categories, criteria and elements of risks defined below identify potential risks of money laundering

and financing of terrorism. 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.

4.1.1 Factors to determine Risk

The FATF risk based guidance for TCSPs sets out all the determining risk factors:

a) The client base
b) The services and products provided
c) Geographic location
d) Delivery channels and business practices

4.1.2 Risk of Client base

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 the UNSCR 1267 (Al Qaeda Sanction List) or 1373, persons whose assets may have been frozen under section 45 of the Dangerous Drugs Act,
(ii) clients considered as high risk (for example, Politically Exposed Persons),
(iii) medium risk client,
(iv) low /standard risk client.

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

a) Titling a residential property in the name of third party; for example, a friend, relative, business associate or lawyer.
b) 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.
c) Non face to face client
d) Politically exposed persons (PEPs)
e) Persons whose assets have been frozen under section 45 of the Dangerous Drugs Act
f) Clients with an affiliation to countries with high levels of corruption or from which terrorist organizations operate.
g) Sectors or industries where opportunities for ML/TF are particularly prevalent
h) Clients conducting their business relationship or requesting services in unusual or unconventional circumstances
i) Clients where the structure of the entity makes it difficult to identify the beneficial owner
j) Management of the company appears to be acting on instructions from unknown or inappropriate person(s)
k) Unnecessarily complex ownership or control structure
l) Cash intensive businesses
m) Non Profit Organizations (NPOs) not subject to monitoring
n) Instructions or funds outside of their personal or business sector profile
o) Individual or classes of transactions that take place outside the established business profile, and expected activities/ transaction unclear

p) Payments received from un-associated or unknown third parties and payments for fees in cash where this would not be a typical method of payment
q) Large international payments with no business rationale
r) Inexplicable change in ownership
s) Legal structure altered frequently without explanation
t) Over and under or multiple invoicing of goods or services
u) Reluctant to provide relevant information
v) Previous criminal records
w) Transfer of the seat of a company to another jurisdiction without any justification
x) No address or multiple address
y) Use of legal persons and arrangements without any apparent legal or legitimate tax, business, economic or other reason

4.2 Risk of Products/Services

An essential element of risk assessment is to review new and existing services that the CSPs 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.

Given the nature of services offered by CSPs, they may be exposed to transactions risks such as:-
Transaction/service and associated delivery channel risk

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

a) Use of pooled client accounts or safe custody of client money or assets or bearer shares, without justification.

b) Situations where advice on the setting up of legal persons or legal arrangements may be misused to obscure ownership or real economic purpose (including setting up of trusts, companies or other legal entities, or change of name/corporate seat or establishing complex group structures). This might include advising in relation to a discretionary trust that gives the trustee discretionary power to name a class of beneficiaries that does not include the real beneficiary (e.g. naming a charity as the sole discretionary beneficiary initially with a view to adding the real beneficiaries at a later stage). It might also include situations where a trust is set up for the purpose of managing shares in a company with the intention of making it more difficult to determine the beneficiaries of assets managed by the trust.

c) In case of an express trust, an unexplained (where explanation is warranted) nature of classes of beneficiaries and acting trustees of such a trust.

d) Services where TCSPs 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.

e) Services that are capable of concealing beneficial ownership from competent authorities.

f) 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 TCSP.

g) Use of virtual assets and other anonymous means of payment and wealth transfer within the transaction without apparent legal, tax, business, economic or other legitimate reason.

h) Transactions using unusual means of payment (e.g. precious metals or stones).

i) The postponement of a payment for an asset or service delivered immediately to a date far from the moment at which payment would normally be expected to occur, without appropriate assurances that payment will be made.

j) Successive capital or other contributions in a short period of time to the same company with no apparent legal, tax, business, economic or other legitimate reason.

k) Acquisitions of businesses in liquidation with no apparent legal, tax, business, economic or other legitimate reason.

l) Power of Representation given in unusual conditions (e.g. when it is granted irrevocably or in relation to specific assets) and the stated reasons for these conditions are unclear or illogical.

