BANK OF MAURITIUS

GUIDELINE ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION

January 2020

Table of Content

1. INTRODUCTION

1.01 The ability to launder the proceeds of criminal activity through the financial system is a key element to the success of criminal operations.

1.02 The unchecked use of the financial systems for this purpose has the potential to undermine individual financial institutions and, ultimately, the entire financial sector. The increased integration of the world's financial systems, the removal of barriers to the free movement of capital and the expansion of electronic banking have enhanced the ease with which criminal money can be laundered and simultaneously complicate the tracing process.

1.03 Terrorists acts perpetrated by terrorists and terrorist organizations also necessitate money, which may be derived from diverse sources and layered through the global financial system to conceal the destination and the purpose for which the money has been collected. Terrorists and terrorist organizations therefore employ techniques similar to those used by money launderers to hide the sources and uses of their money.

1.04 Similarly, money is required for the proliferation of weapons of mass destruction (WMD)[1]. In view of the interconnectedness between proliferation financing[2] and terrorism and terrorism financing, it is essential to counter these financing activities in order to prevent the commission of terrorist acts. In fact, a number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials.

1.05 The Financial Action Task Force (FATF)[3] has developed a series of Recommendations[4] that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. A key element of the FATF's revised 2012 Recommendations is the application of a risk based approach. Under the risk-based approach, countries and financial institutions are expected to understand, identify and assess their ML/TF risks, take appropriate actions to mitigate those risks and allocate their resources efficiently by focusing on higher risk areas.

1.06 These Recommendations form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. They are intended to be of universal application.

1.07 In recognition of the nefarious consequences of money laundering and the financing of terrorism and proliferation, the State of the Republic of Mauritius has through numerous initiatives demonstrated its firm willingness to combat money laundering and terrorist and proliferation financing.

---

[1] The FATF defines proliferation of weapons of mass destruction (WMD) as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials.

[2] Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

[3] The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

[4] The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation issued, in February 2012, by the FATF are available on the website of the FATF at www.fatf-gafi.org.

1.08 Mauritius has, further, committed itself to the FATF Forty Recommendations and to its Mutual Evaluation procedure.

1.09 Mauritius being a founder member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)[5], which is an associate member of the FATF, participates in a self-assessment process to assess its progress in implementing the FATF Recommendations.

1.10 Mauritius has also ratified and acceded to numerous international conventions, protocols and treaties to express its commitment towards the international community to combat this scourge.

1.11 Several pieces of legislations have been enacted since the year 2000 to combat money laundering and terrorism financing. The legal framework was further enhanced in 2018 with a view to aligning it with the 2012 FATF Standards, amongst others.

1.12 The relevant legislative enhancements aimed at strengthening the AML/CFT framework by, inter alia,:

(a) enabling Mauritius to adhere to FATF Recommendations 6 and 7 and to implement the restrictive measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations, through the enactment of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (UN Sanctions Act).

(b) enhancing the existing legal framework for preventive measures that apply to financial institutions and Designated Non-Financial Businesses and Professions, which are now collectively referred to as "reporting persons" in the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) and the Financial Intelligence and Anti-Money Laundering Regulations 2018 (FIAML Regulations) which address the following FATF requirements, inter alia:

(i) Customer Due Diligence;
(ii) Politically exposed persons;
(iii) Correspondent banking;
(iv) Money or value transfer services;
(v) New technologies;
(vi) Wire transfers;
(vii) Reliance on third parties; and
(viii) Internal control and foreign branches and subsidiaries.

(c) extending the scope of the FIAMLA to include the financing of proliferation;

(d) establishing a legal framework to support the National Risk Assessment exercise;

[5] The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), which comprises 18 countries in the eastern and southern African region, is a Regional Body subscribing to global standards to combat money laundering and financing of terrorism and proliferation. Its main objectives are to -
(a) adopt and implement the 40 Recommendations of the FATF;
(b) apply anti-money laundering measures to all serious crime;
(c) implement measures to combat the financing of terrorism, and
(d) implement any other measures contained in the multilateral agreements and initiatives relevant to prevention and control of laundering of proceeds of all serious crimes and the financing of terrorism and proliferation of weapons of mass destruction.

(e) vesting Regulatory Bodies, specified in Part I of the First Schedule of FIAMLA, with the powers to supervise and enforce compliance by members of relevant professions or occupations falling under their purview with the AML/CFT requirements imposed under the FIAMLA and the UN Sanctions Act and any regulations or guidelines made thereunder.

1.13 Mauritius has also adopted a National Strategy for Combating Money Laundering and the Financing of Terrorism and Proliferation 2019-2022 which sets out the approach which Mauritius will adopt to tackle money laundering (ML), terrorist financing (TF) and proliferation financing (PF) threats over the next three years. In addition, it describes the priorities and objectives in addressing financial crime, and assists Mauritius in meeting international obligations set by the Financial Action Task Force.

1.14 The Strategy is based on the findings of the National Risk Assessment (NRA) and the gaps identified in the AML/CFT Mutual Evaluation Report (MER) of Mauritius, which was published in September 2018.

1.15 The National AML/CFT Strategy comprises eight core themes that enhances the ability of Mauritius to prevent, detect and deter money laundering and the financing of terrorism and proliferation, namely –

(i) strengthening the AML/CFT legal and regulatory framework;
(ii) implementing a comprehensive risk-based supervision framework;
(iii) strengthening the process by which the ML/TF threats are detected and disrupted, criminals are prosecuted and illegal proceeds are confiscated;
(iv) enhancing national co-ordination and cooperation;
(v) consolidating capacity building, training and awareness raising programs;
(vi) enhancing transparency of legal persons and arrangements;
(vii) implementing an effective data collection management system in all relevant competent authorities; and
(viii) enhancing regional and international cooperation.

1.16 In view of the substantive changes brought to the AML/CFT legislative and regulatory framework, a review of the Guidance Notes on AML/CFT (Guidance Notes) issued by the Bank of Mauritius in June 2005 and updated as at July 2017, was necessary.

2. AUTHORITY, PURPOSE, SCOPE OF APPLICATION AND STATUS OF THIS GUIDELINE

AUTHORITY

2.01 The Bank of Mauritius ('Bank') is the designated AML/CFT supervisory authority of financial institutions under its purview and is required to supervise financial institutions with respect to the AML/CFT requirements set out under the banking laws[6] by, inter alia, ascertaining that these requirements are effectively complied with and implemented by these financial institutions.

2.02 For the purposes of this Guideline and unless specified otherwise, "financial institution" shall include banks[7], non-bank deposit taking institutions[8], cash dealers[9], and money lenders[10] licensed by the Bank of Mauritius under the Banking Act 2004 as well as any licencee[11] under the National Payment Systems Act 2018.

2.03 The Guideline on Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation ('Guideline') is issued to financial institutions by the Bank of Mauritius by virtue of powers conferred upon it under section 18(1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002, sections 64B and 100 of the Banking Act 2004, section 50(2) of the Bank of Mauritius Act 2004, sections 4(2)(e) and 17(1)(a) of the National Payment Systems Act 2018 and section 40 of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019.

2.04 This Guideline supersedes the Guidance Notes on Anti-Money Laundering and Combating the Financing of Terrorism for Financial Institutions issued by the Bank under cover of the Bank's letter dated 20 January 2017.

PURPOSE

2.05 The Guideline sets out the broad parameters within which financial institutions should operate in order to ward off money laundering, terrorist financing and proliferation financing risks.

---

[6] "banking laws" – (a) means this Act, the Bank of Mauritius Act, the Convention for the Suppression of Financing of Terrorism Act, the Financial Intelligence and Anti-Money Laundering Act, the Prevention of Terrorism Act, the Prevention of Terrorism (International Obligations) Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019; and (b) includes such other enactment as may be prescribed.

[7] "bank" is defined in the Banking Act as a company incorporated under the Companies Act, or a branch of a company incorporated abroad, which is licensed under section 7(5) of the Banking Act to carry on any of the following: banking business, Islamic banking business, private banking business.

[8] "non-bank deposit taking institution" is defined in the Banking Act as an institution other than a bank that has been authorised by the central bank to conduct deposit taking business.

[9] "cash dealer" is defined in the Banking Act as a person licensed by the central bank to carry on the business of foreign exchange dealer or money-changer. A money changer is a body corporate licensed as such under the Banking Act to carry on solely the business of (a) buying and selling of foreign currency notes, coins and travellers' cheques; (b) replacement of lost or stolen traveller's cheques; and (c) encashment under credit cards. A foreign exchange dealer is a body corporate licensed as such by the central bank to carry on the business of: (a) buying and selling foreign currency, including spot and forward exchange transactions and wholesale money market dealings; (b) a money changer; (c) money or value transfer services.

[10] "moneylender" is defined in the Banking Act as a person, other than a bank or a non-bank deposit taking institution, whose business is that of moneylending or who provides, advertises or holds himself out in any way as providing that business, whether or not he possesses or owns property or money derived from sources other than the lending of money, and whether or not he carries on the business as a principal or as an agent.

[11] Under the National Payment Systems Act, "licensee" means a person who has been issued with a licence or granted an authorisation under the Act.

Financial institutions should, on their part, maintain updated anti-money laundering and terrorist financing deterrence policies, including regular update and training of concerned staff to keep up with new emerging typologies.

2.06 The Guideline outlines the relevant requirements of the Financial Intelligence and Anti-Money Laundering Act 2002 (as amended), the Financial Intelligence and Anti-Money Laundering Regulations 2018 (as amended), Banking Act 2004 and the United Nations (Financial Prohibitions, Travel Ban and Arms Embargo) Sanctions Act 2019.

2.07 The Guideline provides guidance and assistance to financial institutions in order to assist them to understand and effectively perform their statutory obligations under the legal and regulatory framework. It sets out the minimum expectations of the Bank regarding the factors that should be taken into consideration by financial institutions when identifying, assessing and mitigating the risks of money laundering and the financing of terrorism and proliferation.

2.08 Nothing in this Guideline is intended to limit or otherwise curtail the application of any additional or supplementary guideline, instruction, directive, guidance or any other notification issued by the Bank or other competent authorities and which are applicable to financial institutions.

2.09 It is recognised that for the Guideline to be effective, they need to be reviewed on a regular basis to reflect changing circumstances and experience. Revisions and updates will be communicated to all financial institutions as and when necessary and published on the website of the Bank.

SCOPE OF APPLICATION AND STATUS

2.10 The Guideline applies to ALL financial institutions, members of their board of directors, management and employees.

2.11 The Guideline is a statement of the minimum standard expected from ALL financial institutions and are intended to be used by all their officers and staff. The Guideline provides practical guidance to assist financial institutions and their senior management in designing and implementing their own policies, procedures and controls in the relevant operational areas, taking into consideration their special circumstances, so as to meet the relevant statutory and regulatory requirements. The Guideline, however, is not intended to provide an exhaustive list of systems and controls to counter money laundering and the financing of terrorism and proliferation.

2.12 In complying with statutory requirements and in applying the provisions and requirements of the Guideline, financial institutions should as far as possible adopt an appropriate and intelligent risk based approach and always consider additional measures that could be necessary to prevent its exploitation, and that of its products and services, by persons seeking either to launder money or to finance terrorism or proliferation.

2.13 For the avoidance of doubt, where the word “shall”, “must” or “should”, or words having similar meaning, is used in the Guideline with respect to an action, provision, consideration or measure, it is a mandatory requirement and financial institutions are required to comply or implement the said action, provision, consideration or measure.

2.14 The Bank of Mauritius, in the exercise of its supervisory duties, will monitor adherence to the Guideline and failure to measure up to the standard contained in the Guideline will be dealt

with, as appropriate, by the Bank in accordance with its Sanctions Framework[12]. Regulatory actions may entail the imposition of non-monetary sanctions, monetary penalties and in very serious instances, may lead to the revocation of the licence of the financial institution. It must be emphasised that it is a criminal offence for financial institutions to fail to take measures to prevent their institutions or the services their institutions offer from being used to commit or to facilitate the commission of money laundering.

STRUCTURE OF THE GUIDELINE

2.15 This Guideline is divided into the following Chapters :

Chapter 1	Introduction
Chapter 2	Authority, purpose, scope of application and status of the Guideline
Chapter 3	Overview of the legislative framework
Chapter 4	Risk-based approach
Chapter 5	Internal Controls, policies and procedures
Chapter 6	Customer due diligence / Identification Procedures
Chapter 7	Ongoing monitoring
Chapter 8	Terrorist financing, financial sanctions and proliferation financing
Chapter 9	Reporting of Suspicious transactions
Chapter 10	Record-keeping
Chapter 11	Staff training

EFFECTIVE DATE AND TRANSITION PERIOD

2.16 The Guideline comes into effect from the date of issue. All regulated entities must conduct a gap analysis against the requirements of the Guideline and devise an implementation plan to address any gaps. This plan should be submitted to the Bank upon request.

2.17 Financial institutions will be required to conduct their 2020 AML/CFT external audits using the revised Guideline. In instances where financial institutions would not have completed their implementation plan by the 2020 audit cycle, the external audit should consider the status of the financial institution's implementation plan in its assessment.

2.18 Any enquiries pertaining to this Guideline should be addressed to :

The Second Deputy Governor
Bank of Mauritius
Sir William Newton Street
Port Louis
Tel : 202 3958
Fax : 212 6131
e-mail : sdg@bom.mu

[12] The Sanctions Framework sets out the methodology and procedures which govern the Bank's decision-making process and its approach in deciding on enforcement actions and sanctions which are proportionate and dissuasive and are effective at ensuring future compliance by the sanctioned licensee. The Framework outlines the underlying principles to be observed by the Bank when determining and applying sanctions, that is, objectivity, reasonableness, transparency, fairness and consistency and aligns the Bank's enforcement efforts, activities and resources to achieve the Bank's statutory objectives while ensuring that enforcement actions are commensurate with the severity of the wrongdoing and are applied consistently across financial institutions in similar circumstances.

3. OVERVIEW OF THE LEGISLATIVE FRAMEWORK

A. ANTI-MONEY LAUNDERING MEASURES

WHAT IS MONEY LAUNDERING?

3.01 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it allows them to maintain control over those proceeds and, ultimately provides them with a legitimate cover for the source of their income.

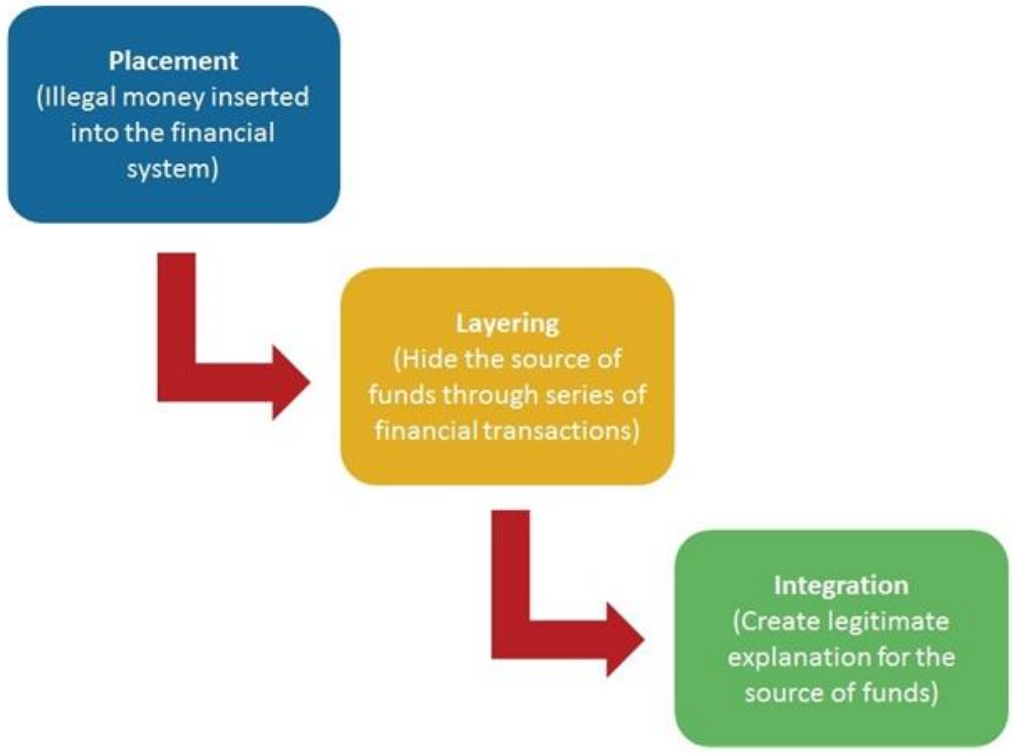
THE NEED TO COMBAT MONEY LAUNDERING

3.02 It is vital in the fight against crime that criminals be prevented from legitimising the proceeds of their criminal activities by converting funds from 'dirty' to 'clean'.

3.03 The long term success of any financial system depends on attracting and retaining legitimately earned funds. Criminally earned money is invariably transient in nature. It damages reputation and the integrity of banking systems and deters the honest depositor. Any person or institution that becomes involved in money laundering will risk possible prosecution, and the loss of his good market reputation.

STAGES OF MONEY LAUNDERING

3.04 The laundering process is generally accomplished in three stages, as follows, which may comprise numerous transactions by the launderers that could trigger suspicion on money laundering.



a) **Placement** - the physical disposal of the initial proceeds derived from illegal activity

b) **Layering** - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity

c) **Integration** - the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases or may also occur simultaneously or may overlap.

THE FATF FORTY RECOMMENDATIONS

3.05 In 1990, the FATF issued its Forty Recommendations setting out the basic framework for anti-money laundering efforts. The Forty Recommendations were first revised in 1996, then in June 2003 and again in February 2012, to take into account changes in money laundering methods, techniques and trends that have developed as counter-measures to combat this crime. The FATF Standards aim at strengthening global safeguards and further protect the integrity of the financial system. The FATF Recommendations are the basis on which all countries should meet the shared objective of tackling money laundering, terrorist financing and the financing of proliferation. The FATF has called upon all countries to effectively implement these measures in their national systems.

LEGAL FRAMEWORK

3.06 The main pieces of legislation relating to money laundering are

(i) The Financial Intelligence and Anti-Money Laundering Act 2002 (as amended);

The FIAMLA provides for the establishment of the Financial Intelligence Unit, the offences of money laundering, reporting of suspicious transactions, and sets out the preventive measures to be adopted by financial institutions amongst others.

(ii) The Financial Intelligence and Anti-Money Laundering Regulations 2018 (as amended);

The FIAML Regulations set out detailed requirements regarding the preventive measures to be adopted by financial institutions.

(iii) The Financial Intelligence and Anti-Money Laundering (Registration of Reporting Persons) Regulations 2019;

Financial Institutions, through their Money Laundering Reporting Officers, are required to register themselves with the FIU under this Regulation.

(iv) Part VIIIA of the Banking Act 2004;

A new Part VIIIA entitled “Prevention of money laundering and terrorism financing”, comprising sections 64A to 64D, has been added to the Banking Act.

Section 64A requires every financial institution and every holder of a licence, including its branches and subsidiaries, to implement programmes against money laundering and terrorism financing, which are commensurate with the money laundering and terrorism financing risks to which it or he is exposed and the size of its or his business.

Pursuant to section 64B, the Bank may, from time to time, issue such guidelines, directives or instructions to any financial institution, class of financial institutions or holder of a licence, as it considers necessary for the prevention of money laundering or terrorism financing.

Non-compliance with any guideline, directive or instruction issued by the Bank is tantamount to an offence punishable, on conviction, to a fine not exceeding one million rupees and, in the case of a continuing offence, to, after conviction, a further fine of 100,000 rupees for every day or part of a day during which the offence continues.

(v) The Prevention of Corruption Act 2002

The Prevention of Corruption Act 2002 creates an Independent Commission Against Corruption which is vested under the Act with powers to, inter alia, investigate money laundering offences.

Money Laundering Offences

3.07 Money laundering offences relate to the proceeds of crime generally.

3.08 In the interpretation section of the FIAMLA, money laundering is defined as an offence under Part II of the Act. Under Part II of the FIAML, the following offences are money laundering offences -

"3. Money laundering

(1) Any person who -

(a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or

(b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.

(2) A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.*

(3) Reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include

concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

[* as defined in the FIAMLA]

4. Conspiracy to commit the offence of money laundering

Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence.

3.09 The term 'crime' as defined in the Act

(a) means an offence punishable by -
  (i) penal servitude;
  (ii) imprisonment for a term exceeding 10 days;
  (iii) a fine exceeding 5,000 rupees;

(b) includes an activity carried on outside Mauritius and which, had it taken place in Mauritius, would have constituted a crime; and

(c) includes an act or omission which occurred outside Mauritius but which, had it taken place in Mauritius, would have constituted a crime.

LIMITATION ON PAYMENT IN CASH AND EXEMPT TRANSACTIONS

Limitation on Payment in Cash

3.10 Section 5 of the FIAMLA imposes a limitation on payment in cash. This limitation was designed and meant to provide an effective remedy to respond to a pressing need in the public interest to combat money-laundering[13]. It also aims at securing an audit trail and acts as a preventive measure against the laundering of the proceeds of crime. Accordingly, apart from certain exempt transactions, described below, transactions in cash in excess of 500,000 rupees are prohibited altogether.

Exempt Transactions

3.11 Exempt transactions are transactions for which the limit of 500,000 rupees does not apply and are generally transactions between

(i) the Bank of Mauritius and any other person,
(ii) a bank and another bank,
(iii) a bank and a financial institution*,
(iv) a bank or a financial institution* and a customer, where
  (a) the transaction does not exceed an amount that is commensurate with the lawful activities of the customer, and
    1) the customer is, at the time the transaction takes place, an established customer of the bank or financial institution; and
    2) the transaction consists of a deposit into, or withdrawal from, an account of a customer with the bank or financial institution; or

[13] L.A Abongo versus The State [2009 SCJ 81]

b) the chief executive officer or chief operating officer of the bank or financial institution, as the case may be, personally approves the transaction in accordance with any guidelines, instructions or rules issued by a supervisory authority in relation to exempt transactions; or

(v) between such other persons as may be prescribed.