m) Transactions involving closely connected persons and for which the client and/or its financial advisors provide inconsistent or irrational explanations and are subsequently unwilling or unable to explain by reference to legal, tax, business, economic or other legitimate reason.

n) Situations where a nominee is being used (e.g. friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the beneficial owner), with no apparent legal, tax, business, economic or other legitimate reason.

o) Commercial, private, or real property transactions or services to be carried out by the trust, company or other legal entity with no apparent legitimate business, economic, tax, family governance, or legal reasons.

p) Products/services that have inherently provided more anonymity or confidentiality without a legitimate purpose.

q) Existence of suspicion of fraudulent transactions, or transactions that are improperly accounted for. These might include: i. over or under invoicing of goods/services. ii. Multiple invoicing of the same goods/services. iii. Falsely described goods/services – over or under shipments (e.g. false entries on bills of lading). iv. Multiple trading of goods/services.

r) Any attempt by the settlor, trustee, company or other legal entity to enter into any fraudulent transaction.

s) Any attempt by the settlor, trustee, company or other legal entity to enter into any arrangement to fraudulently evade tax in any relevant jurisdiction.

As stated in the FATF guidance on CSPs at:
https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf

4.3 Geographical locations of the business/clients/products being used

Geographic location is generally accepted as a contributing factor to the level of risk. However, there is definite, independent system for assessing the money laundering risks of various territories. While some firms may design their own methods of assessing the jurisdictional risk, other may take certain elements into consideration namely:

(i) lists published by authorities in different jurisdictions e.g., U.S Office of Foreign Assets Control, the U.S. Financial Crimes Enforcement Network, the European Union, the World Bank and the United Nations Security Council Committee,

(ii) whether the country is a member of the FATF or of a FATF-style regional body and has AML requirements equivalent to international best practices
(iii) overall reputation of the country
(iv) Political instability Regime
(iv) High levels of internal drug production or to be in drug transit regions. Reference can be made to annual International Narcotics Control Strategy Report and yearly "Corruption Perception Index", among others.

4.4 Business practices/delivery channels

CSPs 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 (eg. Internet based services) that you are planning to implement. The risk assessment should be conducted prior to the new technology being implemented.

4.5 Risk Assessment Tool

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

4.6 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. As part of its internal controls, when the risk assessment determines that risks are higher for ML or FT, 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. Annex 2 provides a list of risk mitigation measures that may be appropriate for situations that you have determined to be high risk.

It is important that the risk mitigation strategies are developed by the CSPs 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 updated.

4.7 Risk monitoring

In addition to risk assessment and risk mitigation activities, a risk-based approach also requires CSPs 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 at any point in time.

The reporting entity's policies, controls and procedures has 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.

5. 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 CSPs that could facilitate money laundering or terrorism financing.

AML/CFT programs should be risk based. This means that CSPs should adopt the program tailored to their situation to mitigate money laundering and terrorism financing risks. This approach recognizes that not all aspects of an institution's business present the same level of risks. The reporting entity is in the best position to assess the risk of their clients, products and services and to allocate resources to counter the identified high risk areas. The basics of an AML/CFT program consist of the following elements:

- Internal policies, procedures and controls
- Nomination of a compliance officer and Money Laundering Reporting Officer (MLRO) at the management level
- Suspicious Transaction Reporting & Monitoring
- On-going Employment Screening and training program
- Independent/self audit function to test the AML/CFT program

5.1 Internal policies, procedures and controls

CSPs should arrange to have in place adequate policies, procedures and internal controls that promote high ethical and professional standards and prevent their profession from being misused by criminals. These policies, procedures and internal controls should be efficiently introduced and maintained and CSPs and qualified secretaries should be aware of their responsibilities, thus ensuring compliance with FIAMLA

2002 and the Guidelines whereby their AML safety obligations are mentioned. Annex 3 provides a template to assist CSPs in the development of internal policies, procedures and controls

5.2 Appointment of Key Officers

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

5.3 The Compliance Officer

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

The CSPs must ensure that the CO:-

(a) has timely and unrestricted access to the records of the CSP;
(b) has sufficient resources to perform his or her duties;
(c) has the full co-operation of the CSP's staff;
(d) is fully aware of his or her obligations and those of the CSP; 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 CSP 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 CSP where applicable and senior management;
(b) undertaking day-to-day oversight of the program for combating 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 combating 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 CSP considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfill both roles effectively.