*[*has the same meaning as in the FIAMLA]*

3.12 The Intermediate Court has jurisdiction to try any offence under the FIAMLA or regulations made thereunder and may, on conviction, impose any penalty including forfeiture. The Court may, on conviction, impose a fine not exceeding 10 million rupees and penal servitude for a term not exceeding 20 years. Any property belonging to or in the possession or under the control of, any person who is convicted of a money laundering offence is deemed, unless the contrary is proved, to be derived from a crime and the Court may order its forfeiture.

B. TERRORIST FINANCING

3.13 The main pieces of legislation relating to terrorist financing are –

(i) the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019;
(ii) The Convention for the Suppression of the Financing of Terrorism Act;
(iii) The Prevention of Terrorism Act 2002; and
(iv) The Financial Intelligence and Anti-Money Laundering Act 2002.

3.14 'financing of terrorism' is defined under the UN Sanctions Act as the financing of terrorists, terrorist acts and terrorist organisations.

3.15 Terrorist financing, while an offence in itself, is also a predicate offence for money laundering.

3.16 Financial institutions should, therefore, protect themselves from being used as a conduit for such activities and make use of their already existing due diligence requirements, along with current policies and procedures on money laundering and enhance them where necessary to detect transactions that may involve terrorist funds. Financial institutions should review their practices in this area as part of their general internal and external audit processes.

3.17 The NRA Report 2019 identified the overall TF risk in Mauritius as Medium given that the TF threat was rated as Medium-Low and TF vulnerability as Medium-High. Financial institutions are encouraged to consider the risks identified by the FATF in its Reports and other documents, when reviewing their policies and procedures and due diligence requirements. They should pay special attention to the terrorist financing methods and techniques identified in these Reports and document and enhance their systems and controls accordingly.

C. PROLIFERATION FINANCING

3.18 The main pieces of legislation relating to Proliferation financing are –

(i) the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019;
(ii) The Financial Intelligence and Anti-Money Laundering Act 2002.

3.19 'Proliferation' and 'Proliferation financing' have been defined in the FIAMLA as follows:

"proliferation" means –

(a) the manufacture, production, possession, acquisition, stockpiling, storage, development, transportation, sale, supply, transfer, import, export, transshipment or use of –

(i) nuclear weapons;
(ii) chemical weapons;
(iii) biological weapons;
(iv) such other materials, as may be prescribed, which are related to nuclear weapons, chemical weapons or biological weapons; or

(b) the provision of technical training, advice, service, brokering or assistance related to any of the activities specified in paragraph (a);

"proliferation financing", in relation to a person, means the person who –

(a) makes available an asset;
(b) provides a financial service; or
(c) conducts a financial transaction; and

knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended to, in whole or in part, facilitate proliferation regardless of whether the specified activity occurs or is attempted;

3.20 The issue of proliferation received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation In 2004, the UN Security Council issued Resolution 1540, requiring states to put in place a number of measures in order to prevent the proliferation of nuclear, chemical or biological weapons. Subsequently, the FATF started in 2007 to consider the threats related to proliferation financing and its interconnection with terrorism and terrorism financing.

3.21 The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing.

3.22 Such measures are included in Recommendation 7 of the revised 2012 FATF Recommendations. It requires countries to put in place to implement the United Nations Security Council ("UNSC") Resolutions concerning the prevention, suppression and disruption of proliferation of WMD and its financing.

3.23 The UNSC Resolutions have designated certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSC Resolutions may be found on the UN website[14].

3.24 The financial prohibitions and other sanctions under the UN Sanctions Act apply to any person so designated.

14 https://www.un.org/sc/suborg/en/s/res/1737-(2006) and https://www.un.org/sc/suborg/en/sanctions/1718.

4. RISK BASED APPROACH

INTRODUCTION

4.1 Financial institutions are required to apply a risk-based approach to the implementation of the AML/CFT regime.

4.2 A risk-based approach is a process that allows financial institutions to identify, assess and understand the money laundering and terrorist financing risks to which they are exposed and develop strategies including AML/CFT measures commensurate with those risks in order to manage and mitigate them in an effective and proportionate manner.

4.3 The principle of risk-based approach allows financial institutions to allocate their resources more effectively and apply preventive measures that are commensurate with the nature and level of risks, in order to focus their AML/CFT efforts in the most effective way.

4.4 The approach to the management of risk and risk-mitigation requires the leadership and engagement of senior management towards the detection and deterrence of money laundering and terrorist financing. Senior management is ultimately responsible for making management decisions related to policies, procedures and processes that mitigate and control the risks of money laundering and terrorist financing within a business.

4.5 The scope of applied measures for prevention and detection of money laundering and terrorist financing should be proportional to the identified money laundering and terrorist financing risk degree (risk-based approach).

STATUTORY REQUIREMENTS

Financial Intelligence and Anti Money Laundering Act

4.6 Section 17(1) of the FIAMLA requires financial institutions to –

(a) take appropriate steps to identify, assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions or delivery channels; and

(b) consider all relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied.

4.7 Section 17(2) of the FIAMLA specifies that the nature and extent of any assessment of money laundering and terrorism financing risks under section 17(1) must be appropriate having regard to the nature and size of the business of the financial institution and must take into account –

(a) all relevant risk factors including –

(i) the nature, scale and complexity of the financial institution's activities;
(ii) the products and services provided by the financial institution;
(iii) the persons to whom and the manner in which the products and services are provided;
(iv) the nature, scale, complexity and location of the customer's activities;
(v) reliance on third parties for elements of the customer due diligence process; and
(vi) technological developments; and

(b) the outcome of any risk assessment carried out at a national level and any guidance issued.

4.8 Section 17(3) of the FIAMLA requires financial institutions, prior to the launch of a new product or business practice or the use of a new or developing technology, to identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices, or new or developing technologies for both new and pre-existing products, and take appropriate measures to manage and mitigate these risks.

4.9 Financial institutions must, in terms of section 17(4) of the FIAMLA document the risk assessments in writing, keep it up to date and, on request, make it available to relevant competent authorities without delay.

4.10 Pursuant to section 17A of the FIAMLA, financial institutions are required to establish policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the financial institution. Financial institutions must monitor the implementation of, regularly review, update and where necessary, enhance the policies, controls and procedures.

4.11 Financial institutions are required under section 17C(3) of the FIAMLA, where the risks are higher, to conduct enhanced due diligence measures consistent with the risks identified and may pursuant to section 17C(4), conduct simplified due diligence measures where risks are lower, unless there is a suspicion of money laundering or terrorism financing in which case enhanced CDD measures shall be undertaken.

4.12 The Ministry of Financial Services and Good Governance (Ministry) is mandated In terms of section 19D(2) of FIAMLA, to conduct an assessment of the risks of money laundering and terrorist financing affecting the domestic market and relating to cross border activities and shall in particular, identify –

(a) the areas of the domestic market that are of greatest risk;

(b) the risk associated with each segment of the financial services sector and the sector relating to members of a relevant profession or occupation;

(c) the most widespread means used by criminals to launder illicit proceeds;

(d) the features and types of non-profit organisations which are likely to be at risk for terrorism financing abuse.

4.13 The Ministry shall, to the extent possible, make available the findings of the national risk assessment to financial institutions, in order to assist them to identify, understand, manage and mitigate the risk of money laundering and terrorism financing and proliferation.

4.14 Section 19D(4) of the FIAMLA requires the Bank of Mauritius to use the findings of their risk assessment to, inter alia, assist in the allocation and prioritisation of resources to combat money laundering and terrorism financing and ensure that appropriate measures are put in place to mitigate the risks of money laundering and terrorism financing.

Financial Intelligence and Anti-Money Laundering Regulations

4.15 Pursuant to Regulation 11(1), a financial institution may apply simplified CDD measures where lower risks have been identified. The simplified CDD measures must be commensurate with the lower risk factors and in accordance with any guidelines issued by the Bank.

4.16 Regulation 11(2) further stipulates that, where a financial institution determines that there is a low level of risk, it must ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment conducted by the Bank of Mauritius, whichever is most recently issued.

4.17 However, as per Regulation 11(3), simplified CDD shall not apply where a financial institution knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

4.18 Regulation 12(1), on the other hand, requires financial institutions to perform enhanced CDD –

(a) where a higher risk of money laundering or terrorist financing has been identified;

(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;

(c) where a customer or an applicant for business is from a high risk third country;

(d) in relation to correspondent banking relationships;

(e) where the customer or the applicant for business is a political exposed person;

(f) where a financial institution discovers that a customer has provided false or stolen identification documentation or information and the financial institution proposes to continue to deal with that customer;

(g) in the event of any unusual or suspicious activity.

4.17 In addition, Regulation 12(5) prescribes that, where a financial institution determines that the beneficiary who is a legal person or a legal arrangement presents a higher risk, it must take enhanced due diligence measures which shall include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary at the time of payout.

GENERAL GUIDANCE

RISK ASSESSMENTS

NATIONAL RISK ASSESSMENT

4.19 Mauritius completed its first National Risk Assessment (NRA) in August 2019[15]. The NRA identified the most significant money laundering and terrorism financing threats, vulnerabilities, and risks that different sectors in Mauritius face[16], and makes an assessment of the overall national money laundering and terrorism financing risk that the country faces.

4.20 Based on the NRA, customers posing high threat of money laundering include high net worth individuals, non-residents and politically exposed persons for banking institutions; and walk-in and one-off customers for other financial institutions licensed by the Bank of Mauritius.

4.21 Examples of products/services/delivery channels provided by banking institutions which are vulnerable to money laundering include: services to Global Business Companies (GBCs), safe deposit box services, money or value transfer services, internet banking, and prepaid cards. Examples of products/services/delivery channels provided by other financial institutions which are vulnerable to money laundering include: deposit services provided by NBTIs and foreign currency exchange services.

INSTITUTIONAL RISK ASSESSMENT

4.22 The key purpose of an Institutional Risk Assessment (IRA) or enterprise wide ML/TF risk assessment (EWRA) is to improve the effectiveness of ML/TF risk assessment management through the identification of the general and specific ML/TF risks to which a financial institution is exposed, determination of how these risks are mitigated by the controls embedded in the financial institution's AML/CFT programmes and establishing the residual risk that remains for the financial institution.

4.23 Thus, an effective enterprise wide risk assessment can allow financial institutions to identify gaps and opportunities for improvement in their framework of internal AML/CFT policies, procedures and controls, as well as to make informed management decisions about risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are appropriately aligned with residual risks.

4.24 Financial institutions should decide on both the frequency and methodology of enterprise-level ML/FT risk assessments, including baseline and follow-up assessments, that are appropriate to their particular circumstances, taking into consideration the nature of the inherent and residual ML/FT risks to which they are exposed, as well as the results of the NRA. In most cases, financial institutions should consider performing such risk assessments annually; however, assessments that are more frequent or less frequent may be justified, depending on the particular circumstances. They should also decide on policies and procedures related to the periodic review of their enterprise wide risk assessment methodology, taking into consideration changes in internal or external factors. These decisions should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

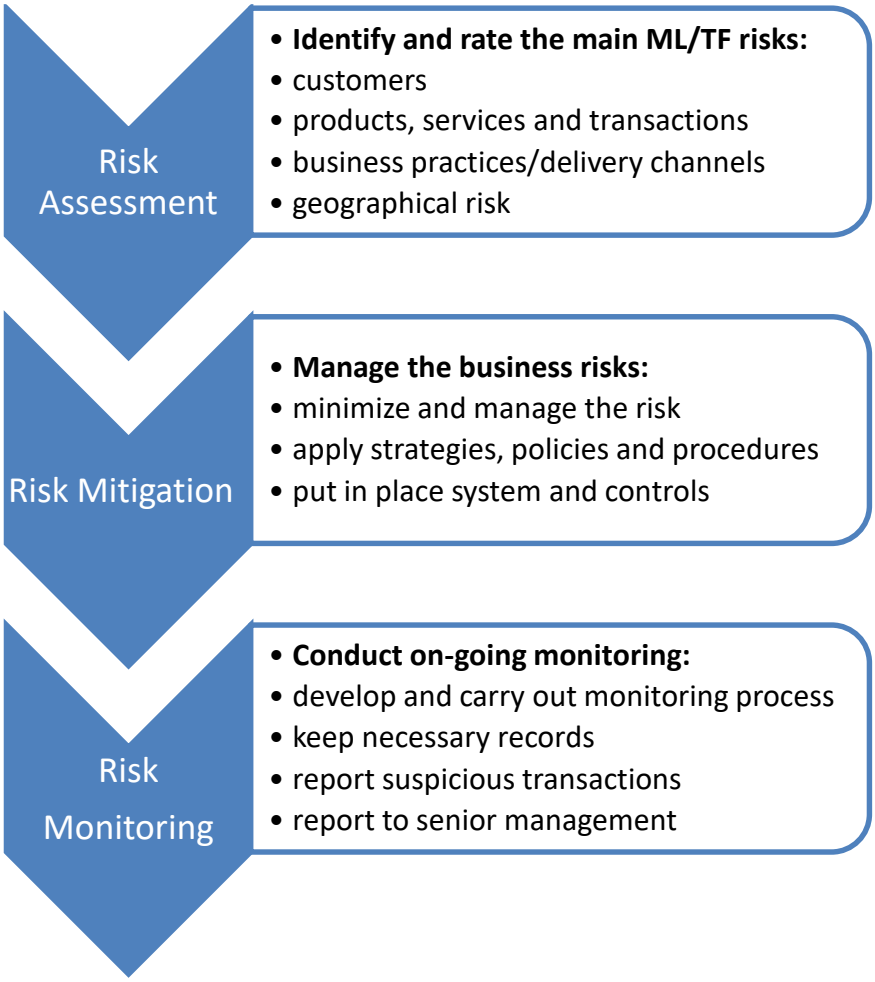
4.25 The following diagram depicts visually the three different steps in implementing a risk-based approach, that is, risk assessment, risk mitigation and risk monitoring.

---

[15] The NRA Report was disseminated in August 2019 and is available at http://financialservices.govmu.org/English/Documents/2019/NRA Report/Public Report 2019-compressed.pdf.

[16] These sectors include the banking sector; the securities sector; insurance sector; the other Non-Bank Financial Institutions (NBFIs); the global business sector; and Designated Non–Financial Businesses and Professions (DNFBP).

Diagram 1: Risk-based Approach



4.26 The first step in a risk-based approach is to conduct a risk assessment, that is, an analysis of potential threats and vulnerabilities to ML/TF to which the financial institution's business is exposed. The assessment should be commensurate with the nature, size and complexity of the financial institution's business.

4.27 When conducting their risk assessment, financial institutions should identify and assess the ML/TF risks in the following categories:

- customers;
- products, services and transactions;
- business practices/delivery channels; and
- geography.

Customer risk

4.28 Financial institutions have to consider the nature and business of their clients to determine the level of risk of ML/TF. In other words, financial institutions have to know their clients to perform a risk assessment. Knowing clients is not limited to identification or record keeping requirements. It is about understanding clients, including their activities, transaction patterns,

how they operate, etc. Other elements, such as the magnitude of a client's assets or the number of transactions involved, might also be relevant.

Financial institutions should adopt a risk-based approach in the conduct of their risk assessment of their customers. This approach may involve the grouping of customers by category, based on the nature of their business, for the conduct of a risk assessment for clusters of customers. The rationale for such risk assessment should be documented with the criteria used for customer segmentation and the allocation of a risk level for each group of customers clearly defined.

4.29 As per the NRA Report 2019, the type of customer segments that pose higher ML/TF include High Net Worth Individuals (HNWIs), corporates with complex structures, GBCs and trusts (especially those involving non face-to-face or introduced business), Politically Exposed Persons (PEPs), walk-in customers and one-off customers.

Products, services and transaction risk

4.30 Financial institutions should be aware of and be able to identify products, services and transactions that may pose higher ML/TF risks. Legitimate products and services can be used to mask illegal origins of funds, to move funds to finance terrorist acts or to hide the true identity of the actual owner or beneficiary of the product, service or transactions. Products, services and transactions that can support the movement and conversion of assets into, through and out of the financial system may pose a high risk. In addition, products and services assessed in the National Risk Assessment, by the Bank, national authorities or other credible sources as being potentially high risk for money laundering or terrorist financing should be considered.

4.31 Products/services/transactions highlighted as having higher money laundering vulnerability in the NRA Report 2019 include deposits (especially deposit accounts of domestic legal persons, non-domestic legal persons and GBCs), private banking (involving HNWIs, high volume of deposits and transactions and non face-to-face clients), safe deposit box services, trade finance, internet banking transactions, foreign currency exchange services, money or value transfer services and prepaid cards[17]

4.32 Different activities conducted by financial institutions will face different risks related to the characteristics of these activities. Box 4.1 outlines some of ML/TF risks associated with different banking activities.

Box 4.1. Examples of ML/TF risk associated with different banking activities

- **Retail banking**: provision of services to cash-intensive businesses, volume of transactions, high-value transactions, diversity of services.
- **Wealth management:** culture of confidentiality, difficulty to identify beneficial owners, concealment (use of offshore trusts), banking secrecy, complexity of financial services and products, PEPs, high value transactions, multiple jurisdictions.
- **Investment banking:** layering and integration, transfer of assets between parties in exchange for cash or other assets, global nature of markets.

[17] Risk mitigation measures for prepaid cards should be aligned with the *FATF Guidance for a Risk-Based Approach – The Banking Sector*, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf , and the *Wolfsberg Guidance on Prepaid and Stored Value Card*, available at https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/11.%20Wolfsberg_Guidance_on_Prepaid_and_Stored_Value_Cards_Oct_14%2C_2011.pdf.

- **Correspondent banking:** high value transactions, limited information about the remitter and source of funds especially when executing transactions with a bank located in a jurisdiction that does not comply or complies insufficiently with FATF Recommendations, the possibility that PEPs are involved in the ownership of a bank.

Business practices/delivery channels risk

4.33 Financial institutions are also required to 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 financial institution (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 ML/TF risks.

Geographical risk

4.34 Financial institutions have to consider whether geographic locations in which they operate or undertake activities pose a potentially higher risk for money laundering and terrorist financing.

4.35 **Annex 1 of this Chapter** (Annex 1) provides a list of higher risk situations in the above categories. Where the financial institution has identified a customer or situation as having higher ML/TF risk, it should apply appropriate risk mitigations measures and enhanced due diligence. The financial institution is not required to refuse the transaction or end the business relationship.

Variables that can have an impact on the risk

4.36 Financial institutions should take into account the peculiarities, the risk degree or suspiciousness of a transaction or business relationship. Therefore, the risk assessment procedure shall cover the variable risks which are specific for a certain client or a type of business as these will impact the appropriate level of CDD measures.

4.37 The following are variables which can have an impact on increasing or decreasing of the potential risk posed by certain client or type of business:

- The nature, scale, diversity and complexity of their business;
- Their target markets;
- The internal audit and regulatory findings;
- The existing legislative framework or the existence of the supervision by competent bodies. For example, clients who are subject to a satisfactory system of money laundering and financing of terrorism prevention represent a lower risk than clients from the industry where there is a risk of money laundering because they are not regulated for the purpose of preventing these activities;
- Reputation and publicly available information on the client. Legal persons which are transparent and well known in the public domain and which are in operation for many years without criminal convictions being delivered against them (represent a lower risk of money laundering;
- Duration of a business relationship;
- Knowledge of the client's country including the knowledge of local laws, regulations and rules, as well as the structure and scope of a regulatory supervision;
- Proportionality between the size or scope and longevity of client's doing business including the nature of the requested service;
- Risks resulting from the use of new technology which enables a business relationship without the client's presence (non-face-to-face) and which favours anonymity;
- Structure of a corporate/entity or structure of a transaction;

- Structures without visible legal, tax, business, economic or other legislative purpose may increase the risks.

Higher Risk Situations

4.38 FIAML Regulation 12 prescribes enhanced CDD in the following situations:

- where a higher risk of money laundering or terrorist financing has been identified;
- where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
- where a customer or an applicant for business is from a high risk third country;
- in relation to correspondent banking relationships;
- where the customer or the applicant for business is a political exposed person;
- where a financial institution discovers that a customer has provided false or stolen identification documentation or information and the financial institution proposes to continue to deal with that customer;
- in the event of any unusual or suspicious activity.

4.39 With respect to new technologies, the financial institution should use the same methodology to evaluate the risk associated with new technologies as with other products/services and transactions. The risk assessment should examine the client, delivery channel and geographic risk associated with the new technology and be conducted prior to the launch or use of the product or service.

4.40 When dealing with clients who are engaged in the provision of money or value transfer services (MVTS) (including virtual currencies), the financial institution should determine the risks related to the service provider's client base, the types of product, service and transactions it provides, geographical risk factors as well as the type of delivery channel used.

4.41 If it is determined that the activities of the MVTS service provider are higher risk the financial institution should implement appropriate mitigation measures such as those listed at **Annex 2 of this Chapter**. The financial institution may also want to inquire on the risk mitigation measures that are being applied by the MVTS service provider to ascertain whether ML/TF risks are being adequately monitored and controlled. It is the decision of the financial institution, based on its risk tolerance or appetite, to determine whether it wants to establish or pursue a business relationship with any client, including money or value transfer services.

4.42 Financial institutions should also consider any higher risk identified in other relevant risk assessments which may be issued from time to time such as the National Risk Assessment for ML/TF risks and other sectoral risk assessment made by the authorities.

Lower Risk Situations

4.43 FIAML Regulations allow a financial institution to apply simplified CDD measures where lower risks have been identified. Where a financial institution determines that there is a low level of risk, it must ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment of the Bank of Mauritius. The simplified CDD measures must be commensurate with lower risk factors and in accordance with guidance issued by the Bank. Furthermore, simplified CDD measures shall not apply where there is a suspicion of ML/TF.

4.44 Simplified measures can include obtaining less information (e.g., not requiring information on the address or the occupation of the potential client), and/or seeking less robust verification, of the customer's identity and the purpose and intended nature of the business relationship or postponing the verification of the customer's identity.

4.45 While the legislative framework allows for the application of simplified CDD measures in low risk scenarios, it must be highlighted that the NRA Report 2019 has not identified any low risk sectors. As such, the application of simplified CDD measures does not arise in the current risk environment.

Characteristics of a comprehensive ML/TF Risk Assessment

4.46 The following criteria outline the characteristics of a robust risk assessment. The Bank will use these characteristics to determine whether the financial institutions have adequately implemented their statutory obligations to implement a risk assessment.

4.47 *The risk assessment is documented* - It is important that the risk assessment developed by the financial institution is documented. This allows the risk assessment strategies to be shared with management and employees.

4.48 *The risk assessment is proportionate* - Due regard must be accorded to the vast and profound differences in practices, size, scale and expertise, amongst financial institutions. As a result, consideration must be given to these factors when evaluating a financial institution's risk assessment and mitigation strategies. The risk assessment can take different forms depending on the size and operations of the financial institution. A checklist may be appropriate for a small firm but a more comprehensive document including a risk matrix may be appropriate for larger entities.

4.49 *The risk assessment should take into account key risk elements* - An entity's risk assessment should be comprised, at a minimum, of the following elements:

4.50 Customer risk – The financial institution should consider the nature and business of its customers and their business relationships to determine the level of ML/FT risk associated with each type of customer or business relationship. I. Examples of customer risk are included in Annex 1.

4.51 Product/services/transactions - An overall risk assessment should include determining the potential risks associated with the products and services offered by the financial institution noting that various financial institutions provide a broad and diverse range of products and services. The context of the products/services being offered is always fundamental to a risk-based approach. Examples of product/service/transactions risk are included in Annex 1.

4.52 Business practices/delivery channels – The financial institution should consider the channels used to deliver their products and services. Many delivery channels do not bring the customer into direct face to face contact with the customer. Attention should be paid to the remoteness of distribution channels as they can also be used to obscure the true identity of a client or beneficial owners. Examples of business practices/delivery channels risk are included in Annex 1.

4.53 Geographical risk – The financial institution should consider whether the geographic locations in which it operates, undertakes activities or where a client is located poses a potentially higher risk for ML/FT. Examples of geographical risk are included in Annex 1.

4.54 *A risk assessment is conducted for new products, business practice or technology*. The risk assessment should be conducted prior to the introduction of the new product, new business practice or new technology for both new and pre-existing products. The assessment is documented and availed to the FIU or supervisory authority upon request.

4.55 *The risk assessment is approved by senior management*. – Strong senior management leadership and engagement in AML/CFT is an important aspect of the application of the risk-based

approach. The senior management should approve the risk assessment and have a strong understanding of AML/CFT risks affecting the financial institution.

4.56 *The risk assessment is shared with employees.* - For a risk management framework to be effective employees need to be aware of those situations that have been identified as high risk.

4.57 *The financial institution has appropriate mechanisms to provide risk assessment information to competent authorities.* The financial institution should establish mechanism to make available not only the documented AML/CFT risk assessment but also risk assessment information on customers, products/services/transactions, delivery channels and geography related to its operations.

Risk mitigation

4.58 Risk mitigation is about implementing measures to limit the potential money laundering and terrorist financing risks the financial institution has identified while staying within its risk tolerance or appetite level. As part of its internal controls, when the risk assessment determines that risks are high for ML or FT, the financial institution 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.

Characteristics of a comprehensive risk mitigation

4.59 The following are characteristics of a comprehensive risk mitigation program.

4.60 *Policies, controls and procedures approved by senior management manage and mitigate the risks that have been identified.* The results of the AML/CFT risk assessment should be reflected in the drafting of AML/CFT policies, procedures and control. Procedures and controls should be drafted with the specific intent of reducing ML/TF risks that have been identified.

4.61 *The risk mitigation strategies to reduce the ML/TF risks are documented* - It is important that the risk mitigation strategies are developed by the financial institution 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.

4.62 *The risk mitigation strategies are shared with management and employees*. - This will allow employees to apply risk mitigation measures established by senior management.

Risk monitoring

4.63 In addition to risk assessment and risk mitigation activities, financial institutions are also required 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 to the ML/TF risks as outlined in the entity's risk assessment.

4.64 Ongoing monitoring means the scrutiny of transactions to determine whether those transactions are consistent with the financial institution's knowledge of the customer and the nature and purpose of the product and the business relationship.[18] Monitoring also involves identifying changes to the customer profile (for example, their behaviour, use of products and the amount

[18] *Guidance for a Risk-Based Approach – The Banking Sector,* Financial Action Task Force, October 2014. http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

of money involved), and keeping it up to date, which may require the application of new, or additional, CDD measures. Monitoring transactions is an essential component in identifying transactions that are potentially suspicious.

4.65 When establishing automated systems, it is important that the financial institution understands their operating rules, verify their integrity on a regular basis and check that they adequately address the identified ML/TF risk.

Box 4.2. Examples of monitoring in high/lower risk situations[19]

Monitoring in high risk situations: daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds, establishment of red flags based on typologies reports, reporting of monitoring results to senior management, etc.

Monitoring in lower risk situations: thresholds, low frequency, automated systems.

4.66 The financial institution's policies, controls and procedures has to determine what kind of monitoring is done for particular high-risk situations, including the detection of suspicious transactions. The policies, controls and procedures should also describe when monitoring is done (its frequency), how it is reviewed, and how it will be consistently applied.

4.67 In addition, senior management should monitor the effectiveness of AML/CFT risk controls and make necessary changes where applicable. This includes a documented review of the AML/CFT risk assessment and corresponding with mitigation and regular reporting to senior management.

Characteristics of a comprehensive risk monitoring

4.68 The following are characteristics of a comprehensive risk monitoring program

4.69 *Senior management should receive periodic reports on the implementation of AML/CFT risk controls and enhance them if necessary.* Senior management should receive at a minimum quarterly reports on the effectiveness of AML/CFT controls including the identification of breaches with established policies and procedures as well as areas of emerging risk. Senior management should also examine where AML/CFT procedures and controls could be enhanced.

4.70 *The risk assessment and risk mitigation strategies are reviewed by senior management*. Senior management should ensure that the risk assessment and corresponding risk mitigation strategies are reviewed at least once every two years taking into account changes such as the entry of the institution into new markets, and the introduction of new products and services.

4.71 *Business relationships are monitored.* On-going monitoring is conducted in a risk sensitive basis with higher risk situation and these are monitored more frequently. More specifically, financial institutions shall monitor on an ongoing basis all complex, unusual, suspicious or large transactions whether completed or not as well as transactions which have no apparent economic or lawful purpose.

4.72 *Monitoring activities take into account the purpose of the business relationships and the intended source of funds*. When conducting on-going monitoring, the financial institution should refer to purpose of the business relationship and intended source of funds that was documented

[19] *Idem*

at the beginning of the business relationship to ensure that activities correspond to what was stated by the client.

4.73 *Unjustified or abnormal changes in the activities of your client are documented* – The financial institution should flag changes in activities that is contrary to normal transaction patterns or client activities. A process is in place to elevate concerns as necessary.

4.74 *Monitoring parameters are established* – Financial institutions should set business limits or indicators regarding transactions that would trigger early warning signals and require mandatory review. These indicators should be informed by the ML/TF risks of your business. Operational documents demonstrate that the policy is effectively applied.

4.75 *High risk transactions or relationships are monitored more frequently* – Reporting institutions review high risk transactions more frequently against suspicious transaction indicators relevant to the relationship and escalate them should additional indicators be detected.

4.76 *Suspicious transactions are reported to the FIU* – The purpose of on-going monitoring activities is to identify suspicious transactions. Transactions that are identified by entities as being suspicious during monitoring activities should be reported to the FIU. Although a strictly quantitative analysis of the number of STRs reported would not be appropriate given the varying levels of ML/FT risk in each financial institution sector, the number of suspicious transactions detected can potentially be an indicator of an effective monitoring program.

4.77 *Complex and unusual transactions are identified.* Financial institutions should pay special attention to all complex and unusually large transactions, as well as to each unusual form of transaction without apparent economic or visible lawful purpose even in instances when reasons for suspicion of money laundering or terrorist financing have not yet been detected in relation to such transactions.

4.78 *Analysis of background and purpose of transaction is documented.* Also, financial institutions should analyze the background and purpose of complex and unusually large transactions, and make a written record of the result of the analysis.

ANNEX 1 – HIGHER RISK SITUATIONS[20]

Higher Risk Situations Related To Customer Risk May Include:

- Politically exposed persons
- Foreign legal persons that do not perform nor are allowed to perform trading activity in the country they have been registered in trusts
- Charitable or other non-profit organizations, which do not have an organized supervision of its doing business by competent supervisory bodies or structural supervision bodies (particularly those that often work cross-border)
- Clients that perform transactions in unusual circumstances (For example, significant and unexplainable geographic distance between the headquarters of the customer and the financial institution
- Clients with complex organizational structure or nature which makes the determination of a beneficial owner difficult
- Clients where you suspect they are acting for a third party
- Clients for which there are indications that they perform suspicious transactions.
- Clients with intensive cash operations
- Clients dealing with money operations
- Clients whose activity is not cash-intensive, but some transactions are performed by using larger cash amounts
- Clients establishing a business relationship through an accountant or tax adviser or a person carrying out an activity on the client's behalf
- Clients using financial intermediaries, financial institutions or lawyers who are not subject to the application of measures for preventing money laundering and financing of terrorism and are not adequately supervised by competent bodies or professional associations
- Clients who do not have an address or who have several addresses without justified reason
- Client who use legal persons or arrangements without visible legal, business or economic reason
- Persons appearing on the terrorist or criminal list
- International clients from high risk jurisdictions
- Intermediaries, such as lawyers and accountants
- Intermediary structures, such as holding companies, legal arrangements numbered companies that have no apparent business purpose
- Clients whose nationality/residence/location of employment is associated with a country on a prohibited country list or a high-risk country list
- Cash and cash equivalent intensive businesses, such as: casinos, MSBs, foreign exchange business, etc.
- Non face-to-face customer, where doubts exist about the identity of such customer
- Customer who uses agents or associates where the nature of the relationship or transaction(s) makes it difficult to identify the beneficial owner of the funds
- Customer knows little or is reluctant to disclose details about the payee of a wire transfer (address/contact info, etc.)
- Consumer gives inconsistent information (e.g. provides different names)
- Customer involved in the transactions that have no apparent ties to the destination country and with no reasonable explanations
- Customer who offers false/fraudulent identification, whether evident from the document alone, from the document's lack of connection to the customer, or from the document's context with other documents (e.g. use of identification cards or documents in different names without reasonable explanation)

[20] Higher risk situations are derived, *inter alia*, from the FATF Risk Based Approach Guidance for Banks (October 2014) http://www.fatf-gafi.org/publications/fatfrecommendations/documents/risk-based-approach-banking-sector.html and Money or Value Transfer Services (February 2016) http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf.

- Customer whose transactions and activities indicate connection with potential criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities (e.g. FIU, law enforcement etc.)
- Customer whose transaction patterns appear consistent with generation of criminal proceeds; e.g. illegal drug growing season, drug trafficking, illegal immigration and human trafficking, corruption etc.; based on information available with the MVTS provider

Higher Risk Situations Related To Products, Services and Transactions Risk May Include:

- Deposit taking, especially cash, and insurance products that allow large one-time or regular payments or deposits, to be made and subsequently withdrawn
- Credit accounts where large credit balances are allowed to be maintained
- Wire transfers
- Trade finance services
- Private banking
- "Free look" or "cooling off" periods coupled with premium refunds,
- Payable through accounts
- Internet banking
- Sale of stored value cards
- Products or services that may inherently favour anonymity
- Products that can readily cross international borders, such as cash, online money transfers stored value cards, money orders and international money transfers by mobile phone
- Products or services that have a very high or no transaction limit
- The global reach of the product or service offered
- The complexity of the product or service offered
- Products or services that permit the exchange of cash for a negotiable instrument, such as a stored value card or money order
- Services which deliberately offer more anonymity or depend on more anonymity of a client or participants than it is usual considering the circumstances and an attorney at law earlier experience
- Services of illegal concealing of beneficial ownership from competent bodies
- Transactions intended for persons with a domicile or headquarters in a country which is known as a financial or tax oasis (offshore financial centre)
- Transactions intended for non-profit organizations having headquarters in a country known as an offshore financial centre
- Credit accounts in respect of which large credit balances are allowed to be maintained, for example, some credit and corporate card products
- Payable through accounts that permit clients of a foreign correspondent bank to draw drafts (or cheques) on Mauritian-based accounts
- Pouch services and similar international commercial payment services.
- Trade finance services where:
  - the financial institution is not able to assess whether the values of goods or services being imported or exported are reasonable; or
  - financial institutions confirm, advise or make payments under letters of credit for purposes of their clients' buying or selling goods internationally.

High Risk Situations Related To Business Relationship/Delivery Channels
Risk May Include:

Business relationships

- Business relationships involving complicated financial transactions
- Business relationships involving payments towards/from third persons and cross-border payments
- Intermediary structures, such as holding companies, numbered companies or trusts, that have no apparent business purpose or that make beneficial owners difficult to identify
- Accountants, lawyers or other professionals holding commingled funds accounts where the beneficial ownership of the funds may be difficult to verify
- Use of the financial institution's products or services by clients of clients, for example, clients of correspondent banks.

Delivery Channels

- Channels that supports high transaction volumes, high speed movement of funds
- Use of intermediaries or introducers e.g. mortgage and deposit agents
- Non-face-to-face delivery channels such as internet, telephone and mail when used as a complete substitute for face to face interaction with the client
- Products offered through the use of agents

Higher risks specific to money or value transfer services

- Agents representing more than one MVTS provider
- Agents located in a higher-risk jurisdiction/country or serving high-risk customers or transactions
- Agents conducting an unusually high number of transactions with another agent location particularly with an agent in a high risk geographic area or corridor customers or transactions.
- The transaction volume of the agent is inconsistent with either overall or relative to typical past transaction volume
- Transaction pattern indicating value of transactions just beneath any applicable CDD threshold
- Agents that have been the subject of negative attention from credible media or law enforcement sanctions
- Agents that have failed to attend or complete the training programs
- Agents that operate sub-standard compliance programs, i.e. programs that do not effectively manage compliance with internal policies, monetary limits, external regulation, etc.
- Agents with a history of regulatory non-compliance and that are unwilling to follow compliance program review recommendations, and therefore subject to probation, suspension or termination
- Agents who fail to provide required originator information upon request
- Agents whose data collection or record keeping is lax, sloppy or inconsistent
- Agents willing to accept false identification or identification records that contain false information, non-existent addresses that would be known to be non-existent to a person in that area, or phone numbers that are used as fillers
- Agents with a send-to-receive ratio that is not balanced, consistent with other agents in the locale, or whose transactions and activities indicate potential complicity in criminal activity.
- Agents whose seasonal business fluctuation is not consistent with their incomes or with other agents in the locale or is consistent with patterns of criminal proceeds
- Agents whose ratio of questionable or anomalous customers to customers who are not in such groups is out of the norm for comparable locations

High Risk Situations Related To Geographical Risk May Include:

- A country against which the United Nations or other international institutions have imposed sanctions, embargo or other similar measures
- A country which is known, based on the knowledge of relevant international organizations. for a high degree of organized criminal, particularly corruption, arms trade, trafficking in human beings or for breaching human rights, production or organized and developed drug trade
- A country which, according to the data of the international organization FATF or a FATF-style regional body, pertains to non-cooperative countries or territories or if it is about an offshore financial centre
- Countries which are estimated by relevant international organizations as countries lacking the appropriate AML/CFT legislation, regulations and other measures
- Countries in which the undertaking of terrorist activities is being supported or enabled
- A country subject to Mauritius or other national sanctions, embargoes or similar measures
- A jurisdiction identified by credible sources as providing support for terrorist activities
- A jurisdiction not member of the FATF or a FATF Style Regional Body (FSRB)
- Regional or local geographical factors related to risk (e.g., Mauritius domestic risk based on urban vs. rural; known crime/gang areas, etc.)

ANNEX 2 - RISK MITIGATION MEASURES

Risk Mitigation Measures For Higher Risk Situations May Include:

- obtaining additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment
- carrying out additional searches (e.g., verifiable adverse media searches) to inform the individual customer risk assessment
- commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity
- verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime
- seeking additional information from the customer about the purpose and intended nature of the business relationship
- increased awareness of higher risk situations within business lines across the entity
- increased monitoring of transactions
- the approval of the establishment of relationships is escalated to senior management
- the levels of on-going controls and reviews of relationships are increased;
- personnel that have clear lines of authority, responsibility and accountability
- adequate segregation of duties (for example, an employee establishing a relationship with a client is not authorized to also approve it as that authorization is the responsibility of someone else in the organization);
- proper procedures for authorization (for example, an employee processing a transaction for which the amount exceeds a certain threshold has to follow a procedure to get approval for the transaction by someone else in the financial institution)
- obtaining additional information about the intended nature of the relationship, including estimates regarding the amount and type of business activity
- requesting high risk clients to provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists
- getting independent verification of information (i.e. from a credible source other than the client)
- stopping any transaction with a potential client until identification information has been obtained
- implementing an appropriate process to approve all relationships identified as high risk as part of the client acceptance process or declining to do business with potential clients because they exceed your risk tolerance or appetite level
- implementing a process to exit from an existing high-risk relationship which is beyond the entity's stated risk tolerance or appetite level
- analyzing money laundering and terrorist financing risk vulnerabilities for new acquisition processes and for product or service development processes

5. INTERNAL CONTROLS, POLICIES AND PROCEDURES

A. RISK MANAGEMENT

5.01 As a general rule and for the purposes of AML/CFT, the business units, namely the front office, customer-facing activity, are the first line of defence in charge of identifying, assessing and controlling the risks of their business. They should be allotted sufficient resources to execute their duties effectively. The financial institution's policies, procedures and controls on AML/CFT should be clearly specified in writing, and communicated to all relevant employees in the business units. The financial institution should adequately train employees to implement the AML/CFT policies and procedures and to be aware of their obligations in ensuring compliance with prevailing AML/CFT laws, regulations and guidelines.

5.02 The second line of defence includes the Compliance officer or the Chief Officer in charge of AML/CFT, the compliance function, as well as other support functions which work together with the AML/CFT compliance function to identify ML/TF risks when they process transactions or applications or deploy systems or technology. The third line of defence is ensured by the internal audit function. Accordingly, financial institutions' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. Other support functions such as operations, human resource or technology also play a role to help mitigate the ML/TF risks that the financial institution faces.

5.03 As the third line of defence, internal audit plays an important role in independently evaluating the risk management controls and processes, systems and of the effectiveness of the first and second line of defense functions through periodic evaluations. The findings and related corrective actions shall be reported to the Audit Committee. Management should ensure that internal audit functions are staffed adequately with individuals who are well versed in such policies and procedures.

5.04 The AML/CFT framework of the financial institution should, therefore, be subject to periodic audits (including sample testing). Such audits should be performed not just on individual business functions but also on an institution-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF.

5.05 External auditors also have an important role to play in monitoring financial institutions' internal controls and procedures, and in confirming that they are in compliance with laws, rules, regulations and this Guideline.

STATUTORY REQUIREMENT

Financial Intelligence and Anti Money Laundering Act

5.06 Section 17A(1) of the FIAMLA requires every financial institution to –

(a) establish policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the financial institution under section 17[21];

[21] Please refer to Chapter 4

(b) monitor the implementation of, regularly review, update and, where necessary, enhance the, policies, controls and procedures established under paragraph (a);

(c) maintain a record in writing of –

(i) the policies, controls and procedures established under paragraph (a);

(ii) any changes to those policies, controls and procedures made as a result of the review and update required under paragraph (b); and

(iii) the steps taken to communicate those policies, controls and procedures, or any changes to them, internally.

5.07 The policies, controls and procedures must in terms of section 17A(2), be proportionate to the size and nature of the business of the financial institution and approved by its senior management.

Banking Act and the Financial Intelligence and Anti-Money Laundering Regulations

5.08 Section 64A(1)(b) of the Banking Act and Regulation 22 of the Financial Intelligence and Anti-Money Laundering Regulations 2018 require financial institutions to implement programmes, against money laundering and terrorism financing, which are commensurate with the ML and TF risks to which it is exposed and the size of its business. These programmes shall, at a minimum, include the following internal policies, procedures and controls–

(a) designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the financial institution with internal programmes, controls and procedures with the requirements of the FIAMLA and FIAML Regulations;

(b) screening procedures to ensure high standards when hiring employees;

(c) an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to –

(i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and

(ii) instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i); and

(d) an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and FIAML regulations.

B. AML/CFT GOVERNANCE FRAMEWORK

5.09 Financial institutions are required to have in place adequate policies, procedures and internal controls that promote high ethical and professional standards and prevent their institutions from being used, intentionally or unintentionally, by criminal elements. Financial institutions must therefore establish clear responsibilities to ensure that policies, procedures and internal controls are introduced and maintained which prevent criminals and their associates from gaining employment at their financial institution and deter criminals from using their facilities for money laundering and terrorist financing, thus ensuring that they comply with their obligations under the law.

5.10 The ultimate responsibility and accountability for ensuring compliance with AML/CFT laws, regulations, guidelines and instructions vest with the board of directors and senior management of the financial institution. It is imperative that the board and senior management of financial institutions ensure that the policies, procedures, systems and processes are put in place to prevent ML/FT and PF, as appropriate. The financial institutions' AML/CFT programme should be risk-based and commensurate with their nature, size, complexity and inherent risks.

5.11 Explicit responsibility should be allocated within the financial institutions for ensuring that the policies and procedures are managed effectively. While certain responsibilities can be delegated to senior AML/CFT employees, final accountability rests with the board of director and senior management of the financial institution. Financial institutions should ensure that there is a strong compliance culture throughout the organization, where the board of directors and senior management set the right tone. The board of directors and senior management should set a clear risk appetite and ensure a compliance culture which prevents the financial institution from being abused by money launderers and terrorist financiers.