5.4 The Money Laundering Reporting Officer

In accordance with Regulation 26(1) of FIAML Regulations 2018, the CSP shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable

suspicion that another person is engaged in money laundering or the financing of terrorism. The MLRO must be sufficiently senior within the organization and must have the technical skills required to make an assessment of internal reports prior to determining whether an STR should be filed with the FIU.

There should be clear reporting lines internally, to ensure that all employees including directors or partners, know what the process is to report any suspicion that they may have internally to the MLRO. Records must be kept by the CSP of both internal and external disclosures.

Where due to its size or the nature of its business a CSP 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 Regulations. In these instances, the STR is filed by the CSP with the FIU directly.

5.5 EMPLOYMENT SCREENING AND TRAINING

5.5.1 Employment Screening

CSPs should apply strict screening procedures before employing their personnel. They should put in place measures as to ensure high standards when hiring employees. In this context, 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;
- 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).

5.5.2 Employee Training

A training program should be designed to train the appropriate personnel on a regular basis. A successful training program not only should meet the standards set out in laws (i.e. FIAMLA Act 2002) but should also satisfy internal policies and procedures in place. For the purpose of this "Guideline", 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 along with the following:

a) Legal Requirements under relevant AML/CFT legislations[6] and the statutory obligations under these laws

b) Understanding ML/TF risk of the sector and of their firm

c) Penalties for anti-money laundering violations

d) How to react when facing a suspicious client or transaction

e) Duties and accountabilities of employees

f) New developments together with information on current money laundering and financing of terrorism techniques, methods and trends.

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

All CSPs should keep records of all the transactions in which they are involved and the identification data of clients (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) and business correspondence for at least seven years after the business relationship has ended. This will enable competent authorities to investigate and prosecute money laundering offences or other related offences. Furthermore, they should keep records on all internal reports of suspicious transactions that have been raised by their employees to the responsible officer, the reasons/documentations for not filing any such reports to the FIU, reports of suspicious transactions flagged to the FIU, training provided to their employees, if applicable, or training that the CSPs have undergone in respect of the following:

Financial Intelligence and Anti-Money Laundering Act 2002, the Prevention of Corruption Act 2002 in so far as it is applicable to money laundering, the Prevention of Terrorism Act 2002 with regard to the financing of terrorism and the Convention for the Suppression of the Financing of Terrorism Act 2003 and Regulations applicable to them.

5.6 Auditing AML/CFT program

5.6.1 Auditing/Review of AML/CFT Program

Putting in place an AML/CFT Program is not sufficient; the program must be monitored and evaluated. The CSPs should assess their anti-money laundering programs at a minimum every two years to ensure their effectiveness and to look for new risk factors. The audit program should address issues such as :

(i) the adequacy of AML risk assessment
(ii) the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements.
(iii) the adequacy of the risk based approach in relation to the services offered clients and geographic locations
(iv) 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 record keeping
(viii) Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transaction among others.

The audit can be conducted by an internal or external auditor. If the reporting entity does not have an auditor, it can conduct a self-review given their important role they play. 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 proprietorships, the review can be conducted by the sole proprietor directly.

The objective of a self-review is similar to the objectives of a review conducted by internal or external auditors. It should address whether policies and procedures are in place and are being adhered to, and whether procedures and practices comply with legislative and regulatory requirements.

The results of the audit should be documented and presented either to the Board of Directors (if applicable) or to senior management. The recommended changes should be implemented no later than a month following the completion of the audit.

6. Preventive Measures

6.1. Identification and Verification Procedures

Where the CSPs cannot obtain all the information required to establish the identity of the client to its full satisfaction, he shall not commence the business relation or perform the transaction and consider making a suspicious transaction report to the FIU. Moreover, if during the course of its business activities, the CSPs have doubts about the veracity or adequacy of previously obtained client identification data, he should terminate the business relationship and consider making a suspicious transaction report to the FIU.

It is important that the CSPs know with whom they are dealing with ("know your customer" principle) when they carry out either face to face or non-face to face transactions. They need to identify and verify the true identity of their respective client or if the client is being represented by the authorised person(s) acting on behalf of the client. In case of corporate bodies, they need to ascertain the company's ultimate beneficial owner, 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.

Identification and verification measures need to be in place:

a) when establishing a business relationship,
b) when entering into a transaction,
c) when dealing with a one-off client,
d) where there is a suspicion of money laundering or financing of terrorism; and
e) where there are doubts concerning the veracity of previous identification information.

It is essential that the current permanent address of the client be verified as an integral part of identity. Satisfactory evidence of address can be obtained by a recent utility bill or a recent bank or credit card statement or a recent bank reference or any other document or documents which either singly or cumulatively establishes, beyond reasonable doubt, the address of the applicant for client
The information gathered above should assist the CSPs to develop a sound CDD program. Also, it will enable the CSPs to develop transaction and activity profile of the client, assess and grade the money laundering and financing of terrorism risks that the client may pose.

6.2 Individuals (Face to Face transactions)

An individual's identity consists of a totality of his name, current address, previous addresses, date of birth, place of birth, photo, ID, employment history, financial history and family circumstances.

6.2.1 Residents of Mauritius

The residence criteria should be verified from an original official valid document such as National identity cards, current valid passports, or current valid driving licenses or any proof of address such as utility bills.

CSPs may also request for additional verification of identity by:-

i. checking a local telephone directory
ii. checking a current register of electors
iii. visiting the applicant for business at his permanent residential address.

Identify means to ascertain who a person claims to be.
Verify means to obtain evidence that tends to show that the person is who he says he is.

Non Resident of Mauritius.:

Regarding clients who are not resident in Mauritius but who make face-to-face contact with any CSP, they should be required to provide the following information 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 residency certificate. Documents required are namely: National Identity Card or current valid passports, and or current valid driving licenses.

6.2.2 Individuals – (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, CSPs should apply uniformly effective customer identification procedures as for those mentioned above (for both residents and non- residents of Mauritius) and other specific and appropriate measures to mitigate the higher risk posed by non-face-to-face verification of clients.

A copy of any important document should be duly certified by a lawyer, accountant or other professional persons.

6.2.2.1 Corporate

(a) Domestic Companies

With regard to domestic companies, CSPs should verify:

(i) the identity of those who ultimately own or have control over the company's business and assets, more particularly,

(ii) their directors,

(iii) their significant shareholders and their representatives signatories,

(iv) the legal existence of the company directly from the website of the CBRD.

Documents should be verified in the case of locally incorporated companies:

(i) their directors and significant shareholders (the documents as are required for the identification of a personal customer);

(ii) Official details which collectively establish the status and legal existence of that entity, e.g. the original or certified copy of the certificate of incorporation of company, details of its registered office and place of business etc.

Enquiries may be carried out through verification on the website of CBRD. In case of doubts and on sight verifications may be held to check whether the entity is engaged in legitimate business activities.

6.2.2.2 Legal Arrangements

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

i. the settlor;

ii. the protector;

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

iv. the beneficiaries or class of beneficiaries; and

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

6.2.2.3 Settlor

A CSP 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.

6.2.2.4 Beneficiaries

A CSP 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 CSP is satisfied that it knows who the beneficiaries are. This does not require a CSP to verify the identity of all beneficiaries using reliable, independent source documents, data or information but the CSP 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 CSP should obtain information to enable it to identify the named discretionary beneficiaries (e.g. as identified in the trust deed).

6.2.2.5 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 CSP 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 CSP 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 CSP 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 CSP 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 CSP 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 CSP should satisfy itself that it has sufficient information to identify the individual beneficial owner.