5.12 Financial institutions' board of directors and senior management should have a clear understanding of the ML/TF risks to which the financial institution is exposed and how the financial institution's AML/CFT control framework operates to mitigate those risks.

C. RESPONSIBILITIES OF THE BOARD OF DIRECTORS[22]

5.13 The Board's oversight should align with international best practices, including the Guideline on Corporate Governance issued by the Bank. The key responsibilities of the Board shall include:

i. Approving the AML/CFT programme including all AML/CFT policies;

ii. Ensuring the establishment of appropriate mechanisms for the periodic review of the AML/CFT policies and procedures to ensure their continued relevance in line with changes in the financial institution's products and services and to address new and emerging ML/TF risks;

iii. Ensuring the establishment of an appropriate AML/CFT risk management framework with clearly defined lines of authority and responsibility for AML/CFT;

iv. Ensuring that the Board receives the requisite training on AML/CFT and understand the institution's specific AML/CFT risks and controls;

[22] Board' means the board of directors of a financial institution; except for branches of foreign banks 'board' means local advisory board/committee

v. Ensuring that the Board receives information about ML/TF risk assessment in a timely, complete, understandable and accurate manner so that it is equipped to make informed decisions. The reports escalated to the Board should include, inter alia, the following:

- Internal / External audit reports and supervisory reports on AML/CFT
- Remedial action plans, if any, to address the results of compliance testing and self-identified instances of non-compliance with AML/CFT requirements, the findings of internal and/ or external audits; and regulatory reports received from the Bank and other regulators on their assessment of the institution's AML/CFT programme;
- Recent developments in AML/CFT laws and regulations and implications if any, to the financial institution;
- Details of recent significant risk events and potential impact on the financial institution; and
- Statistics, including on statutory reporting to the FIU, orders from law enforcement agencies, sanctions imposed by regulators, refused or declined business and de-risked relationships.

D. ROLE OF SENIOR MANAGEMENT

5.14 Senior Management is responsible for the implementation, monitoring and management of the financial institution's AML/CFT programme, including ensuring adherence to established AML/CFT policies and procedures. Senior Management should, amongst others, ensure that the policies and procedures are risk-based, proportional and adequate to mitigate ML/TF risks of the financial institution; comply with all relevant AML/CFT laws, regulations and guidelines and are implemented effectively across relevant business areas.

5.15 Senior Management shall carry out a periodic review of the policies and procedures, at least every two years or earlier in the event of changes in regulatory or prudential requirements to ensure their continued relevance in line with developments, such as, changes in business model, new products/services, new and developing technologies and regulatory and legislative changes.

5.16 Senior Management should also ensure that:

i. It receives sufficient, regular and objective information and reports to assess the ML/TF risk to which the financial institution is exposed through its activities and business relationships and the effectiveness of the AML/CFT controls;

ii. Remedial actions are taken on a timely basis regarding recommendations made by internal and external auditors and regulators in respect of the AML/CFT programme;

iii. Relevant, adequate and timely information regarding AML/CFT matters is provided to the Board;

iv. Training is provided to all relevant categories of staff, including Compliance Officer and the MLRO/Deputy MLRO, on an ongoing basis which enables them to effectively discharge their AML/CFT responsibilities; and

v. The Compliance and Internal Audit functions are provided with sufficient resources, including but not limited to staff and IT resources, to execute all responsibilities effectively.

E. FINANCIAL INSTITUTION OPERATING IN A GROUP STRUCTURE

STATUTORY REQUIREMENT

Banking Act and Financial Intelligence and Anti-Money Laundering Regulations 2018

5.17 Financial institutions operating in a group structure are required in terms of section 64A(2) of the Banking Act and Regulation 23 (1) of Financial Intelligence and Anti-Money Laundering Regulations 2018 shall implement group-wide programme against money laundering and terrorism financing, which shall be applicable, and appropriate to, all branches and subsidiaries of the group and which shall include —

(a) the internal policies, procedures and controls set out in regulation 22;

(b) policies and procedures for sharing information required for the purposes of customer due diligence and money laundering and terrorism financing risk management;

(c) procedures to ensure that group-level compliance, audit, Money Laundering and Reporting Officer shall have the power to request customer, account and transaction information from branches and subsidiaries as necessary to perform their functions in order to combat money laundering and terrorism financing;

(d) the provision by the group-level functions to branches and subsidiaries, of information and analysis of transactions or activities which appear unusual when relevant and appropriate to risk management; and

(e) adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.

5.18 The financial institution is further required, under section 23(2) of the Financial Intelligence and Anti-Money Laundering Regulations 2018, to ensure that its foreign branches and subsidiaries —

(a) apply measures to combat money laundering and terrorism financing consistent with the home country requirements, where the minimum requirements of the host country are less strict than those of the home country, to the extent that host country laws and regulations permit; and

(b) where the host country does not permit the proper implementation of anti-money laundering and combating the financing of terrorism measures, apply appropriate additional measures to manage the money laundering and terrorism financing risks, and inform their home supervisors.

GENERAL GUIDANCE

5.19 Financial groups[23] incorporated in Mauritius with overseas branches or subsidiary undertakings should apply the financial group's AML/CFT programmes, to ensure that all branches and

[23] "financial group" means a group that consists of a parent company or of any other entity exercising control and coordinating functions over the rest of the group for the application of group supervision under the core principles, together with branches or subsidiaries that are subject to Anti-Money Laundering or the Combating the Financing of Terrorism policies and procedures at the group level.

subsidiary undertakings that carry on the same business as a financial institution in a place outside Mauritius have procedures in place to comply with the CDD and record keeping requirements similar to those imposed under this Guideline to the extent permitted by the law of that place.

5.20 The financial group should communicate the group programmes to its overseas branches and subsidiary undertakings. These programmes should include policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management.

5.21 The financial group should have a thorough understanding of all the risks associated with its customers across the group, either individually or as a category, and should document and update these on a regular basis, commensurate with the level and nature of risk in the group.

5.22 When a branch or subsidiary undertaking of a financial group outside Mauritius is unable to comply with requirements that are similar to those imposed under this Guideline because this is not permitted by local laws, the financial institution must:

(a) inform the Bank of such failure; and

(b) take additional measures to effectively mitigate ML/TF risks faced by the branch or subsidiary undertaking as a result of its inability to comply with the above requirements.

5.23 Financial groups that use agents should include them in their AML/CFT programmes and monitor them for compliance with these programmes. The financial institution should maintain a current list of its agents and make this list available to the Bank upon request.

Additionally, a MVTs provider shall –

(a) maintain a list of all its agents or subagents which shall be provided –

(i) to the FIU or to the relevant supervisory authority upon request;
(ii) to competent authorities in countries in which its agent operates;

(b) include agents in their programs for combating money laundering and terrorism financing and monitor them for compliance with these programs.

F. APPOINTMENT OF A COMPLIANCE OFFICER

STATUTORY REQUIREMENT

Banking Act and Financial Intelligence and Anti-Money Laundering Regulations 2018

5.24 Financial institutions are required to appoint a Compliance Officer at Senior Management level in accordance with section 64A(1)(b)(i) of the Banking Act and Regulation 22(1)(a) of the Financial Intelligence and Anti-Money Laundering Regulations 2018, who will bear the responsibility for implementation and ongoing compliance of the financial institution with internal programmes, procedures and controls relating to money laundering and the financing of terrorism activities.

GENERAL GUIDANCE

5.25 Financial institutions are required to appoint a Compliance Officer who will ensure that the responsibilities of financial institutions with respect to AML/CFT are being discharged as required under the Financial Intelligence and Anti-Money Laundering Act and Financial Intelligence and Anti-Money Laundering Regulations 2018.

5.26 The appointment of a Compliance Officer should be in line with the requirements of the prudential guidelines issued by the Bank, regarding, amongst others, their fitness and probity.

5.27 The Compliance Officer should have the necessary authority within the financial institution, such that, issues raised by him/her receive the necessary attention by the Board, Senior Management and business lines. He/she shall have a direct reporting line to the Board or a committee of the Board.

5.28 It is important that the procedures and responsibilities for monitoring compliance with, and effectiveness of, anti-money laundering and financing of terrorism policies and procedures are clearly laid down by all financial institutions.

5.29 It is not necessary, however, to appoint a Compliance Officer in each and every branch of the financial institution. The appointment of a Compliance Officer at the Head Office with jurisdiction over its branches will suffice.

5.30 Although it is advisable for the Compliance Officer and the MLRO to be two distinct persons, it is left to individual financial institutions to decide whether the Compliance Officer may also cumulate the functions of the MLRO.

5.31 The financial institution must ensure that the Compliance Officer has sufficient resources, including sufficient time and compliance support staff which are commensurate with its size and complexity of its business activities.

5.32 Senior Management should ensure that the Compliance Officer is capable of accessing on a timely basis all available information, both from internal and external sources for the purpose of discharging his responsibilities.

5.33 The responsibilities of the Compliance Officer should include –

(a) developing written AML/CFT policies and procedures that are approved by the Board;

(b) carrying out, or overseeing the carrying out of, ongoing monitoring of all AML/CFT obligations of the financial institutions including business relations. This implies sample testing of compliance and review of exception reports to alert Senior Management or the Board of Directors of any non-adherence to AML/CFT procedures;

(c) keeping the AML/CFT program updated relative to the financial institution's identified inherent risks and giving consideration to local and international developments in ML and TF;

(d) conducting periodic assessments of AML/CFT control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF risks;

(e) conducting enterprise-wide risk assessments of ML/TF risks including the timely assessments of new products and services as well as new technology and processes, as prescribed in this Guideline;

(f) ensuring systems resources, including those required to identify and report suspicious transactions, are appropriate in all relevant areas of the institution;

(g) promoting compliance with the AML/CFT laws, regulations and this Guideline, and taking overall charge of all AML/CFT matters within the organisation;

(h) informing employees and officers promptly of regulatory and legislative changes and of revisions to policies and procedures;

(i) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;

(j) ensuring that ongoing training programs on ML and TF are current and relevant and are carried out for all employees, senior management and the Board

(k) ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information;

(l) reporting to senior management on the outcome of reviews of the financial institution's compliance with the AML/CFT laws, regulations and this Guideline, and risk assessment procedures; and

(m) reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising from audit, inspection, and compliance reviews, to the financial institution's senior management and to the Board[24] or a committee of the Board.

5.34 The business interests of financial institutions should not interfere with the effective discharge of the above-mentioned responsibilities of the compliance officer, and potential conflicts of interest should be avoided. To enable unbiased judgments and facilitate impartial advice to management, the compliance function should, for example, be distinct from the internal audit and business line functions. Where any conflicts between business lines and the responsibilities of the compliance officer arise, procedures should be in place to ensure that AML/CFT concerns are objectively considered and addressed at the appropriate level of the financial institution's management.

G. INTERNAL AUDIT FUNCTION

STATUTORY REQUIREMENT

Banking Act and Financial Intelligence and Anti-Money Laundering Regulations 2018

5.35 Section 64A(1)(b)(iv) of the Banking Act and Regulation 22(1)(d) of the Financial Intelligence and Anti-Money Laundering Regulations 2018 require financial institutions to implement programmes, against money laundering and terrorism financing, which are commensurate with the ML and TF risks to which it is exposed and the size of its business, which shall include an

[24] Board' means the board of directors of a financial institution; except that for branches of foreign banks 'board' means local advisory board/committee

independent internal audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the Financial Intelligence and Anti-Money Laundering Act and Financial Intelligence and Anti-Money Laundering Regulations 2018.

GENERAL GUIDANCE

5.36 The Internal Audit function should perform regular reviews to evaluate the adequacy of implementation of the financial institution's AML/CFT policies, procedures and systems. The review process should identify weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions, including ensuring that recommendations made by the external auditor and the Bank have been satisfactorily addressed.

5.37 All audit documentation, including, amongst others, work plan, audit scope, transaction testing, should be made available to the Bank upon request. Deficiencies noted during the audit including any breaches of policy or procedure, regulatory or legislative requirement should be clearly documented in an audit report and reported to Senior Management and the Audit Committee/ the Board. Senior management should advise on corrective actions to address deficiencies and a timeline for implementing such actions. The Audit Committee/ Board should follow up in a consistent manner to ensure that corrective actions are implemented in a timely manner.

5.38 The internal auditor should carry out a regular review of the adequacy of the financial institution's AML/CFT programme to establish the effectiveness of its overall AML/CFT policies and processes and the quality of its risk management across its operations and business units. The review should include, but not be limited to:

i. A review of the adequacy of the financial institution's ML/TF risk assessment framework and the application of a risk-based approach;

ii. A review of the effectiveness of the financial institution's staff in implementing the in implementing and complying with established AML/CFT policies and procedures;

iii. An evaluation of management's efforts to take corrective actions in respect of deficiencies noted in previous audits and regulatory examinations;

iv. A review of the effectiveness of the compliance function;

v. A review of level of awareness of staff having AML/CFT responsibilities;

vi. A review of the effectiveness of the suspicious activity monitoring systems used for AML/CFT compliance including a review of the criteria and processes for identifying and reporting suspicious transactions;

vii. An assessment of the overall process for identifying and reporting suspicious activity, including a review of 'not filed' (closed as not suspicious) internal suspicious transactions reports, to determine the adequacy, completeness and effectiveness of the STR filing process. The internal audit review does not include a review of actual STRs filed with the FIU.

5.39 The frequency and extent of the review should be commensurate with the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses. The basis for the audit frequency must be clearly articulated in the financial institution's audit policy and scope.

H. SCREENING OF EMPLOYEES

STATUTORY REQUIREMENT

Banking Act and Financial Intelligence and Anti-Money Laundering Regulations 2018

5.40 Financial institutions are required, in terms of section 64A(1)(b)(ii) of the Banking Act and regulation 22 of the Financial Intelligence and Anti-Money Laundering Regulations 2018, to implement programmes against money laundering and terrorism financing which shall, inter alia, cover internal policies, procedures and controls on screening procedures to ensure high standards when hiring officers.

GENERAL GUIDANCE

5.41 Every financial institution should ensure that employees recruited have integrity. In this respect, consideration may be given to–

(a) obtaining and confirming appropriate references at the time of recruitment;

(b) requesting information from the employee with regard to any regulatory action taken against him or action taken by a professional body; and

(c) requesting information from the employee with regard to any criminal convictions and the provision of a check of his criminal record. The financial institution should also take steps to manage potential conflicts of interest for staff with AML/CFT responsibilities.

I. ONGOING AML/CFT TRAINING

5.42 Ongoing staff training is an integral element of an effective AML/CFT system to prevent and detect potential illicit transactions pertaining to money laundering, terrorist or proliferation financing activities as outlined in Chapter 11 of the Guideline. It is therefore important for every financial institution, in order to combat money laundering and the financing of terrorism and proliferation in an efficient and effective manner, to implement an ongoing training programme for its employees in order to discharge part of its statutory duty to take reasonable measures in that regard.

J. APPOINTMENT OF A MONEY LAUNDERING REPORTING OFFICER

STATUTORY REQUIREMENT

Financial Intelligence and Anti-Money Laundering Regulations 2018

5.43 Regulation 26 (1) of the FIAML Regulations 2018 requires that a financial institution shall appoint a Money Laundering Reporting Officer (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 ML or TF.

5.44 Pursuant to Regulation 26 (2) of the FIAML Regulations 2018, financial institutions are required to appoint a Deputy MLRO to perform the duties of the MLRO in his absence.

5.45 Regulation 26 (4) of the FIAML Regulations 2018 requires that the Money Laundering Reporting Officer and the Deputy Money Laundering Officer shall –

(a) be sufficiently senior in the organisation of the financial institution or have sufficient experience and authority; and

(b) have a right of direct access to the board of directors of the financial institution and have sufficient time and resources to effectively discharge his functions.

5.46 The MLRO/Deputy MLRO must have appropriate independence, in particular from customer-facing and business development roles and should have sufficient time and resources to effectively discharge their functions.

5.47 The financial institution must ensure that the MLRO is fully aware of both his and the institution's obligations under the FIAMLA and FIAML Regulations 2018.

5.48 In branches of financial institutions, there should be a responsible officer on whom responsibility for AML/CFT matters would devolve.

5.49 It is incumbent on the MLRO, on behalf of the financial institution, to make Suspicious Transaction Reports to the FIU.

RECOMMENDED PROCEDURES

5.50 All financial institutions operating within Mauritius should:

(a) have procedures for the prompt validation of suspicions and subsequent reporting by the internal employees to the MLRO.

(b) provide the MLRO with necessary access to systems and records to enable him to investigate and validate internal suspicions reports which have been reported to him.

(c) inform all employees of the identities of the MLRO and Deputy MLRO.

K. NEW TECHNOLOGIES

Financial Intelligence and Anti Money Laundering Act and Financial Intelligence and Anti-Money Laundering Regulations 2018

5.51 Financial institutions are required, in terms of section 17(3) of the Financial Intelligence and Anti-Money Laundering Act, and Regulation 19 of the Financial Intelligence and Anti-Money Laundering Regulations 2018, to identify and assess the money laundering and terrorism financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. They are required to undertake the risk assessments prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks.

Banking Act 2004

5.52 Pursuant to section 53A of the Banking Act, every financial institution and every holder of a licence shall, in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products -

(a) undertake a risk assessment prior to the launch or use of such products, business practices and technologies;

(b) identify and assess the money laundering and terrorism financing risks that may arise in relation to the launch or use of such products, business practices and technologies; and

(c) take appropriate measures to manage and mitigate the risks identified.

5.53 Financial institutions should have policies in place or take such measures as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Financial institutions may, for the purposes of risk assessment, refer to the reports on "Risk Management Principles for Electronic Banking"[25] issued by the Basel Committee in July 2003 and to the reports on (i) "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems" issued by the FATF on 10 July 2008 and (ii) "Money Laundering Using New Payment Methods" issued by the FATF in October 2010. The FATF has also issued typologies reports which focused on the potential for new payment products and services to be misused by criminals, the identification of risk factors which can significantly differ from one new payment product or service to another, depending on functionality; and risk mitigates which can be tailored to particular new payment product or service to address its specific risk profile. In 2013, the FATF issued guidance on taking a risk-based approach to prepaid cards, mobile payments and internet payment systems[26], which financial institutions are recommended to consider prior to offering new payment products and services.

5.54 Financial institutions should ensure that there are systems and controls in place to identify and assess emerging ML/TF risk associated with technological developments, and where appropriate, incorporate these into the risk assessments in a timely manner.

[25] https://www.bis.org/publ/bcbs98.pdf
26 https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

6. CUSTOMER DUE DILIGENCE AND IDENTIFICATION PROCEDURES

6.01 Financial institutions must develop and implement risk based policies and procedures to mitigate the ML/TF risks identified in their business and customer risk assessments. The risk assessment framework should identify which customers or categories of customers present higher risk and therefore require the application of enhanced due diligence (EDD).

6.02 Similarly, where the financial institution determines that a customer or a category of customer presents low risk, simplified due diligence (SDD) should be applied. Where SDD measures are applied on the basis of an assessment of low ML/TF risk, the customer due diligence (CDD) policies and procedures should clearly articulate the rationale and the applicable measures to be undertaken.

6.03 Financial institutions are reminded, however, that the application of a risk-based approach to CDD measures is not to be taken as a static formula by which, for example, all medium-risk customers are necessarily always subjected to normal CDD measures and all low-risk customers are always subjected to SDD measures. Each customer's ML/FT risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behaviour, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, financial institutions should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/FT risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/FT risk category.

REGULATORY FRAMEWORK

Banking Act

6.04 Section 55 of the Banking Act 2004 in respect of identity of customers provides as follows:-

(1) Every financial institution shall only open accounts for deposits of money and securities, and rent out safe deposit boxes, where it is satisfied that it has established the true identity of the person in whose name the funds or securities are to be credited or deposited or the true identity of the lessee of the safe deposit box, as the case may be.

(2) Every financial institution shall require that each of its accounts be properly named, at all times, so that the true owner of the accounts can be identified by the public and no name shall be allowed that is likely to mislead the public.

6.05 It is therefore mandatory for financial institutions to verify the true identity of their customers before opening any account, accepting any deposit of money and securities and renting a safe deposit box. In that respect, it is in context to state that the Financial Intelligence and Anti-Money Laundering Regulations 2003 expressly prohibit financial institutions from opening anonymous or fictitious accounts.

6.06 By virtue of Section 55(2) of the Banking Act 2004 the keeping of reference accounts by financial institutions is prohibited.

6.07 Breach of section 55 of the Banking Act 2004 is an offence which carries a fine of not less than one million rupees and not more than 5 million rupees.

Financial Intelligence and Anti-Money Laundering Act

Fictitious and anonymous accounts

6.08 It is prohibited under Section 17B for a financial institution to establish or maintain an anonymous account or an account in a fictitious name.

Customer due diligence requirements

6.09 Pursuant to Section 17C, a financial institution shall undertake CDD measures by means of such reliable and independent source documents or information as may be prescribed, and in the following circumstances –

(a) when opening an account for, or otherwise establishing a business relationship with, a customer;

(b) where a customer who is neither an account holder nor in an established business relationship with the financial institution wishes to carry out –

(i) a transaction in an amount equal to or above 500, 000 rupees or an equivalent amount in foreign currency or such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked; or

(ii) a domestic or cross-border wire transfer;

(c) whenever doubts exist about the veracity or adequacy of previously obtained customer identification information;

(d) whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

6.10 A financial institution shall, with respect to each customer and business relationship, when applying CDD measures take into account the outcome of the risk assessment required to be carried out under section 19D.

6.11 Where the risks are higher, a financial institution shall conduct enhanced due diligence measures consistent with the risks identified.

6.12 Where the risks are lower, a financial institution may conduct simplified due diligence measures, unless there is a suspicion of money laundering or terrorism financing in which case enhanced CDD measures shall be undertaken.

6.13 In all cases, a financial institution shall apply such CDD measures as may be prescribed or specified in this Guideline.

6.14 Any person who knowingly provides any false or misleading information to financial institutions in connection with CDD requirements under this Act or any guidelines issued under this Act 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.

Existing customers

6.15 A financial institution shall under Section 17E, apply the CDD requirements to customers and beneficial owners with which it had a business relationship prior to the commencement of section 17C on 9 August 2018

6.16 The CDD requirements shall be applied at appropriate times and on the basis of materiality and risk, depending on the type and nature of the customer, the business relationship, products or transactions and taking into account whether and when CDD measures have previously been applied and the adequacy of the data obtained, or as may be specified in any guidelines issued under the Act.

6.17 For the purpose of section 17E, "beneficial owner" –

(a) means the natural person –

(i) who ultimately owns or controls a customer;
(ii) on whose behalf a transaction is being conducted; and

(b) includes those natural persons who exercise ultimate control over a legal person or arrangement and such other persons as may be prescribed.

Third party reliance

6.18 in terms of section 17D, a financial institution may rely on third parties to perform CDD measures to comply with the requirements of section 17C, subject to such terms and conditions as may be prescribed. The financial institution shall, nonetheless, remain responsible for compliance with the requirements under the Act.

'KNOW YOUR CUSTOMER'

6.19 The foundation of any effective system to combat money laundering and the financing of terrorism is the 'Know Your Customer' (KYC) Principle. It is the degree of proximity between the financial institution and the customer which the KYC principle entails that will allow financial institutions to gauge a situation, decide whether a transaction is suspicious and be able to avert risks inherent in money laundering and the financing of terrorism.

6.20 The safety and soundness of financial institutions are therefore largely dependent on their KYC procedures. Sound KYC procedures, inter alia,

(i) reduce the likelihood of financial institutions being used as a vehicle for the laundering of the proceeds of criminal activities or the moving of terrorist funds.

(ii) constitute an essential part of sound risk management by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities.

6.21 The inadequacy or absence of KYC standards can subject financial institutions to serious risks, especially

(i) **Reputational risk** - that is, the risk that adverse publicity regarding a financial institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution.

(ii) **Operational risk** – that is, the risk that the financial institution will suffer direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events which in the context of KYC relates to weaknesses in the implementation of programmes, ineffective control procedures and failure to practise due diligence.

(iii) **Legal risk** – that is, the possibility that lawsuits, adverse judgements or contracts turn out to be unenforceable and disrupt or adversely affect the operations or condition of a financial institution.

6.22 The need for financial institutions to know their customer is therefore vital for the prevention of money laundering and the financing of terrorism.

6.23 When a business relationship is being established, the nature of the business that the customer expects to conduct with the financial institutions should be ascertained at the outset, to show what might be expected as normal activity. In order to be able to judge whether a transaction is or is not suspicious, financial institutions should have a clear understanding of the legitimate business of their customers and effect an ongoing monitoring of the activities of those customers in order to detect whether those transactions conform or otherwise with the normal or expected transactions of that customer.

6.24 KYC should be a core feature of financial institutions' risk management and control procedures, and should be complemented by regular compliance reviews and internal audit.

ESSENTIAL ELEMENTS OF KYC STANDARDS

6.25 The essential elements of KYC standards should start from the financial institutions' risk management and control procedures and should include the following :

(i) customer acceptance policy,
(ii) customer identification,
(iii) ongoing monitoring of accounts and transactions; and
(iv) risk management.

6.26 Sound risk management requires the identification and analysis of ML/TF risks present within the financial institution and the design and effective implementation of policies and procedures that are commensurate with the identified risks. Financial institutions should :

(i) develop a thorough understanding of the inherent ML/TF risks present in its customer base, products, delivery channels and services offered and the jurisdictions within which it or its customers do business; and

(ii) design and implement their policies and procedures for customer acceptance, due diligence and ongoing monitoring to adequately control those identified inherent risk.

6.27 In addition to assessing the ML/TF risks presented by an individual customer, financial institutions should identify and assess ML/TF risks on an enterprise-wide level. This should include a consolidated assessment of the institution's ML/TF risks that exist across all its business units, product lines and delivery channels. The enterprise-wide ML/TF risk assessment is intended to enable the financial institution better understand its overall vulnerability to ML/TF risks and forms the basis for the institution's overall risk-based approach.

6.28 The senior management of the financial institution should approve the enterprise-wide ML/TF risk assessment and relevant business units should give their full support and active co-operation to the enterprise-wide ML/TF risk assessment.

6.29 The scale and scope of the enterprise-wide ML/TF risk assessment should be commensurate with the nature and complexity of the financial institution's business. In conducting an enterprise-wide risk assessment, the broad ML/TF risk factors that the financial institution should consider are set out in Chapter 4.

6.30 As far as possible, financial institutions' enterprise-wide ML/TF risk assessment should entail both qualitative and quantitative analyses to ensure that the financial institution accurately understands its exposure to ML/TF risks. A quantitative analysis of the financial institution's exposure to ML/TF risks should involve evaluating data on the financial institution's activities using the applicable broad risk factors set out in paragraph 6.17D.

6.31 In assessing its overall ML/TF risks, financial institutions should make its own determination as to the risk weights to be given to the individual factor or combination of factors.

6.32 The nature and extent of AML/CFT risk management systems and controls implemented should be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment, which should also serve to guide the allocation of AML/CFT resources within the institution.

6.33 Financial institutions should assess the effectiveness of its risk mitigation procedures and controls by monitoring the following:

(a) the ability to identify changes in a customer profile (e.g. Politically Exposed Persons status) and transactional behaviour observed in the course of its business;

(b) the potential for abuse of new business initiatives, products, practices and services for ML/TF purposes;

(c) the compliance arrangements (for e.g. through its internal audit or quality assurance processes or external review);

(d) the balance between the use of technology-based or automated solutions with that of manual or people-based processes, for AML/CFT risk management purposes;

(e) the coordination between AML/CFT compliance and other functions of the financial institution;

(f) the adequacy of training provided to employees and officers and awareness of the employees and officers on AML/CFT matters;

(g) the process of management reporting and escalation of pertinent AML/CFT issues to the financial institution's senior management;

(h) the coordination between the financial institution and regulatory or law enforcement agencies; and

(i) the performance of third parties relied upon by the financial institution to carry out CDD measures.

6.34 In order to keep its enterprise-wide risk assessments up-to-date, financial institutions should review its risk assessment at least once every two years or when material trigger events occur, whichever is earlier. Such material trigger events include, but are not limited to, the acquisition of new customer segments or delivery channels, or the launch of new products and services by the financial institution. The results of these reviews should be documented and approved by senior management even if there are no significant changes to the enterprise-wide risk assessment of the institution.

6.35 Financial institutions should ensure that the following documentation are kept on record and made available to the Bank upon request:

(a) enterprise-wide ML/TF risk assessment by the financial institution;

(b) details of the implementation of the AML/CFT risk management systems and controls as guided by the enterprise-wide ML/TF risk assessment;

(c) the reports to senior management on the results of the enterprise-wide ML/TF risk assessment and the implementation of the AML/CFT risk management systems and controls; and

(d) details of the frequency of review of the enterprise-wide ML/TF risk assessment.

CUSTOMER ACCEPTANCE POLICY

6.36 Financial institutions should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a financial institution.

6.37 In preparing such policies, factors such as the customer's background, nature of business or social engagement, country of origin with a view to determining whether those countries have adequate systems in place against money laundering and the financing of terrorism, public or high profile position and other risk indicators should be considered.

6.38 Customer acceptance policies and procedures should accordingly be graduated and require more extensive due diligence for higher risk customers, such as an individual planning to maintain a large account balance and conduct regular cross-border wire transfers or politically exposed persons. Decisions to enter into or pursue business relationships with higher-risk customers should require the application of enhanced due diligence measures, such as approval to enter into or continue such business relationships being taken by senior management. The customer acceptance policy should also define circumstances under which the financial institution would not accept a new business relationship or would terminate an existing one.

6.39 The exercise should however be calibrated to ensure that the customer acceptance policy does not result in a denial of access by the general public to legitimate banking, deposit taking and cash dealer services.

GENERAL IDENTIFICATION REQUIREMENTS AND RISK PROFILING

STATUTORY REQUIREMENTS

6.40 Regulation 3 of the FIAML Regulation requires financial institutions to –

(a) identify his customer whether permanent or occasional and verify the identity of his customer using reliable, independent source documents, data or information, including, where available, electronic identification means, or any other secure, remote or electronic identification process as may be specified by the relevant regulatory body or supervisory authority;

(b) verify that any person purporting to act on behalf of a customer is so authorised, and shall identify and verify the identity of that person;

(c) identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source such that the financial institution is satisfied that he knows who the beneficial owner is;

(d) understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction;

(e) conduct ongoing monitoring of a business relationship, including –

(i) scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer;

(ii) ensuring that documents, data or information collected under the Customer Due Diligence (CDD) process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

6.41 Where there is a suspicion of money laundering, terrorism financing or proliferation financing, the financial institution shall, notwithstanding any applicable thresholds, undertake CDD measures in accordance with this regulation.

6.42 Where a financial institution suspects money laundering, terrorism financing or proliferation financing, and he reasonably believes that performing the CDD process, may tip-off the customer, he shall not pursue the CDD process and shall file a suspicious transaction report under section 14 of the Act. The suspicious transaction report shall specify the reasons for not pursuing the CDD process.

6.43 The overriding requirement is that a financial institution shall undertake CDD measures set out hereinafter,

(a) when opening an account for, or otherwise establishing a business relationship with, a customer;

(b) where a customer who is neither an account holder nor in an established business relationship with the financial institution, wishes to carry out –

(i) a transaction in an amount equal to or above 500,000 rupees or an equivalent amount in foreign currency or such amount as may be prescribed, whether conducted as a single transaction or several transactions that appear to be linked; or

(ii) a domestic or cross-border wire transfer;

(c) whenever doubts exist about the veracity or adequacy of previously obtained customer identification information;

(d) whenever there is a suspicion of money laundering or terrorism financing involving the customer or the customer's account.

6.44 Where a financial institution is unable to comply with relevant CDD measures under the FIAML regulations, he shall –

(a) not open the account, commence the business relationship or perform a transaction; or
(b) terminate the business relationship; and
(c) in relation to the customer, file a suspicious transaction report under section 14 of the Act.

Where the Customer is a natural person

6.45 For a customer who is a natural person, the financial institution shall obtain and verify–

(a) the full legal and any other names, including, marital name, former legal name or alias;
(b) the date and place of birth;
(c) the nationality;
(d) the current and permanent address; and
(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

The documentary evidence specified in this Guideline shall be used for the purposes of verification of identity requirement.

6.46 Where the customer is a legal person or legal arrangement, the financial institution shall –

(a) with respect to the customer, understand and document –

(i) the nature of his business; and
(ii) his ownership and control structure;

(b) identify the customer and verify his identity by obtaining the following information –

(i) name, legal form and proof of existence;
(ii) powers that regulate and bind the customer;
(iii) names of the relevant persons having a senior management position in the legal person or arrangement; and
(iv) the address of the registered office and, if different, a principal place of business.

Beneficial Owner

6.47 The FIAML Regulations define a "beneficial owner" as the natural person (i) who ultimately owns or controls a customer; or (ii) on whose behalf a transaction is being conducted, and includes those natural persons who exercise ultimate control over a legal person or legal arrangement and such other persons as specified in regulations 6 and 7 of the FIAML Regulations.

6.48 Regulation 3(c) of the FIAML Regulation requires financial institutions to identify the beneficial owner and take reasonable measures, i.e. appropriate measures which are commensurate with the money laundering or terrorist financing risks, to verify the identity of the beneficial owner, using relevant information or data obtained from a reliable source such that the financial institution is able to justify his assessment to competent authorities[27], an investigatory body or the FlU, that he knows who the beneficial owner is.

6.49 The FATF has in its Guidance on Transparency and Beneficial Ownership[28] emphasised that the purpose of the FATF standards on transparency and beneficial ownership is to prevent the misuse of corporate vehicles for money laundering or terrorist financing and recommends that the misuse of corporate vehicles could be significantly reduced if information regarding both the legal owner and the beneficial owner, the source of the corporate vehicle's assets, and its activities were readily available to the authorities.

6.50 The FATF Guidance highlights that beneficial ownership information can be obscured through the use of: a) shell companies (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership which is spread across jurisdictions b) complex ownership and control structures involving many layers of shares registered in the name of other legal persons c) bearer shares and bearer share warrants d) unrestricted use of legal persons as directors e) formal nominee shareholders and directors where the identity of the nominator is undisclosed f) informal nominee shareholders and directors, such as close associates and family, and g) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets. h) use of intermediaries in forming legal persons, including professional intermediaries.

6.51 When an individual is the sole shareholder of a company and controls it directly, that individual is the BO of the company. However, there may be more layers involved in the ownership structure, perhaps a chain of entities between a legal vehicle and its BO. For further guidance to identify and collect beneficial ownership information, financial institutions may refer to the Beneficial Ownership Implementation Toolkit prepared by the Secretariat of the Global Forum on Transparency and Exchange of Information for Tax Purposes and the Inter-American Development Bank[29].

Where the customer is a legal person

6.52 Pursuant to the FIAMLA, "legal person" refers to any entity, other than a natural person, that can establish a permanent business relationship with a financial institution or otherwise own property, and includes a company, a foundation, an association, a limited liability partnership or such other entity as may be prescribed.

6.53 Where the customer is a legal person, the financial institution shall identify and take reasonable measures to verify the identity of **beneficial owners** by obtaining information on –

(a) the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;

---

[27] "competent authorities" — (a) means a public authority to which responsibility to combat money laundering or terrorist financing is designated; and (b) includes a supervisory authority, regulatory body and an investigatory authority;

[28] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf

[29] https://www.oecd.org/tax/transparency/beneficial-ownership-toolkit.pdf

(b) where there is doubt under paragraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as may be specified by relevant regulatory body or supervisory authority; and

(c) where no natural person is identified under paragraph (a) and (b), the identity of the natural person who holds the position of senior managing official.

6.54 Financial institution must keep records of the actions taken under paragraph 6.50 as well as any difficulties encountered during the verification process.

Where the customer is legal arrangement

6.55 "legal arrangement" is defined under the FIAMLA as an express trust or any other similar arrangement.

6.56 For customers that are legal arrangements, financial institutions shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information–

(a) for trusts, on the identity of the settlor, the trustee, the beneficiaries or class of beneficiaries, and where applicable, the protector or the enforcer, and any other natural person exercising ultimate effective control over the trust, including through a chain of control or ownership;

(b) for other types of legal arrangements, on the identity of the persons in equivalent or similar positions.

Timing of verification

6.57 A financial institution shall verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers.

6.58 Where doubts exist about the veracity or adequacy of previously obtained customer identification information, the financial institution shall identify and verify the identity of the customer and beneficial owner before the customer may conduct any further business.

6.59 In determining when to take CDD measures in relation to existing customers, a financial institution shall take into account, among other things –

(a) any indication that the identity of the customer or the beneficial owner, has changed;

(b) any transactions which are not reasonably consistent with his knowledge of the customer;

(c) any change in the purpose or intended nature of his relationship with the customer;

(d) any other matter which might affect the financial institution's assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

Simplified CDD Measures

6.60 A financial institution may apply simplified CDD measures where lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with the guidance set out hereunder.

6.61 Where a financial institution determines that there is a low level of risk, the financial institution shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment conducted by the Bank, whichever is most recently issued.

6.62 Simplified CDD shall not apply where, a financial institution knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or terrorist financing.

6.63 SDD generally involves a more lenient application of certain aspects of customer due diligence measures, including, but not limited to, such elements as:

- A reduction in verification requirements with regard to customer or Beneficial Owner identification;
- Fewer and less detailed inquiries in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions;
- More limited supervision of the Business Relationship, including less frequent monitoring of transactions, and less frequent review/updating of customer due diligence information.

6.64 The application of SDD may be considered in the following circumstances:

- *Identified low-risk customers.* When the customer or Beneficial Owner is identified as posing a low risk of ML/FT, FIs are permitted to complete the verification of their identity after the establishment of a Business Relationship under the conditions specified in this Guideline. In this regard, financial institutions are required to implement appropriate and effective measures to control the risks of ML/FT, including the risks in regard to the customer or Beneficial Owner benefitting from the Business Relationship prior to the completion of the verification process.

- The NRA Report 2019 has however not identified any low risk sector. Therefore, the application of simplified CDD measures does not arise in the current risk environment.

Examples of SDD Measures

6.65 The SDD measures described below are for guidance only and should not be considered as prescriptive or exhaustive. Where a financial institution determines, based on its risk assessment that the ML/TF risks are lower, the financial institution may apply one or more of the following SDD measures:

i. *Adjust the timing of CDD where the product or transaction has features that limit its use for ML/TF purposes.*

ii. *Adjust the quantity of information requested from the customer for identification, verification or monitoring purposes.*

iii. *Adjust the quality or source of information obtained for identification, verification or monitoring purposes*

iv. *Adjust the frequency of CDD updates and reviews of the business relationship*

v. *Adjust the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only*.

SPECIFIC GUIDANCE ON CDD DOCUMENTS AND MEASURES

6.66 Financial institutions are required to ensure at the outset whether a prospective customer[30] is acting on his behalf or on behalf of a third party. Financial institutions should establish to its satisfaction that it is dealing with a real person or organisation, and verify the identity of the person or organisation accordingly. If funds that are to be deposited or transferred are being supplied on behalf of a third party, then the identity of the third party should be established and verified. In case a financial institution is not able to determine whether the applicant for business is acting for a third party, it should make a record of the grounds for suspecting that the applicant for business is so acting and make a Suspicious Transaction Report to the Financial Intelligence Unit.

6.67 Financial institutions should also require customers to complete a written declaration of the identity and details of natural person(s) who are the ultimate beneficial owner(s) of the business relationship or transaction as a first step in meeting their beneficial ownership customer due diligence requirements.

6.68 Financial institutions need to obtain all information necessary to establish to their full satisfaction the identity of the applicant for business and the purpose and nature of the business relationship or transaction. They should cross check information by accessing available public databases such as telephone directories and electoral registers and private databases such as Credit Information Bureaux, both at the local and international levels and keep on their files full information on ultimate beneficial owners in case they are not the same persons as the applicant for business, as well as persons acting on their behalf, and accordingly take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is.

6.69 When an existing customer closes one account and opens another there is no need to re-verify identity, although good practice requires that the details on the customer's file be reconfirmed. This is particularly important if there has been no recent contact with the customer e.g. for the past twelve months. Details of the previous accounts and steps originally taken to verify identity or any introduction records should be transferred to the new account records.

6.70 Subsequent changes to the name of the applicant for business, address or employment details of which the financial institution becomes aware, should be recorded and be duly substantiated by the appropriate documentary evidence as part of the KYC process. CDD information on the customer and the beneficial owner has to be kept up to date.

---

[30] "customer" means a natural person or a legal person or a legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes — (a) a signatory to a transaction or account; (b) any person to whom an account or rights or obligations under a transaction have been assigned or transferred; (c) any person who is authorised to conduct a transaction or control an account; (d) any person who attempts to take any action referred to above; (e) an applicant for business;

6.71 In the case of an applicant for business transferring an opening balance from an account which he maintains with one bank or non-bank deposit taking institution directly to another bank or non-bank deposit taking institution, banks and non-bank deposit taking institutions should consider the possibility that the previous account manager may have asked for the account to be closed because of suspicions about dubious activities. If a financial institution has any reason to believe that an applicant is being or has been rejected by another financial institution, it should apply enhanced diligence procedures before accepting the customer.

6.72 Financial institutions should pay special attention to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose and should examine as far as possible the background and purpose of such transactions and set their findings in writing. As part of the broader customer due diligence measures, financial institutions should ensure that information regarding source of funds and/or destination of funds are corroborated. Examples of such transactions or patterns of transactions include : significant transactions relative to a relationship; transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance, or transactions which fall out of the regular pattern of the account's activity. (See further paragraph 7.06 with respect to record keeping requirement.)

6.73 Financial institutions should, as far as is practicable, in the case of personal accounts ensure that evidence of identity is obtained during the course of an interview with the applicant for business so that the financial institution can verify that the customer is actually the person he claims to be, i.e. the applicant for business should be seen personally and photographic evidence of his identity obtained. Financial institutions should verify that any person whether an applicant for business, purporting to act on behalf of the customer or a potential customer is so authorised and any official judgment, signed mandate or equivalent document should be verified together with the identity of that person.

6.74 In respect of joint personal accounts, the names and addresses of all account holders should be verified.

6.75 The verification procedures necessary to establish the identity of the applicant for business should be the same whatever be the type of account or service that is required (e.g. current, deposit, or other accounts). The name of the member of staff undertaking or responsible for the account opening procedure should be noted on the customer's file together with that of the higher ranking officer who has approved the business relationship.

6.76 Generally, the main objective of financial institutions in the case of entities should be to identify those who have control over the business and the assets.

6.77 The best identification documents are those that are the most difficult to obtain illicitly and to counterfeit. No single form of identification can be fully guaranteed as genuine or representing correct identity. To verify identity beyond reasonable doubt, the identification process will generally need to be cumulative.

6.78 Where a financial institution cannot obtain all the CDD information, it shall not open the account, commence the business relations or perform the transaction and consider making a suspicious transaction report to the FIU.

6.79 Financial institutions should apply CDD requirements to existing customers on the basis of materiality and conduct due diligence on such existing relationships at appropriate times. Examples of when it may be appropriate to do so are when–

(a) a transaction of significance takes place,

(b) customer documentation standards change substantially,

(c) there is a material change in the way that the account is operated,

(d) the institution becomes aware that it lacks sufficient information about an existing customer.

6.80 In the case where financial institutions have doubts about the veracity or adequacy of previously obtained customer identification data, it should terminate the business relationship and consider making a suspicious transaction report to the FIU.