6.2.2.6 Individual and Corporate Trustee

Where a CSP is not itself acting as trustee, it is necessary for a CSP 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 CSP should obtain information to enable it to satisfy itself as to the identity of the directors or other controlling persons. A CSP can rely on external evidence, such as information in the public domain, to satisfy itself as to the beneficial owner of the regulated trustee (e.g. the web-site of the body that regulates the trustee and of the regulated trustee itself).

6.2.2.7 Sociétés

Procedures set out for verification of individual clients may be applied to verify the identity of those in control of the société. Besides for sociétés, the original or certified copy of the Acte de Société should be requested and retained and for Mauritian sociétés, the CSPs should ensure, by verifying with the Registrar of Companies, that the société does not continues to exist after its expiration.

6.2.2.8 Third Party Reliance for CDD measures

In case of entities that are subject to AML/CFT inspections and CDD measures by licensee of other sector supervisors/regulatory bodies, the CSPs may rely on the CDD carried out by the corresponding licensee of that sector supervisor on its licensee, e.g., the CSPs may rely on the CDD carried out by management companies on the directors, shareholders and ultimate beneficial owners of the GBCs which are client of the CSPs. However, simplified CDD measures shall not be acceptable whenever the CSPs has suspicion of money laundering or financing of terrorism activities being carried out by their clients. In case CDD is carried out by another authority, the CSPs must ensure that the information on the client, director, shareholders and ultimate beneficial owners of entities are readily available to them otherwise they will remain liable.

6.3 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, CSPs must identify and take reasonable measures to

verify the identity of the beneficial owners. This should be done by obtaining the following information:

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

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

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

When gathering the above data, CSPs 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.

6.3.1 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 CSPs.

CSPs 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. CSPs 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 CSP 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.

6.4 Verification of Source of Wealth

Source of wealth describes the activities which have generated the total net worth of a person both within and outside a business relationship, that is, those activities which have generated a client's net assets and property.

Verification can be performed by checking the (i) Details of the client's occupation, or (ii) details of any businesses currently owned and the client's role within such businesses, or (iii) details of any businesses sold by the client, (iv) details of any wealth (including businesses) inherited from other family members among others.

6.5 Enhanced Due Diligence (EDD)

Regulation 12 of the FIAML Regulations 2018 provides that CSPs 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, CSPs 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 CSP may undertake with relation to a high-risk relationship.

Where a CSP 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). A list of enhanced due diligence measures can be found at Annex 2.

6.6 Record Keeping

All dealers 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.

6.7 Simplified Due Diligence

In general, the full range of CDD measures should be applied by CSPs. 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 CSP 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 CSP 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 of measures. It only allows for the application of reduced measures. The ultimate decision rests with the CSP 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, CSPs must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if simplified CDD measures are adopted. CSPs 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, CSPs 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.

6.8 Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic and international organisation, 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.

6.8.1 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 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.

6.8.2 PEPs and Due Diligence Measures

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

6.9 Suspicious Transaction Reporting & Monitoring

Proper due diligence may require management to gather further information regarding a client or his transaction before deeming it suspicious and deciding to report to the FIU as part of a AML/CFT program. Systems for monitoring and reporting suspicious activity should be risk-based, and should be determined by factors such as the firm's size, the nature of its business, its location, frequency and size of transactions and the types and geographical location of its clients, among others. In such context internal reports may be created. Some of the reports may include:

- The procedures to identify potential suspicious transactions or activity.
- A formal evaluation of each instance, and continuation, of unusual transactions or activity.
- A documentation of the suspicious transaction reporting decision, whether or not filed with the authorities.

Procedures within each entity may be determined for reporting suspicious transactions to the FIU, taking into consideration speed and confidentiality principles.