Risk Profiling

6.81 Financial institutions should have policies and procedures in place to conduct due diligence on its customers sufficient to develop customer risk profiles either for particular customers or categories of customers. Financial institutions should use the information obtained during the customer identification and verification process to build an understanding of the customer's profile and behaviour. Examples of information typically collected are (i) the purpose of the relationship or the occasional banking transaction, (ii) the level of assets or the size of transactions of the customer and (iii) the regularity or duration of the relationship. The information collected should be determined by the level of risk associated with the customer's business model and activities as well as the financial products or services requested by the customer. Financial institutions should also carry out additional searches, including carrying out verifiable adverse media searches, when performing the customer risk assessment. The customer risk profile will further determine the level and type of ongoing monitoring and support the bank's decision whether to enter into, continue or terminate, the business relationship.

6.82 When the account opening is the start of a customer relationship, financial institutions should collect the following information on the natural or legal person with a view to developing an initial customer risk profile :

(i) **Natural Persons**

The following key attributes are useful in establishing the first step of the customer's risk profile:

a) occupation, public position held;
b) income;
c) expected use of account : amount, number, type, purpose and frequency of the transactions expected;
d) financial products or services requested by customers.

Potential additional information, on the basis of risks, which may be requested are:

a) name of employer, where applicable;
b) sources of customer's wealth;
c) sources of funds passing through the account;
d) destination of funds passing through the account.

Financial institutions should also consider, on a risk-sensitive basis, whether the information regarding sources of wealth and funds or destination of funds should be corroborated.

(ii) **Legal Persons**

As a minimum, financial institutions may consider the following in establishing the risk profile of a legal person :

a) Nature and purpose of the activities of the legal entity and its legitimacy;
b) Expected use of the account : amount, number, type, purpose and frequency of the transactions expected.

The following potential additional information, on the basis of risk may be requested :

a) Financial situation of the entity;
b) Sources of funds paid into the account and destination of funds passing through the account.

(iii) **Legal Arrangements**

As a minimum, financial institutions should collect the following information :

a) Description of the purpose/activities of the legal arrangement (e.g. in a formal constitution, trust deed);
b) Expected use of the account : amount, number, type, purpose and frequency of the transactions expected.

Potential additional information, on the basis of risks, which may be collected are:

a) Source of funds;
b) Origin and destination of funds passing through the account.

ACCOUNT OPENING FOR PERSONAL CUSTOMERS

6.83 Financial institutions are required to maintain the following identification procedures in respect of individual customers.

FACE-TO-FACE APPLICATIONS

Residents of Mauritius (Personal)

6.84 An individual's true identity comprises his/her name, his/her date of birth, his/her current permanent residential address, the nature of his/her business, his/her normal financial transactions and any agency or beneficiary relationship.

Name

6.85 The name of individuals residing in Mauritius should, during the course of an interview with him, be verified from an original official valid document bearing his/her recent photograph and any of the following may be relied upon:-

- National identity cards
- Current valid passports

- Current valid driving licences.

On the basis of risks involved, any other names used such as marital name, former legal name or alias and the gender of the applicant for business may be collected.

6.86 What constitutes recent, for the purposes of the photograph, will in the circumstances, be decided during the course of the interview with the individual. A material difference in the photograph will lead the inference that the photograph may not be recent.

6.87 Financial institutions should keep a copy of that page which contains the photograph of the applicant for business and ensure that the relevant reference numbers of those documents are recorded.

6.88 Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against the dangers of fraud, it would be appropriate to ensure that applicants for business do not send those identity documents by post to financial institutions.

Address

6.89 In addition to the name, it is important that the current permanent address of the applicant for business be verified as an integral part of identity. Satisfactory evidence of address can be obtained by any of the following, a copy of which should be retained, after the originals have been sighted. The retained copy shall be duly annotated "original sighted". Alternatively, the original document may be scanned and retained in electronic form in such manner that it may be retrieved as and when information is sought on the applicant for business.

- a recent[31] utility bill
- a recent bank or credit card statement
- a recent bank reference
- any other document or documents which either singly or cumulatively establishes, beyond reasonable doubt, the address of the applicant for business.

On the basis of risks involved, the business address, email address and landline or mobile telephone number as well as the residency status of the applicant for business may be collected.

6.90 Financial institutions may effect additional verification of identity by -

- checking a local telephone directory
- checking a current register of electors
- visiting the applicant for business at his/her permanent residential address.
- contacting the customer by telephone, letter or email to confirm the information supplied, after an account has been opened.
- checking references provided by other financial institutions.
- For higher-risk customers, additional sources of information such as requesting for prior bank reference, verification of income sources, funds and wealth, may be considered.

[31] For the purposes of this paragraph 'recent' refers to not more than 3 months.

Non Residents (Personal)

6.91 Regarding applicants for business who are not resident in Mauritius but who make face-to-face contact with a financial institution, they should be required to complete a standard application form which should incorporate the following details :-

- 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 an independent bank reference

6.92 The form, duly filled in must be supported by a clear legible copy of any of the following documents:-

- National Identity Card
- Current valid passports
- Current valid driving licences
- Armed forces identity card

6.93 Financial institutions should keep a copy of that page which contains the recent photograph of the applicant for business, ensure that the relevant reference numbers of the passports or National Identity Card, driving licences or armed forces identity card of those documents are duly recorded.

6.94 In the case of non-residents making face-to-face contact, however, financial institutions should in addition verify identity and current permanent address of the applicant for business with a reputable credit or financial institution in the applicant's normal home country or country of residence.

NON FACE-TO-FACE VERIFICATION

6.95 It is most important that the procedures adopted to confirm identity for non-face-to-face verification be at least as robust as those for face-to-face verification. Examples of non-face to face operations include: business relationships concluded over the Internet or by other means such as through the post; services and transactions over the Internet including trading in securities by retail investors over the Internet or other interactive computer services; use of ATM machines; telephone banking; transmission of instructions or applications via facsimile or similar means and making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid or reloadable or account-linked value cards.

6.96 As with face-to-face verification, the procedures to check identity must serve two purposes:

- they must ensure that a person bearing the name of the applicant exists and lives at the address provided; and

- that the applicant is that person.

6.97 Accordingly, in accepting business from non-face-to-face customers:

- financial institutions should apply equally effective customer identification procedures as for those available for interview; and

- other specific and adequate measures to mitigate the higher risk posed by non-face-to-face verification of customers.

Non-Resident (Personal) Applying from Abroad

6.98 Non-Residents applying from abroad should be required to complete a standard application form, which should incorporate the following details:

- 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)
- passport details, or National Identity Card, driving licence or armed forces identity card details (i.e. number and country of issuance), together with issue date and expiry date
- signature/signatures
- authority to obtain independent verification of any data provided

6.99 The application form, duly filled in, should be accompanied by the following supporting documents :-

- Identity - a clearly legible photocopy of any of the following documents :-

  - National Identity Card
  - Current valid passports
  - Current valid driving licences
  - Armed forces identity card

  duly certified as a true copy by a lawyer, accountant or other professional persons who clearly adds to the copy (by means of a stamp or otherwise) his name, address and profession to aid tracing of the certifier if necessary and which the financial institution believes in good faith to be acceptable to it for the purposes of certifying.

- Address –

  (i) an original or certified copy of utility bill addressed to the applicant at the address from which he, she or they are applying;

  (ii) an original or certified copy of a bank statement addressed to the applicant at the address from which he, she or they are applying.

6.100 The following additional steps may be taken :- developing independent contact with the customer, confirmation by the financial institutions from directory enquiries or from a recognised telephone directory for the locality from which the applicant is applying, containing an entry for the applicant and showing the address from which he, she or they are applying.

6.101 Financial institutions may also rely on other regulated institutions to verify identity of non-resident customers, in accordance with paragraphs 6.83 to 6.91 on "Reliance On Other Regulated Institutions To Verify Identity".

ACCOUNT OPENING FOR LEGAL PERSONS AND ARRANGEMENTS

6.102 Financial institutions should verify the identity of the customer as set out below, using reliable, independent source documents[32], data or information. The measures to verify the information produced should be proportionate to the risk posed by the customer relationship and should allow the financial institution to satisfy itself that it knows the customer's identity. Financial institution may consider the following non-exhaustive list:

- reviewing a copy of the latest financial statements (audited, if available). for established corporate entities;
- undertaking a company search and/or other commercial enquiries to ascertain that the legal person has not been, or is not in the process of being, dissolved, struck off, wound up or terminated;
- utilising an independent information verification process, such as by accessing public corporate registers, private databases or other reliable independent sources (e.g. lawyers, accountants);
- validating the Legal Entity Identifier (LEI), if available, and associated data in the public access service;
- obtaining prior bank references;
- visiting the corporate entity, where practical;
- contacting the corporate entity by telephone, mail or e-mail.

Locally Incorporated Companies

6.103 With regard to locally incorporated companies, financial institutions should verify:-

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

- their directors,
- beneficial owner(s)[33],
- their significant shareholders, and
- their authorised signatories. In the absence of an authorised signatory, the identity of the relevant person who is the senior managing official[34].

32 Reliable documents include, but are not limited to, any valid form of Government Issued Identification such as driver's license, passport or ID card. Identification documents which do not bear photographs or signatures are not considered appropriate evidence of identity.

33 The FATF defines 'beneficial owner' as the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

34 Senior managing official means an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer or who has the capacity to affect significantly the financial standing of a customer.

(ii) the legal existence of the company, namely, the name, legal form, status and proof of incorporation of the legal person as well as its permanent address of the principal place of the legal person's activities, its mailing and registered address.

6.104 The following documents should be obtained and retained in the case of locally incorporated companies :

(i) In respect of employees authorised to open and operate accounts on their behalf, the beneficial owners, their directors and significant shareholders, proof of identity, proof of current permanent address and such other documents as may be required to enable the financial institution to establish their identity;

(ii) A certified copy of the resolution of the Board of Directors or managing body and the power of attorney granted to its employees to open and to operate accounts on their behalf; and

(iii) Official documents which collectively establish the legal existence of that entity, e.g. the original, including an electronic certificate of incorporation issued by the Registrar of Companies of Mauritius, or certified copy of the certificate of incorporation of the company, business registration number, details of its registered office and permanent address of the principal place of business etc.

6.105 Enquiries should be made to confirm :

(i) by 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;

(ii) 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.

6.106 As with personal accounts, 'know your customer' is an ongoing process. If changes to the company structure or ownership occur subsequently, or if suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a company account, further checks should be made to ascertain the reason for the changes.

Foreign Companies

6.107 Where the applicant for business is a foreign company, the same documents as are required for locally incorporated companies should be requested and retained.

6.108 In addition financial institutions should check the veracity of the information provided with a credit or financial institution of good standing in the permanent place of business of the company.

6.109 Financial institutions may also rely on other regulated institutions to verify identity of foreign companies, in accordance with paragraphs 6.83 to 6.91 on "Reliance On Other Regulated Institutions To Verify Identity".

Partnerships /Unincorporated Businesses

6.110 Where the applicant for business is a partnership or an unincorporated business,

(i) the identity of any partner owning or controlling more than 20% of the partnership, controllers of the unincorporated business and their authorised signatories should be verified in accordance with procedures required for the identification of personal applicants for business, and

(ii) the same documents as are required for personal applicants for business should be requested and retained.

6.111 In the case of unincorporated businesses, in addition, the necessary licence given by the competent Authorities for the conduct of such business should be requested and retained and in the case of partnerships, an original or certified copy of the partnership deed obtained.

6.112 Financial institutions should also in cases of doubt make enquiries to confirm the true nature of the business activities to ascertain whether those business activities have a legitimate purpose.

Clubs and Charities

6.113 It is increasingly being recognised that terrorists and terrorist groups are having recourse to clubs and charities for the financing of terrorism.

6.114 Accordingly, in the case of accounts to be opened for clubs or charities, financial institutions should at the very beginning satisfy themselves as to the legitimate purpose of the organisation by requesting a certified copy of the constitution of the club or charity and also in case of doubt by paying a visit to its premises, where practicable, to satisfy themselves as to the true nature of its activities. They may also satisfy themselves by independent confirmation of the purpose of the club or charity.

6.115 The identity of the persons in control of the club or charity should be ascertained, in accordance with the procedures required for personal customers.

6.116 Control of clubs and charities are most likely to change from time to time and the identity of those new controllers of the clubs or charities should be verified as and when financial institutions are advised of any change.

Sociétés

6.117 In the case of sociétés, the original or certified copy of the Acte de Société should be requested and retained.

6.118 For Mauritian sociétés, the financial institution should ensure, by verifying with the Registrar of Companies, that the société continues to exist.

6.119 As regards foreign sociétés the financial institution should obtain a certificate of good standing from them.

6.120 Financial institutions should also, in accordance with the procedures set out for personal customers, verify the identity of those in control of the société, e.g. its administrators and gérants etc. and retain the same relevant documents as are required for personal customers accordingly.

Cooperatives

6.121 Where cooperatives are applicants for accounts, those persons, quite often the board members as well as executives and account signatories, exercising control or significant influence over the organisation's assets should be considered the beneficial owners and therefore identified and verified, in addition to the normal identification documents establishing the legal existence of the Cooperative.

Trusts

6.122 Financial institutions should exercise particular caution with respect to trusts, given the common perception that trusts are often misused for laundering the proceeds of crime and hiding terrorist funds.

6.123 In the case of trusts, the following information should as a minimum be required for identification purposes: name of trust, proof of existence, address, country of establishment, nature, purpose, objects, names of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership). Financial institutions should collect further information such as certified extracts of the original trust deed or probate copy of a will creating the trust, documentary evidence pertaining to the appointment of the current trustees and the nature and purpose of the trust, as well as documentary evidence as are required for personal customers on the identity of the current trustees, the settlor and/or beneficial owner of the funds and of any controller or similar person having power to appoint or remove the trustees should be requested and retained.

6.124 Financial institutions should also obtain written confirmation from the trustees that they are themselves aware of the true identity of the underlying principals i.e. the settlors/named beneficiaries, and that there are no anonymous principals.

6.125 Financial institutions should also gather the maximum information on the trust's operations prior to opening of the account and should also monitor on a regular basis the inflows and outflows in line with the given business plan.

‘Client Accounts’ Opened By Professional Intermediaries

6.126 Professional intermediaries, such as stockbrokers, fund managers, law practitioners, accountants, estate agents and other professional intermediaries, frequently hold funds on behalf of their clients in ‘client accounts’ opened with financial institutions. Such accounts may be opened on behalf of either a single client or for many clients.

6.127 When a professional intermediary opens a customer account on behalf of a single customer, the financial institution must identify the customer.

6.128 Where funds held by the professional intermediary are not co-mingled but “sub-accounts” are established which can be attributed to each beneficial owner, the financial institution must identify all beneficial owners of the account held by the professional intermediary.

6.129 Where the funds are co-mingled, the financial institution should look through to the beneficial owners. However, where the professional intermediary is subject to due diligence standards in respect of its customer base that are equivalent to those applying to the financial institution itself, the latter may not need to look beyond the intermediary and may obtain an undertaking from it that it has verified the identity of its clients and secured particulars of the identity of those clients.

6.130 Where the professional intermediary is subject to due diligence as stated in paragraph 6.81C above and an account is opened for an open or closed-end investment company, unit trust or limited partnership that is subject to customer due diligence requirements which are equivalent to those applying to the financial institution itself, the latter should treat this investment vehicle as its customer and take steps to identify:

i. the fund itself;
ii. its directors or any controlling board where it is a company;
iii. its trustee where it is a unit trust;
iv. its managing (general) partner where it is a limited partnership;
v. account signatories; and
vi. any other person who has control over the relationship e.g. fund administrator or manager.

6.131 Where other investment vehicles are involved, the same steps should be taken as in paragraph 6.81D where it is appropriate to do so. In addition, in cases when no equivalent due diligence standards apply to the investment vehicle, all reasonable steps should be taken to verify the identity of the beneficial owners of the funds and of those who have control of the funds.

Retirement benefit programmes

6.132 Where an occupational pension programme, employee benefit trust or share option plan is an applicant for business, the trustee and any other person who has control over the relationship (e.g. administrator, programme manager or account signatories) can be considered as beneficial owners. The financial institution should conduct, in accordance with the procedures laid down in Paragraphs 6.01 to 6.80 as applicable, due diligence on the applicant.

Foundations

6.133 A foundation may be established in Mauritius or elsewhere and registered in Mauritius in accordance with the Foundations Act 2012. A foundation will not have legal personality unless it is registered and has been issued with a certificate of registration by the Registrar of Companies who also cumulates the function of Registrar of Foundations.

6.134 A foundation may be charitable or non-charitable, or both.

6.135 When verifying the identity of a foundation, the financial institution must, in line with guidance provided for individuals and legal bodies, verify:

With respect to the foundation:

(a) its name;
(b) its date of registration with the Registrar of Foundations;
(c) its date and country of incorporation;
(d) its official identification number;
(e) its business address;
(f) its principal place of business and operations (if different),

by using the following verification methods, namely, the Charter (or equivalent) of the foundation, search at the Registrar of Foundations, the latest audited financial statements and independent data sources.

With respect to the persons who are concerned with the foundation :

(g) the identity of, *inter alia*, (i) the council members, specially those who have authority to operate a business relationship or to give instructions concerning the use or transfer of funds or assets, (ii) the founder, (iii) the executor, (iv) the protector, (v) the beneficiary, and (vi) the administrator.

6.136 Where a foundation is a charitable foundation, the financial institution must ensure that it adheres to the guidance issued for 'Clubs and Charities' at paragraphs 6.70 to 6.73 above.

THIRD PARTY RELIANCE

6.137 Although the ultimate responsibility for verifying the identity and address of customers always lies with the financial institution, it is recognised that to avoid duplication, financial institutions may rely on other eligible or group introducers to verify the identity of applicants for business. Financial institutions should however have clear policies and procedures on whether and when it is acceptable and prudent to rely on other eligible or group introducers.

STATUTORY REQUIREMENTS

6.138 Regulation 21 of the FIAML Regulation empowers a financial institution to rely on a third party to introduce business or to perform the CDD measures under regulation 3(a), (c) and (d).

6.139 Where a financial institution relies on a third party to introduce business or perform the CDD measures set out under above, the financial institution shall –

(a) obtain immediately the necessary information required under regulation 3(a), (c) and (d);

(b) take steps to satisfy himself that copies of identification data and other relevant documentation related to CDD requirements shall be made available from the third party upon request without delay;

(c) satisfy himself that the third party is regulated and supervised or monitored for the purposes of combating money laundering and terrorism financing, and has measures in place for compliance with CDD and record keeping requirements in line with the FIAMLA and the FIAML Regulations.

6.140 A financial institution shall not rely on a third party based in a high risk country.

6.141 A financial institution may rely on a third party that is part of the same financial group, where –

(a) the group applies CDD and record-keeping requirements and programmes against money laundering and terrorism financing, in accordance with the FIAMLA and the FIAML Regulations;

(b) the implementation of those CDD and record-keeping requirements and programmes against money laundering and terrorism financing is supervised at a group level by a competent authority; and

(c) any higher country risk is adequately mitigated by the group's policies to combat money laundering and terrorism financing.

6.142 Where a financial institution relies on customer identification documentation in the possession of an eligible or group introducer, it is not required to retain copies of the customer identification documentation in its own records where the financial institution is satisfied that he may obtain that customer identification documentation from the eligible introducer or group introducer upon request without delay. The financial institution should, in its procedures and policies, document the reliance and should establish adequate controls and review procedures for such a relationship and should identify and mitigate any additional risk posed by reliance on multiple parties and its risk assessment should identify reliance on third parties as a potential risk factor.

6.143 In addition, financial institutions should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above. For that purpose, the financial institution should obtain all the CDD information and documents from the eligible or group introducer and assess due diligence conducted, including screening against local databases to ensure compliance with local regulatory requirements.

6.144 Financial institutions must request group or eligible introducers to provide them with a duly completed Group Introducers Certificate or Eligible Introducers Certificate as the case may be. The financial institution must reach an agreement with the introducer that it will be permitted at any stage to verify the due diligence undertaken by the introducer. Financial institutions should consider terminating reliance on entities that do not apply adequate CDD on their customers and give due consideration to adverse public information about the entity.

TRADE BASED MONEY LAUNDERING/FINANCING OF TERRORISM

6.145 Trade-based money laundering and terrorist financing refers to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origins or finance their activities. Examples of how trade-based money laundering and terrorist financing may be carried out include, but are not limited to: misrepresentation of the price, quantity or quality of imports or exports; and money laundering through fictitious trade activities and/or through front companies. The most basic schemes involve fraudulent trade practices such as: over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipments of goods and services, and falsely describing goods and services. Particular attention should be paid by financial institutions when undertaking transactions on behalf of customers involved in free trade activities.

6.146 Financial institutions shall accordingly, have adequate systems to properly manage risks associated with trade finance activities. Such systems shall depend on the financial institution's size, complexity, location and types of customer relationship and shall effectively enable a financial institution to identify and monitor its trade finance portfolio for suspicious or unusual activities, in particular those that pose a higher risk for money laundering.

6.147 Financial institutions shall also have their trade finance accounts regularly sample-tested with the view to verifying whether they are meeting their customer due diligence, record keeping, monitoring and reporting obligations.

6.148 Financial institutions may, for guidance, refer to the FATF Report on "Money Laundering vulnerabilities of Free Trade Zones" issued by the FATF in March 2010 and to the "Best Practices Paper on Trade Based Money Laundering" and to the report on "Trade Based Money Laundering" issued by the FATF in June 2008 and June 2006 respectively and available on the website of the FATF at http://fatf-gafi.org.

CORRESPONDENT SERVICES

6.149 Correspondent services are the provision of services by one financial institution to another financial institution. Used by financial institutions throughout the world, correspondent services enable financial institutions to conduct business that the financial institutions do not offer directly. Particular care should be taken where correspondent services involve jurisdictions where the correspondent financial institutions have no physical presence. If financial institutions fail to apply an appropriate level of due diligence to such services, they expose themselves to a range of risks and may find themselves holding and/or transmitting money linked to terrorism, corruption, fraud or other illegal activity.