6.9.1 The Process of Suspicious Transaction Reporting

Section 14 of FIAMLA imposes an obligation on CSPs to make a report, **as soon as possible but not later than 15 working days,** to the FIU of any transaction which they have reason to believe may be suspicious. The form, as approved by the FIU and in accordance with section 15 of the FIAMLA, to be used for reporting suspicious transaction is the Suspicious Transaction Report (STR) Form. A copy of the form is available on the website of the FIU on the link below:
http://www.fiumauritius.org/images/stories/STR_FORM_FINAL_VERSION.pdf

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

6.9.2 Suspicious Transaction

'*Suspicious transaction*' is defined under FIAMLA as *a transaction which (a) gives rise to a reasonable suspicion that it may involve (i) the laundering of money or the proceeds of any crime; or (ii) funds linked or related to, or to be used for, financing of terrorism or by proscribed organizations, whether or not the funds represent the proceeds of a crime; (b) is made in circumstances of unusual or unjustified complexity; (c) appears to have no economic justification or lawful objective; (d) is 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; (e) gives rise to suspicion for any other reason.*

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 19 of the FIAMLA. The penalty is a fine not exceeding one million rupees and imprisonment for a term not exceeding 5 year

6.9.3 Request for Information by the FIU

Under Section 13(2) and section 13(3) of FIAMLA, the Director of the FIU may, having regard to the complexity of a case, request additional information from CSPs who submitted the suspicious transaction report or from any other reporting entity 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 CSPs, 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 CSPs 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 per section 19 of the FIAMLA.

6.9.4 Protection of Information

Confidentiality is a key success factor for the operations of an FIU. Under 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. 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.

The FIU takes all the necessary precautions to protect the identity of the person reporting the suspicious transaction when disclosing the information to law enforcement or other competent authorities. As regards physical security, the FIU Mauritius has a well-defined architecture covering access control. Confidentiality of IT-information and databases is well-preserved by IT Security Policies and Procedures.

6.9.5 Tipping Off

After making a suspicious transaction report to the FIU, Section 16 (1) of FIAMLA prevents CSPs 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) or 13(3) of FIAMLA. It shall amount to an offence under the Act punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

6.10 Terrorist Financing Offences

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.

6.10.1 Extension of Obligations

According to section 19H & K of the FIAMLA, a CSP falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act. CSPs 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 (including all CSPs). Under the UN Sanctions Act, there are also several reporting obligations which apply to CSPs. These are set out below.

6.10.2 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.

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

6.10.3 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 CSP should be submitted to the FIU in accordance with section 14 of the FIAMLA. For more information on how to file an STR please refer to the previous section of this guideline.

6.10.4 Internal controls

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 CSP 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 CSP 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 CSP already registered with the FIU will also receive any changes to these lists as soon as

these are made.

6.11 Cash Prohibition

Moreover, CSPs 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.
A transaction is defined as an opening 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 it includes also a proposed transaction.

7. ML/TF INDICATORS FOR CSPs

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 CSPs to detect/identify “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 CSPs’ agents is to be familiar with these indicators, and exercise sound judgment based on their knowledge of the CSPs’ industry, and wherever they identify any “suspicious transactions”, they know which action to take. Some indicator of suspicious transactions include:

a) Transactions that require the use of complex and opaque legal entities and arrangements;

b) The payment of “consultancy fees” to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies;

c) The transfer of funds in the form of “loans” to individuals from trusts and non-bank shell companies. These non-traditional “loans” then facilitate a system of regular transfers to these corporate vehicles from the “borrowing” individuals in the form of “loan repayments”;

d) Cases of corruption where the company paying the bribe to secure a contract or the person brokering a contract will seek to secure a successful outcome by utilising a TCSP to operate a trust with the funds held on deposit for the benefit of the person approving the contract;The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain or submit to competent authorities information on the beneficial ownership of corporate structures formed by them;

e) The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs;

f) The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws;

g) The use by prospective clients of nominee agreements to hide from the TCSP the beneficial ownership of client companies;

h) The carrying out of multiple intercompany loan transactions and/or multijurisdictional wire transfers that have no apparent legal or commercial purpose;

i) Clients who require the use of pre-constituted shell companies in jurisdictions that allow their use but do not require updating of ownership information; and

j) TCSPs that market themselves and/or their jurisdictions as facilitating anonymity and disguised asset ownership.

A more detailed list of indicators can be consulted on:
https://www.fatfgafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf

8. GENERAL GLOSSARY

- "Criminal activity" refers to: (a) all criminal acts that would constitute a predicate offence for money laundering in Mauritius or (b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 3 of the FATF.
- "criminal" means a person committing or intending to commit a criminal activity
- DNFBP" means a business or profession, who is carrying on the below business or profession

  - real estate developers or agents which carry out transactions with a customer involving the buying or selling of real property;
  - dealers in precious metals or precious stones;
  - law firms, notary firms, or other independent legal businesses;
  - accounting, audit firms;

- "guidelines" means the guidelines issued by the FIU under section 10(2)(ba) to members of relevant profession or occupation;
- "member of relevant profession or occupation" , as per First Schedule Part I of the FIAMLA, consists of the following:

  (a) Agent in Land and/or Building or Estate Agency under the Local Government Act
  (b) Attorney
  (c) Barrister
  (d) Dealer under the Jewellery Act
  (e) Land Promoter and Property Developer under the Local Government Act
  (f) Law firm, foreign law firm, joint law venture, foreign lawyer,
  (g) Licensed auditor under the Financial Reporting Act
  (h) Notary
  (i) Person licensed to operate a casino, gaming house, gaming machine, totalisator, bookmaker and interactive gambling under the Gambling Regulatory Authority Act
  (j) Professional accountant, public accountant and member firm under the Financial Reporting Act

- "One-off client" means any client carrying out transaction other than in the course of a business relationship.
- Politically Exposed Persons" has the same meaning as per the Guidance Notes on Anti- Money Laundering and Combating the Financing of Terrorism for Financial Institutions issued by the Bank of Mauritius issued in June 2005 (updated as at July2014)
- "suspicious transaction" means a transaction which–

  (a) gives rise to a reasonable suspicion that it may involve-

  (i) the laundering of money or the proceeds of any crime or

  (ii) funds linked or related to, or to be used for, terrorist financing or by proscribed organisations, whether or not the funds represent the proceeds of crime;

(b) is made in circumstances of unusual or unjustified complexity;

(c) appears to have no economic justification or lawful objective;

(d) is 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

(e) gives rise to suspicion for any other reason.

(f) Useful Websites

CBRD	**www.companies.govmu.org**
FIU	**www.fiumauritius.org**
FATF	**www.fatf-gafi.org**
ESAAMLG	**www.esaamlg.org**

CONTACT DETAILS:-

Corporate Business Registration Department (CBRD)
1 Cathedral Square,
Jules Koenig Street
Port Louis
Tel: 202 0600
comd@govmu.org

Annex 1. Risk Assessment Form for CSPS

Name of CSP:_____

The *Financial Intelligence Anti-Money Laundering Act* requires CSPs to conduct a risk assessment of your exposure to money laundering and terrorism financing and apply corresponding mitigation and controls. This checklist is meant to assist you in meeting these obligations. This form is presented as an example only. You may choose to conduct your risk assessment using a different approach.

Instructions: When you answer yes to one of the questions, this situation or client is considered higher risk and a control measures to reduce the risk should be applied. For each higher risk client or situation a suggested control measure is proposed. You can adapt the control measures to correspond to your business (see Annex 1.A for a list of control measures).