STATUTORY REQUIREMENT

6.150 Regulation 16 of the FIAML Regulations provides as follows with respect to cross-border correspondent banking –

(1) In relation to cross border correspondent banking and other similar relationships, a financial institution shall, in addition to the CDD measures –

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business;

(b) determine from publicly available information the reputation of the respondent institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(c) assess the respondent institution's anti-money laundering and combating the financing of terrorism controls;

(d) obtain approval from senior management before establishing new correspondent relationships;

(e) clearly understand and document the respective responsibilities of each institution.

(2) With respect to payable-through accounts, a financial institution shall be satisfied that the respondent bank –

(a) has performed CDD obligations on its customers having direct access to accounts of the correspondent bank; and

(b) is able to provide relevant CDD information upon request to the correspondent bank.

6.151 Financial institutions should -

(i) gather sufficient information about their correspondents to understand fully the nature of the correspondent's business. Factors to consider include: information about the correspondent's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the identity of any third party entities that use the correspondent services;

(ii) determine from public available information the reputation of the institution and quality of the institution's regulation and supervision, including whether it has been subject to money laundering or terrorist financing investigation or regulatory action;

(iii) assess the institution's AML/CFT controls and ascertain that they are adequate and effective and establish correspondent relationships with foreign financial institutions only if financial institutions are satisfied that the foreign financial institutions are effectively supervised by the relevant authorities and have effective customer acceptance and KYC policies;

(iv) obtain approval from senior management before establishing new correspondent relationships.

(v) document the respective AML/CFT responsibilities of each institution. It is not necessary that the two financial institutions always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures.

(vi) where a correspondent relationship involves the maintenance of "payable-through accounts", be satisfied that –

(a) the respondent financial institution has performed all the normal CDD obligations set out in this Guideline on those of its customers that have direct access to the accounts of the correspondent financial institution; and

(b) the respondent financial institution is able to provide relevant customer identification data upon request to the correspondent financial institution.

6.152 In particular, financial institutions should refuse to enter into or continue a correspondent relationship with a financial institution incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. it may involve shell financial institution). They should also satisfy themselves that the respondent financial institutions do not permit their accounts to be used by shell banks[35]. Financial institutions should pay particular attention when continuing relationships with correspondents or establishing relationships and transactions with persons located in jurisdictions that have poor KYC standards or have been identified as being "non-cooperative" in the fight against anti-money laundering or as having deficiencies in their AML/CFT regime. Financial institutions should establish that their correspondents have due diligence standards as set out in this Guideline, and employ enhanced due diligence procedures with respect to transactions carried out. Where a financial institution finds that those transactions have no apparent economic or visible lawful purpose, it must as far as possible examine the background and purpose of such transactions and keep its findings in writing to be made available to the auditors and to the Bank upon request. Senior management should be regularly informed of high-risk correspondent banking relationship and how they are monitored.

6.153 Financial institutions should be particularly alert to the risk that correspondent services might be used directly by third parties to transact business on their own behalf. Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out for introduced business.

SHELL BANK

6.154 Regulation 17(1) of the FIAML Regulations requires financial institutions not to enter into or continue a business relationship or occasional transaction with a shell bank.

6.155 A financial institution shall take adequate measures to ensure that the financial institution does not enter into or continue a business relationship or occasional transaction with a respondent institution that permits its accounts to be used by a shell bank.

POLITICALLY EXPOSED PERSONS

6.156 The FIAML Regulations define "politically exposed person" or "PEP" as follows —

(a) means a foreign PEP, a domestic PEP and an international organisation PEP; and

(b) for the purposes of the definition —

"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

[35] "shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision;

government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

"foreign PEPs" means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or 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;

"international organisation PEP" means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions, 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 persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

6.157 Regulation 15 of the FIAML Regulations imposes the following requirements with respect to PEP.

6.158 A financial institution shall in relation to a foreign PEP, whether as customer or beneficial owner, in addition to performing the CDD measures under the FIAML Regulations –

(a) put in place and maintain appropriate risk management systems to determine whether the customer or beneficial owner is a PEP;

(b) obtain senior management approval before establishing or continuing, for existing customers, such business relationships;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

(d) conduct enhanced ongoing monitoring on that relationship.

6.159 A financial institution shall, in relation to domestic PEPs or an international organisation PEP, in addition to performing the CDD measures required under the FIAML Regulations –

(a) take reasonable measures to determine whether a customer or the beneficial owner is such a person; and

(b) in cases when there is higher risk business relationship with a domestic PEP, adopt the measures in paragraphs 15(1)(b) to (d) of the FIAML Regulation.

6.160 A financial institution shall apply the relevant requirements of paragraphs 6.158 and 6.159 to family members or close associates of all types of PEP, as set out in the Annex to this Chapter.

6.161 Business relationships with individuals holding important public positions and with persons or entities clearly related to them may expose a financial institution to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") be it local or foreign, are individuals who are or have been entrusted with prominent public functions, including heads

of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations, important political party officials, their family members and their close associates. In the case of entities relating to local PEPs, these would comprise entities that are 20 per cent or more owned or controlled by those local PEPs. The possibility exists that such persons may abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc. The measures applicable to a PEP are also applicable to family members or persons known to be close associates of PEPs as well as persons who have been entrusted with a prominent function by an international organisation.

6.162 A list of PEPs is given in the Annex to this Chapter. Family members of PEPs are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership and shall comprise their spouses, any partner considered by national law as being equivalent to a spouse and their children, the children and their spouses, or persons considered to be equivalent to a spouse, the parents of a PEP. Close associates are individuals who are closely connected to a PEP, either socially or professionally and include (i) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations with a PEP; and (ii) natural persons who have sole beneficial ownership of a legal entity or legal arrangement, which is known to have been set up for the de facto benefit of a PEP. International organisation PEPs are persons who are or have been entrusted with a prominent function by an international organisation and refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.

6.163 Accepting and managing funds from local or foreign corrupt PEPs will severely damage the financial institution's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. Under certain circumstances, the financial institution and/or their officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds were destined for the financing of terrorism or stemmed from corruption or other crimes.

6.164 In Mauritius corruption is a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer). There is a compelling need for a financial institution considering a relationship with a person, be it local or foreign, whom it considers to be a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

6.165 Financial institutions should gather sufficient information from a new customer, including information on the beneficial owner, check publicly available information or access commercial electronic databases, in order to establish whether or not the customer or the beneficial owner is a PEP. Financial institutions should also take reasonable measures to establish the source of wealth and the source of funds of the customer and beneficial owners identified as PEPs. Financial institutions are encouraged to consider the ongoing PEP status of their customers on a case-by-case basis using a risk-based approach. If the risk is low, financial institutions may consider declassifying the relationship, but only after careful consideration of continuing anti-money laundering risks and approval by senior management.

6.166 Financial institutions should put in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner is a PEP. It can reduce risk by conducting detailed due diligence at the out-set of the relationship including requiring a declaration of beneficial ownership and enhanced ongoing monitoring where a business relationship has been established with a PEP.

6.167 All financial institutions should assess which countries, with which they have financial relationships, are most vulnerable to corruption. One source of information is the Transparency International Corruption Perceptions Index at www.transparency.org. Financial institutions which are part of an international group might also use the group network as another source of information.

6.168 Where financial institutions do have business in countries vulnerable to corruption, they should establish who are the senior political figures in that country and, should seek to determine whether or not their customer has any connections with such individuals (for example they are immediate family or close associates). Financial institutions should note the risk that individuals may acquire such connections after the business relationship has been established.

6.169 In particular detailed due diligence should include:

- Close scrutiny of any complex structures (for example, involving companies, trusts and multiple jurisdictions) so as to establish that there is a clear and legitimate reason for using such structures bearing in mind that most legitimate political figures would expect their personal affairs to be undertaken in a more than usually open manner rather than the reverse.

- Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship – again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis.

- The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated.

- An approval at senior management or board level of the decision to commence the business relationship and to continue the business relationship where the customer has been accepted and the customer or beneficial owner is subsequently found to be or subsequently becomes a PEP.

- Regular review by senior management using a risk-based approach, at least yearly, with the results of the review duly documented. Over the course of a business relationship with a PEP, ongoing monitoring procedures may reveal changes to the profile and activity. The PEP may have been promoted or elected to a more senior position, engaged in litigation, or made transactions deviated from the norm. Considered separately, the activities, transactions or profile changes may not be sufficient to raise "red flags." Implementing a periodic review of PEP customers on a risk-based approach, and at least yearly, would help to overcome the approach in which decisions are made transaction-by-transaction, activity-by-activity which would enhance the oversight of the PEPs customer relationships by senior management.

- Close scrutiny of any unusual features, such as very large transactions, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown financial institutions in secrecy jurisdictions and regular transactions involving sums just below a typical reporting amount.

6.170 Where a politically exposed person is no longer entrusted with a prominent public function either domestically or abroad, or with a prominent public function by an international

organisation, financial institutions should, for at least 12 months, take into account the continuing risk posed by that person and apply appropriate and risk sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons. The financial institution should document the reasons justifying the decision to declassify the customer as a PEP and make these reasons available to the Bank upon request.

WIRE TRANSFER TRANSACTIONS

STATUTORY REQUIREMENT

6.171 "wire transfer" means any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

6.172 Regulation 20 of the FIAML Regulations requires financial institution top ensure that all cross border wire transfers are always accompanied by –

(a) required and accurate originator information, which includes –

(i) the name of the originator;
(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and (iii) the originator's address, national identity number, or customer identification number, and date and place of birth;

(b) the following required beneficiary information –

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

6.173 Where several individual cross border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries –

(a) the batch file shall contain required and accurate originator information as set out in paragraph (1)(a), and full beneficiary information, that is fully traceable within the beneficiary country; and

(b) the relevant person shall include the originator's account number or unique transaction reference number.

6.174 For domestic wire transfers, the ordering relevant person shall ensure that the information accompanying the wire transfer shall include originator information as specified in paragraph (1).

6.175 The ordering relevant person shall maintain all originator and beneficiary information collected, in accordance with section 17F of the Act and regulation 14.

6.176 The ordering relevant person shall not execute the wire transfer where it does not comply with the requirements specified in paragraphs (1) to (4).

6.177 For cross border wire transfers, an intermediary financial institution shall ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

6.178 Where technical limitations prevent the required originator or beneficiary information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall keep a record, for at least 7 years, of all the information received from the ordering financial institution or another intermediary financial institution.

6.179 Intermediary financial institutions shall take reasonable measures, which are consistent with straight-through processing, to identify cross border wire transfers that lack required originator information or required beneficiary information.

6.180 Intermediary financial institutions shall have risk-based policies and procedures for determining –

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
(b) the appropriate follow-up action.

6.181 Beneficiary financial institutions shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross border wire transfers that lack required originator information or required beneficiary information.

6.182 A beneficiary financial institution shall verify the identity of the beneficiary, where the identity has not been previously verified, and maintain this information in accordance with section 17F of the Act and regulation 14.

6.183 A beneficiary financial institution shall have risk-based policies and procedures for determining –

(a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) the appropriate follow-up action.

6.184 Investigations of major money laundering cases over the last few years have shown that criminals make extensive use of electronic payment and message systems. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigations. In addition, investigations become even more difficult to pursue if the identity of the originator is not clearly shown in an electronic payment message instruction.

6.185 To ensure that wire transfer systems are not used by criminals as a means to break the audit trail, where a financial institution makes a payment on behalf of its customer, accurate and meaningful originator[36] information (name, residential address[37] and any account number or

[36] Where the originator is acting on behalf of others (e.g. as nominee, agent, or trustee), then it is the name, address, and account number of the nominee, agent, trustee, etc. that should be included. The financial institution making the payment should have on file the name and address of underlying principals.

[37] Registered office address where an originator is a company.

reference of the originator) should be included on all funds transfers and related messages and should remain with the transfer through the payment chain until it reaches its final destination. This information is particularly important for international transfers on behalf of individual customers to ensure that the source of funds can be identified in the event of an investigation in the receiving jurisdiction.

6.186 When the financial institutions act as the ordering institution, -

(1) All domestic or cross-border wire transfers should always be accompanied by the following:

(a) required and accurate originator information:

(i) the name of the originator;

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

(iii) the originator's address, or national identity number, or customer identification number, or date and place of birth.

(b) required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(2) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file should contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country. The financial institution should also include the originator's account number or unique transaction reference number.

(2) Cross-border wire transfers of less than USD/EUR 1,000 should be accompanied by the following :

(a) required originator information:

(i) the name of the originator; and

(ii) the originator account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(b) required beneficiary information:

(i) the name of the beneficiary; and

(ii) the beneficiary account number where such an account is used to process the transaction or, in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

(3) The above information need not be verified for accuracy. However, the financial institution should verify the information where there is a suspicion of money laundering or terrorist financing.

(4) For domestic wire transfers, the financial should ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers.

(5) The financial institution should not execute the wire transfer if it does not comply with the requirements specified above.

6.187 Financial institutions should not omit, delete or alter information in payment messages, for the purpose of avoiding detection of that information by another financial institution in the payment process.

6.188 Financial institutions should monitor payment messages to and from higher risk countries or jurisdictions, as well as transactions with higher risk countries or jurisdictions and suspend or reject payment messages or transactions with sanctioned parties or countries or jurisdictions.

6.189 Where name screening checks confirm that the wire transfer originator or wire transfer beneficiary is a terrorist or terrorist entity, the requirement for the financial institution to block or reject assets of these terrorists or terrorist entities cannot be risk-based.

6.190 Where there are positive hits arising from name screening checks, they should be escalated to the AML/CFT compliance function. The decision to approve or reject the receipt or release of the wire transfer should be made at an appropriate level and documented.

6.191 Where funds transfers are processed as an intermediary, e.g. where financial institution "B" is instructed by financial institution "A" to pay funds to an account held by a beneficiary at financial institution "C", the originator and beneficiary data provided by financial institution "A" should be preserved and, wherever possible, included in the message generated by financial institution "B".

6.192 Where a cross-border wire transfer, regardless of amount, is a cover payment (e.g. MT202COV payments), ordering institutions should ensure that the payment message of the cover payment sent to the intermediary institution contain information of the wire transfer originator and wire transfer beneficiary. The information included in the payment message of the cover payment should be identical to that contained in the cross-border wire transfer message sent directly to the beneficiary institution.

6.193 An intermediary institution that receives and transmits a cover payment should ensure that the relevant fields for storing originator and beneficiary information in the payment message of the cover payment are duly completed. In addition, such intermediary institutions should ensure that the wire transfer originator and wire transfer beneficiary information in the payment

message of the cover payment is complete. The intermediary institution should also screen the names of the wire transfer originator and wire transfer beneficiary.

6.194 Financial institutions should conduct enhanced scrutiny of, and monitor for suspicious activity, incoming funds transfers which do not contain complete originator information. This will involve examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (origin in a country known to harbour terrorists or terrorist organisations, for example). Where an incoming wire transfer is not accompanied by complete wire transfer originator information and wire transfer beneficiary, a beneficiary institution should request the information from the ordering institution. Financial institutions should consider rejecting incoming wire transfers or terminating business relations with overseas ordering institutions that fail to provide originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transaction is suspicious and to consider, as appropriate, whether they are thus required to be reported to the FIU. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet the above requirements.

ANNEX

POLITICALLY EXPOSED PERSONS

'natural persons who are or have been entrusted with prominent public functions' shall include the following:

Domestic PEPs

1. President/Vice President of Republic of Mauritius
2. All members of the National Assembly and the Speaker
3. Chief Judge and Senior Puisne Judge
4. Director of Public Prosecutions
5. Attorney General
6. Commissioner of Police/Prison
7. Leaders and Senior Office Bearers of major Political Parties
8. Members of Rodrigues Regional Assembly
9. Governor/Deputy Governors of the Central Bank
10. Chairman and Chief Executive Officers of Parastatal Organisations, Independent Bodies and State- Owned Enterprises
11. Commissioners of Various Government Bodies
12. Advisor/ Counsellor to Heads of States and Ministers
13. Head of Mauritian Embassies abroad, Consulates and Diplomats
14. Mayors and President of District Councils
15. Head of National Secret Services

Foreign PEPs

1. Heads of state, heads of government, ministers and deputy or assistant minister
2. Members of parliament or of similar legislative bodies
3. Members of the governing bodies of political parties
4. Members of supreme courts, constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances
5. Members of courts of auditors or of the boards of central banks
6. Ambassadors, chargés d'affaires and high-ranking officers in the armed forces
7. Members of the administrative, management or supervisory bodies of state-owned enterprises
8. Directors, deputy directors and members of the board or equivalent function of an international organisation.

7 ONGOING MONITORING

INTRODUCTION

7.1 Ongoing monitoring is an essential aspect of effective KYC procedures. Every financial institution should conduct ongoing monitoring to, inter alia:

a. detect suspicious transactions that are required to be reported to the FIU;

b. keep client identification, beneficial ownership information, and the purpose and intended nature of the business relationship record up to date;

c. re-assess the risk associated with a business relationship based on their transactions and activities; and

d. determine whether the transactions or activities are consistent with the information and risk assessment of that client.

7.2 Financial institutions have an on-going duty to keep CDD information of their customers up to date. In addition, financial institutions should adopt ongoing monitoring measures commensurate with the ML/TF risks associated with their customers, products/services/ transactions, delivery channel and geographic area.

7.3 Failure to adequately monitor customers' activities could expose a financial institution to potential abuse by criminals and may call into question the adequacy of systems and controls, or the prudence and integrity or fitness and properness of the management of the financial institution.

7.4 Additionally, failure to adequately monitor customers' activities would constitute a breach of the requirements under the FIAMLA and the Banking Act.

STATUTORY REQUIREMENTS

Financial Intelligence and Anti-Money Laundering Regulations 2018

7.5 Regulation 3(e) of the Financial Intelligence and Anti-Money Laundering Regulations 2018 (FIAML Regulations) requires financial institutions to conduct ongoing monitoring of all its business relationships.

7.6 The Regulation further provides that ongoing monitoring of business relationships should include

(i) scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer; and

(ii) ensuring that documents data or information collected under the CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

7.7 Regulation 12(1) also stipulates that financial institutions should perform enhanced CDD, amongst others, where higher risk of money laundering or terrorist financing is identified or in the event of any unusual or suspicious activity.

7.8 Pursuant to Regulation 12(2), the enhanced CDD measures that may be applied for higher risk business relationships include conducting enhanced monitoring of the business relationship, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

7.9 Regulation 15 requires that financial institutions conduct enhanced ongoing monitoring in addition to performing CDD measures, in relation to a foreign PEP whether as customer or beneficial owner.

7.10 Under Regulation 14, financial institutions are required to keep and maintain all necessary records relating to transactions in such form which enables the prompt reconstruction of each individual transaction.

7.11 Regulation 12 further provides that where a financial institution is unable to perform enhanced CDD as required under the FIAML Regulations, it should terminate the business relationship and file a suspicious transaction report in terms of section 14 of the FIAMLA.

GENERAL GUIDANCE

7.12 In terms of Chapter 4 of this Guideline, financial instructions should maintain a risk rating framework and conduct a risk assessment of their customers to establish their risk profiles. The principle of proportionality to the risk assessment of the customers/product/services/transactions/geographic area/delivery channel[38] will yield varying levels of ongoing monitoring requirements.

7.13 Once a business relationship has been risk rated, ongoing monitoring measures that are commensurate with the level of risk associated with the relationship must be applied. Business relationships identified as posing a low risk would require less frequent monitoring whereas those in the high-risk category would require enhanced due diligence measures. In terms of regulation 12(2) of the FIAML Regulations, enhanced diligence measures include conducting enhanced monitoring of the business relationship, by increasing the number and frequency of controls applied, and selecting patterns of transactions that need further examination. Therefore, the frequency of ongoing monitoring activities will be determined by the risk assessment.

7.14 In line with regulation 3 of the FIAML Regulations, financial institutions are expected to develop clear policies and procedures, especially on the frequency of periodic review or what constitutes a trigger event, to ensure continuous monitoring of their business relationships in the following aspects:

i) Ongoing Monitoring of Accounts; i.e. ensuring that documents data or information collected under the CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers; and

[38] Financial institutions should refer to the National Risk Assessment Report of Mauritius when conducting their risk assessment. The Report can be found at http://financialservices.govmu.org/English/Documents/2019/NRA%20Report/Public%20Report%202019-compressed.pdf.

ii) Monitoring of Transactions; i.e. scrutiny of transactions undertaken throughout the course of a business relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with the knowledge of the customer and the business and risk profile of the customer.

Ongoing monitoring of accounts

7.15 In terms of Chapter 6, every financial institution is expected to periodically review CDD information in respect of all customers and ensure that it is accurate, relevant, and up to date.

7.16 To be most effective, resources of financial institutions should be targeted towards monitoring those relationships which present a higher risk of money laundering and terrorism financing.

7.17 During periodic reviews, financial institutions are not required to re-verify the identities that have been previously verified (unless there is a trigger event or there are doubts arise as to the veracity or adequacy of the evidence previously obtained for the purposes of customer identification). However, it is expected that identification information must be accurate, relevant and up to date. Where identification information previously obtained has changed, (such as a name or residential address), the revised information must be obtained and verification of this information should be sought on a risk based approach. Consideration should be given as to whether this change may impact on the customer risk assessment undertaken under chapter 4 of this Guideline.

7.18 Relevant persons must ensure that any updated CDD information obtained through meetings, discussions, or other methods of communication with the customer is recorded and retained with the customer's records. Financial institutions should ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

7.19 Periodic review of customer's account should be commensurate to the risk rating assigned to it and should not, in any event, be more than one year for high risk customers or accounts.

7.20 With regard to existing CDD records of a dormant customer. while it is not necessary to regularly review the records, a financial institution should conduct a review upon reactivation of the relationship. The financial institution should define clearly what constitutes a dormant customer in its policies and procedures.