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

Risk Assessment

Higher risk clients and situations	**Yes** **Higher risk**	**No** **Moderate risk**	**Suggested Control Measures**
Clients			
Are your clients or beneficial owners of legal persons or legal arrangement foreigners?			• Determine if individuals are politically exposed persons. • Obtain additional information on source of funds or source of wealth.
Do you have clients or beneficial owners of legal persons or legal arrangement 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 ongoing 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. • 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.
Do your clients that engage in activities that are consistent with the indicators identified for Suspicious Transactions? (See Section 12 of this Guideline and the Guidance Note on AML/CFT Guidance on Suspicious Transaction Reports for suspicious transactions indicators). http://www.fiumauritius.org/English/Reporting/Documents/Guidance%20Note_310817.pdf			• Consider filing a Suspicious Transaction Report (STR). • Obtain additional information on source of funds or source of wealth.
Products and services			
Do you facilitate transactions that involve shell companies?			• Obtain senior management approval to proceed with the transaction. • Obtain information on the shell company. • Ask for additional information, piece of

			identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
Geographic Risk			
Do any of your clients or the source funds originate from foreign jurisdictions known for high levels of financial secrecy or jurisdictions with low tax rates? http://www.imolin.org/imolin/finhaeng.html#Map.%20%20Major%20Financial%20Havens https://www.financialsecrecyindex.com/en/			• 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 you carry out multiple intercompany loan transactions and/or multijurisdictional wire transfers?			• Document rationale for transactions. • Ask for additional information, piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth. • Monitor fund destination to identify high risk jurisdictions.
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 http://www.fiumauritius.org/English/United%20Nations%20Security%20Council/Pages/default.aspx United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list			• Obtain senior management approval to proceed with the transaction. • Ask for additional information, piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.

• Do any of your clients or the source funds originate from foreign jurisdictions identified by the Financial Action Task Force (FATF) as having strategic deficiencies in the fight against money laundering or subject to an FATF statement? FATF: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
• Do any of your clients or the source funds originate from jurisdictions identified by credible sources (for example international 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? http://www.transparency.org/news/feature/corruption_perceptions_index_2016			• Obtain senior management approval to proceed with the transaction. • Ask for an additional piece of identification to confirm the identity. • Obtain additional information on source of funds or source of wealth.
Delivery channel and business practices			•
Do you accept cash?			• Confirm source of funds • Set limits to cash transaction amounts recognizing the 500,000 rupee cash prohibition outlined in the FIAMLA. • Request bank drafts instead of accepting large amounts of cash.

Do you conduct transactions where you do not meet the client?			• Deliver comprehensive AML/CFT training to your employees specifically focused on client due diligence requirements • Ask for an additional piece of identification to confirm the identity. • Confirm the beneficial owner (the natural person who owns or controls the funds or property) • Confirm that any intermediary has the necessary documentation to act on behalf of the client. • Conduct periodic review of records to ensure that client due diligence requirements are adequately implemented
Do you have clients that are referred to you by a third party (such as a lawyer, accountant or other CSPs)?			• 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 agents?			• Include AML/CFT obligations in job descriptions and performance reviews. • Deliver comprehensive AML/CFT training for all employees
Do you undertake high value transactions (over 50 million rupees)?			• Pay special attention for unusual transaction and ML/TF indicators. • Obtain additional

			information on source of funds or source of wealth.
Other risk factors: (list any additional factors)			

_____ _____

Signature of the CSP ***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.

    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).
    Obtaining additional information and, as appropriate, substantiating documentation, on the intended nature of the business relationship.
    Obtaining information on the source of funds and/or source of wealth of the client and clearly evidencing this through appropriate documentation obtained.
14. Obtaining information on the reasons for intended or performed transactions.
15. 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.
16. Requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.
17. Enhanced CDD may also include lowering the threshold of ownership for beneficial ownership purposes, to ensure complete understanding of the control structure of the entity involved. It may also include looking further than simply holdings of equity shares, to understand the voting rights of each party who holds an interest in the entity.

Annex 2. Template for Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Policies and Procedures

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

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

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

See how to conduct a risk assessment in real estate sector for additional guidance.

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 real estate 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 17Fof FIAMLA)

Describe how you will comply with record keeping requirements including:

- How long will you retain records related to real estate 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 12of 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 15of 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 FIAMLA)
Describe how you will comply with ongoing monitoring requirements including:

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

Suspicious transaction Reporting (Section 15 of the FIAMLA)

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

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

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

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

Training (Regulation 22 (1) (c) of the FIAMLR)
Describe how you will comply with training requirements including:

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

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