Monitoring of Transactions

7.21 Financial institutions should have systems in place to detect complex, unusual or suspicious transactions or patterns of activity for all accounts. They should establish and maintain adequate systems and processes to monitor transactions. The design, degree of automation and sophistication of transaction monitoring systems and processes should be developed appropriately having regard to the following factors:

- the size and complexity of its business;
- the ML/TF risks arising from its business;
- the nature of its systems and controls;
- the monitoring procedures that already exist to satisfy other business needs; and

- the nature of the products and services provided (which includes the means of delivery or communication).

7.22 Financial institutions should conduct transaction monitoring in relation to all business relationships following a risk-based-approach. The extent of monitoring, i.e. frequency and intensity of monitoring should be commensurate with the risk profile of the customer. Where the risks are high, the financial institution should conduct enhanced transaction monitoring, while in low risk situations, the financial institution may consider reducing the extent of monitoring.

7.23 In establishing scenarios for identifying such activity, financial institutions should consider the customer's risk profile developed as a result of the financial institution's risk assessment, information collected during its CDD efforts and other information obtained from law enforcement and other authorities in its jurisdiction.

7.24 Using CDD information, financial institutions should be able to identify transactions that do not appear to make economic sense, that involve large cash deposits or that are not consistent with the customer's normal and expected transactions.

7.25 Certain types of transactions should alert financial institutions to the possibility that the customer is conducting complex, unusual or suspicious activities. Therefore, in addition, the following areas should also be monitored :

- the nature and type of the transaction (transactions that do not appear to make economic or commercial sense)

- the frequency and nature of a series or pattern of transactions (transactions that involve small cash deposits made frequently or transactions that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer);

- the amount of any transactions, paying particular attention to particularly large transactions (very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account);

- the geographical origin/destination of a transaction (jurisdictions that pose a higher risk to their particular sector or customer type

- the parties concerned with a view to ensuring that there are no payments to or from a person on a sanctions list or relating to any restricted activities;

- transactions made by customers which pose higher money laundering and terrorism financing risks, such as High Net Worth Individuals, Politically Exposed Persons, cash intensive businesses, amongst others.

7.26 Where a financial institution conducts enquiries and obtains what it considers to be a satisfactory explanation of the transaction or activity, it may conclude that there are no grounds for suspicion, and therefore take no further action. Even if no suspicion is identified, the financial institution should consider updating the customer risk profile based on any relevant information obtained.

7.27 Where a financial institution cannot obtain a satisfactory explanation regarding the transaction or activity, it may conclude that there are grounds for suspicion and the procedures set out in Chapter 10 should be followed.

Monitoring systems

7.28 Financial institutions should ensure that -

a. *Monitoring activities take into account the purpose of the business relationships and the intended source of funds*. When conducting on-going monitoring, financial institutions should refer to the purpose of the business relationship and intended source of funds that was documented at the beginning of the business relationship to ensure that activities correspond to what was stated by the client.

b. *Unjustified or abnormal changes in the activities of your client are documented* – The financial institution should flag changes in activities that is contrary to normal transaction patterns or client activities. A process is in place to elevate concerns as necessary.

c. *Monitoring parameters are established* – Financial institutions should set business limits or indicators regarding transactions that would trigger early warning signals and require mandatory review. These indicators should be informed by the ML/TF risks of the financial institution's business. Operational documents must demonstrate that the policy is effectively applied.

d. *Analysis of background and purpose of transaction is documented.* Also, financial institutions should analyse the background and purpose of complex and unusually large transactions, and make a written record of the result of the analysis.

7.29 Financial institutions should have access to updated, comprehensive and accurate customer profiles and records to be able to effectively monitor and identify suspicious activities. In this respect, they should have in place a monitoring system that is adequate with respect to its size, its activities and complexity as well as the risks present in the financial institution to provide both business units and risk and compliance officers with timely information needed to identify, analyse and effectively monitor customer accounts.

7.30 When an IT system is used, it should cover all accounts of the financial institution's customers and transactions for the benefit of, or by order of, those customers.

7.31 The monitoring system of a financial institution should be robust enough to immediately detect any material changes in the transactional profile of any customer (such as parameter breaches), across any financial institution's network of locations, to enable the business line and the MLRO to take appropriate and expeditious action if warranted.

7.32 The monitoring system should also allow the financial institution to gain a centralised knowledge of information to initiate a trend analysis if necessary on any client, manage client information access and facilitate record retention.

7.33 Financial institutions should ensure that they have adequate management information systems to provide managers and MLROs with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed in the AML/CFT area include transactions made through an account that are unusual.

7.34 Where the basis of the business relationship changes significantly, the financial institution should undertake a new assessment to reassess the customer's risk profile to ensure that the revised risk and basis of the relationship is fully understood, this could include further CDD procedures where necessary.

8 TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING

A. THE UNITED NATIONS (FINANCIAL PROHIBITIONS, ARMS EMBARGO AND TRAVEL BAN) SANCTIONS ACT 2019

8.1 The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the 'Act') enables the Government of Mauritius to implement targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the financing of terrorism and proliferation of weapons of mass destruction.

STATUTORY REQUIREMENTS

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

8.2 Section 23(1) of United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 provides that subject to this Act, no person shall deal with the funds or other assets of a designated party[39] or listed party[40], including –

(a) all funds or other assets[41] that are owned or controlled by the designated party or listed party, and not just those that can be tied to –

(i) a particular terrorist act, plot or threat;

(ii) a particular act, plot or threat of proliferation;

(b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated party or listed party;

(c) funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated party of listed party, and

(d) funds or other assets of a party acting on behalf of, or at the direction of, the designated party or listed party.

---

[39] "designated party" means a party declared as such by the Secretary for Home Affairs pursuant to section 9 or 10

[40] "listed party" means any party listed by or under the authority of the United Nations Security Council

[41] "funds or other assets" means –

(a) any assets, including, but not limited to, financial assets, economic resources and property of every kind, whether tangible, intangible, movable or immovable, however acquired;

(b) legal documents or instruments in any form –

(i) including electronic or digital, evidencing title to, or interest in, such funds or other assets; and

(ii) including, but not limited to, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit;

(c) any interest, dividends or other income on or value accruing from or generated by such funds or other assets, virtual or digital currencies, including cryptocurrencies;

(d) any other assets which potentially may be used to obtain funds, goods or services

8.3 Section 23(2) also stipulates that where a prohibition is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition, provided that any such interest, earnings and payments continue to be subject to the prohibition.

8.4 Section 23(4) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 requires any person who holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party to immediately[42] notify the National Sanctions Secretariat of –

(a) details of the funds or other assets against which action was taken in accordance with subsection (1);

(b) the name and address of the designated party or listed party;

(c) details of any attempted transaction involving the funds or other assets, including –

(i) the name and address of the sender;

(ii) the name and address of the intended recipient;

(iii) the purpose of the attempted transaction;

(iv) the origin of the funds or other assets; and

(v) where the funds or other assets were intended to be sent.

8.5 Section 23(5) further provides that any person who fails to comply with subsection (1) or (2) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

8.6 Further, section 24(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 provides that subject to this Act, no person shall make any funds or other assets or financial or related services available, directly or indirectly, or wholly or jointly, to or for the benefit of –

(a) a designated party or listed party;

(b) a party acting on behalf, or at the discretion, of a designated party or listed party; or

(c) an entity owned or controlled, directly or indirectly, by a designated party or listed party.

8.7 Pursuant to section 24(2) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, any person who contravenes subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

[42] "immediately" means without delay and not later than 24 hours

8.8 Section 25 (1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 requires, where a party is declared as a designated party or listed as a listed party, every financial institution to, immediately, verify whether the details of the designated party or listed party match with the particulars of any customer, and if so, to identify whether the customer owns any funds or other assets in Mauritius, including the funds or other assets referred to in section 23(1).

8.9 Pursuant to section 25(2) (a) and (b) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, where funds or other assets or no funds or other assets are identified by the financial institution , the financial institution shall make a report to the National Sanctions Secretariat and where such a report is made, the financial institution shall, in addition, report same to its relevant supervisory authority.

8.10 Section 25(3) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 provides that any person who fails to comply with subsection 2(a) or (b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to a term of imprisonment not exceeding 10 years.

8.11 Pursuant to section 39(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, a financial institution shall immediately submit any information related to a designated party or listed party which is known to the financial institution to the FIU in accordance with section 14 of the Financial Intelligence and Anti-Money Laundering Act.

8.12 Section 41 of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 requires a financial institution to implement internal controls and other procedures to enable it to effectively comply with their obligations under the said Act.

8.13 Section 40(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 provides that a supervisory authority[43] may, after consultation with the National Sanctions Committee, develop such rules and guidance and disseminate such other relevant information as may be necessary for the purposes of the said Act.

8.14 A supervisory authority is further empowered by section 40(2) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 to supervise and enforce compliance by financial institutions over whom they exercise supervisory control or oversight with the requirements imposed under the said Act.

8.15 Pursuant to section 40(3) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, where it appears or is represented to any supervisory authority that any financial institution has refrained from complying or negligently failed to comply with any requirement of the said Act, the supervisory authority may take, against the financial institution, any action which it may be empowered to take under the relevant enactments.

---

[43] "supervisory authorities" –

(a) means –

(i) the Bank of Mauritius;

(ii) the Financial Services Commission;

(b) includes a regulatory body specified in Column 2 of Part I of the First Schedule

8.16 The following obligations are imposed on financial institutions under the Act :

(i) Financial prohibitions

(a) Prohibition to deal with the funds or other assets of Designated Parties (i.e. any party declared as such by the Secretary for Home Affairs under the Act) and Listed Parties (namely any party listed by or under the authority of the United Nations Security Council) under section 23 of the Act;

(b) Prohibition to make funds or other assets available to Designated Parties and Listed Parties under section 24 of the Act.

(ii) Reporting obligations

(a) financial institutions must immediately (i.e. without delay and not later than 24 hours), verify whether the details of the Designated Party or Listed Party match with the particulars of any of its customer;

(b) if there is a positive match, the financial institution must identify whether the customer owns any funds or other assets with it, including the funds or assets mentioned in section 23(1);

(c) the financial institution is required to make a report to the National Sanctions Secretariat and the Bank of Mauritius where funds or other assets have been identified by it.

(d) a nil report must be submitted to the above authorities if no funds or other assets is identified.

(iii) Reporting of suspicious information

A financial institution must immediately submit to the FIU in accordance with section 14 of the Financial Intelligence and Anti-Money Laundering Act, any information relating to a Listed Party which is known to it.

(v) Internal controls

Financial institutions must implement internal controls and other procedures to enable it to effectively comply with the obligations under the Act.

8.17 The Bank of Mauritius is required, under section 40(2) of the Act, to supervise and enforce compliance by its licensees with the requirements imposed under the Act. Failure to comply with the Act is an offence.

A. TERRORIST FINANCING

8.18 Terrorism is the unlawful threat of action designed to compel the government or an international organization or intimidate the public or a section of the public for the purpose of advancing a political, religious or ideological belief or cause. Financing of terrorism (FT/TF) is the process by which funds are provided to an individual or group to finance terrorist acts.

8.19 The key difference between ML and TF is that with ML, the person seeks to disguise the origins of illicit funds with a profit motive in mind; while in contrast, a person funding terrorism may use legitimately-held funds to pursue illegal and ideological motives. Financial institutions should bear this in mind when assessing the risks posed by those funding terrorism. A financial institution that carries out a transaction, knowing that the funds or property involved are owned

or controlled by terrorists or terrorist organisations or that the transaction is linked to or is likely to be used in terrorist activity, is committing a criminal offence.

8.20 TF often involves small sums of money and may be difficult to detect. Notwithstanding, many of the AML controls financial institutions have in place will overlap with measures to combat the financing of terrorism (CFT). These may include for example, risk assessments, customer due diligence procedures, transaction monitoring and reporting of suspicious activity and transactions. The guidance provided in these Guidelines therefore applies equally to CFT as it does to AML, even where this is not explicitly stated.

8.21 Funding for terrorist groups may come from various sources. While state sponsored terrorism has declined in recent years, other types of funding have been observed. Traditional sources include 'revenue-generating' criminal activities such as kidnapping and extortion. Funding may also include income from legitimate sources such as fundraising by charitable or relief organizations. Donors are led to believe that they are giving to support a worthwhile cause and have no knowledge that some or all of the funds donated is being diverted to support terrorism.

8.22 In recent times, terrorist groups have occupied territories in different jurisdictions by force and exploited the local population and material resources through extortion, taxation and theft. These include bank looting, control of oil fields and refineries and robbery of economic assets. Technology has also been leveraged to obtain funds through modern communication techniques such as crowd-funding.

8.23 While financial gain is generally the objective of other types of criminal activities, the goal of terrorism may be different, but terrorists still require financial support in order to achieve their aims. A successful terrorist group, like any criminal organisation, is therefore necessarily one that is able to build and maintain an effective financial infrastructure. For this it must develop sources of funding, a means of laundering those funds and then finally a way to ensure that the funds can be used to obtain material and other logistical items needed to commit terrorist acts.

LAUNDERING OF TERRORIST RELATED FUNDS

8.24 The methods used by terrorists and their associates to generate funds from illegal sources differ little from those used by traditional criminal organisations. Although funding from legitimate sources need not be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between it and its legitimate funding sources. It follows then that terrorists must find ways to launder these funds in order to be able to use them without drawing the attention of authorities. In examining terrorist related financial activity, FATF experts have concluded that terrorists and their support organisations generally use the same methods as criminal groups to launder funds. Some of the particular methods detected with respect to various terrorist groups include: cash smuggling, deposits to or withdrawals from bank accounts, purchases of various types of monetary instruments (travellers' cheques, bank cheques, money orders), use of credit or debit cards, and wire transfers. The terrorist's ultimate aim is not to generate profit from his fundraising mechanisms but to obtain resources to support his operations. Thus, the direction taken by fund transfers would be particularly relevant to the tracking down of terrorist financing. A view may be taken in this regard on the basis of repetitive similar transactions either from a sole account or from a number of accounts maintained in the same institution by different parties.

8.25 When terrorists obtain their financial support from legal sources (donations, sales of publications, etc.), there are certain factors that make the detection and tracing of these funds more difficult. For example, charities or non-profit organisations and other legal entities have been cited as playing an important role in the financing of some terrorist groups. At first sight,

the apparent legal source of this funding may mean that there are few, if any, indicators that would make an individual financial transaction or series of transactions stand out as linked to terrorist activities.

8.26 Other important aspects of terrorist financing that make its detection more difficult are the size and nature of the transactions involved. Several FATF experts have mentioned that the funding needed to mount a terrorist attack does not always call for large sums of money, and the associated transactions are usually not complex and many involve the movement of small sums through wire transfers.

8.27 Enhanced due diligence techniques are therefore required for tracking down terrorist financing.

8.28 Terrorist financing, while an offence in itself, is also a predicate offence for money laundering.

PROLIFERATION FINANCING

8.29 The FATF has developed a working definition for financing of proliferation as set out in Combating Proliferation Financing: A Status Report on Policy Development and Consultation[44:]

8.30 "Financing of proliferation" refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

8.31 The UNSC Resolutions has designated certain individuals and entities involved in the proliferation of weapons of mass destruction and its financing. The relevant information and full listings of persons designated by UNSC Resolutions may be found on the UN website[45].

8.32 Financial institutions should rely on its CDD measures (including screening measures) to detect and prevent proliferation financing activities and transactions. It is important to ensure that name screening by financial institutions is performed against the latest UN listings as they are updated from time to time. Financial institutions should have in place policies, procedures and controls to continuously monitor the listings and take necessary follow-up action within a reasonable period of time, not to proceed with the transaction and to immediately report the matter to the Bank.

8.33 Financial institutions should also have policies and procedures to detect attempts by its employees or officers to circumvent the above requirement by, namely —

(a) omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by the financial institution itself or other institutions involved in the payment process; and

(b) structuring transactions with the purpose of concealing the involvement of designated persons.

---

[44] available at http://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf
45 https://www.un.org/sc/suborg/en/s/res/1737-(2006) and https://www.un.org/sc/suborg/en/sanctions/1718.

8.34 The financial institution should have appropriate internal controls, policies and procedures to prevent such attempts, and take appropriate measures against such employees and officers and report any suspicious transaction to the FIU in accordance with this Guideline.

Potential Indicators of Proliferation Financing

8.35 Financial institutions should develop indicators that would alert it to customers and transactions (actual or proposed) that are possibly associated with proliferation financing-related activities, including indicators such as whether —

(a) the customer is vague and resistant to providing additional information when asked;

(b) the customer's activity does not match its business profile or the end-user information does not match the end-user's business profile;

(c) the transaction involves designated persons;

(d) the transaction involves higher risk countries or jurisdictions which are known to be involved in proliferation of weapons of mass destruction or proliferation financing activities;

(e) the transaction involves other financial institutions with known deficiencies in AML/CFT controls or controls for combating proliferation financing;

(f) the transaction involves possible shell companies (e.g. companies that do not have a high level of capitalisation or display other shell company indicators);

(g) the transaction involves containers whose numbers have been changed or ships that have been renamed;

(h) the shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner;

(i) the transaction involves the shipment of goods inconsistent with normal geographic trade patterns (e.g. the country involved would not normally export or import such goods);

(j) the transaction involves the shipment of goods incompatible with the technical level of the country to which goods are being shipped (e.g. semiconductor manufacturing equipment shipped to a country with no electronics industry); or

(k) there are inconsistencies in the information provided in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

8.36 The FATF has also provided guidance on measures to combat proliferation financing and it is recommended that financial institutions refer to the FATF website (www.fatf-gafi.org) for additional information.

How can proliferation and its financing be targeted?

8.37 There are two recognised mechanisms by which proliferation can be targeted; namely import/export controls and financial measures.

Why are financial measures important?

8.38 Financial measures act as a supplement to effective import and export controls, to address the financial activity associated with proliferation. Similar to international criminal networks, proliferation networks tend to depend heavily on the formal financial system to carry out transactions and business dealings worldwide. In addition, proliferation support networks often operate for financial gain and are highly vulnerable to public exposure and disruption of funding. These factors make financial measures particularly effective in deterring and disrupting proliferation financial and support networks. Therefore, institutions should be alert to the possibility that their customers may be engaging in, or facilitating, proliferation activities.

8.39 The FATF's February 2010 Working Group Report suggests there are three areas where institutions might have responsibilities in relation to proliferation financing, namely:

a) the risk assessment of customers and products;

b) enhanced due diligence on high-risk transactions and entities; and

c) special attention to trade finance and insurance products.

Why can it be difficult to identify activity linked to proliferation, or proliferation financing?

8.40 Following are some of problems in attempting to identify proliferation financing:

- the purchase and sale of elementary components, as opposed to complete manufactured systems. The individual elementary components may also have legitimate uses (and may even be described as being "dual-use" goods), making their identification for illegitimate purposes even more problematic.
- dual-use goods are difficult to identify, requiring specialist knowledge and can be described in common terms that denote many innocent uses (e.g. they might be described by an innocuous and generic term such as "pumps").
- networks through which proliferation-sensitive goods may be obtained tend to be complex. This, combined with the use of false documentation, allows for such sensitive goods, the entities involved, associated financial transactions and the ultimate end-user to avoid suspicion and detection. Front companies, agents and other false end-users are often used to cover up the true movement of the finance and goods, and the ultimate end-user.
- as a state may be involved in seeking the goods, the source of funds may appear (or be) legal, but the true end-user, and the end-use, of the goods involved is obscured, making identification of such activities difficult.

What is required of Reporting Entities?

8.41 Apart from implementing enhanced KYC and CDD measures as detailed above, financial institutions must adhere to the obligations set out under United Nations Sanctions Act regarding parties listed by the UNSC under Resolution 1518 (2003).

9 REPORTING OF SUSPICIOUS TRANSACTION

INTRODUCTION

9.1. A fundamental element of an effective system to combat money laundering and terrorism and proliferation financing is requirement that financial institutions identify and file suspicious transaction reports (STRs) with their national financial intelligence unit.

9.2. Financial institutions are required to report suspicious transactions to the Financial Intelligence Unit.

9.3. The Financial Intelligence Unit was established on 10 June 2002 under the FIAMLA to act as the central agency in Mauritius responsible for receiving, requesting, analysing and disseminating to the investigatory and supervisory authorities disclosures of financial information –

(a) concerning suspected proceeds of crime and alleged money laundering offences;

(b) required by or under any enactment in order to counter money laundering; or

(c) concerning the financing of any activities or transactions related to terrorism.

9.4. The Financial Intelligence Unit is essentially an intelligence-gathering entity which collects and compiles information on money laundering and terrorism. It acts as the central repository of financial information in connexion with suspected or actual money laundering activities and terrorist financing.

9.5. The Financial Intelligence Unit has issued Guidance Note pursuant to section 10(2)(c) of the FIAMLA and is intended to assist and guide financial institutions in completing the Suspicious Transaction Report form issued by the FIU[46].

9.6. It is recommended that financial institutions consult the Guidance Note on Suspicious Transaction Report issued by the Financial Intelligence Unit which provide insightful guidance to the industry.

STATUTORY REQUIREMENTS

*Financial Intelligence and Anti-Money Laundering Act 2002 (*FIAMLA)

9.7. A 'suspicious transaction'[47] is defined 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, terrorism or acts of terrorism or by proscribed organizations, whether or not the funds represent the proceeds of a crime;

[46] Please refer to the website of the FIU at www.fiumauritius.org.

[47] Section 2 of FIAMLA

(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 reason.

9.8. A 'transaction'[48] would include -

(i) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and

(ii) a proposed transaction or an attempted transaction.

9.9. Section 14 of the FIAMLA stipulates that every financial institution should, as soon as practicable but not later than 15 working days from the day on which it becomes aware of a transaction which it has reason to believe may be a suspicious transaction, make a report to the FIU of such transaction.

9.10. It further provides that a report made in this respect shall be of a general nature and shall not be construed to be a substitute for the institution's own internal screening mechanisms.

9.11. Section 13(2) of FIAMLA further provides that the Director of the FIU, may where an STR has been made under section 14, request further information in relation thereto from the financial institution who made the report or from any other financial institution who is, or appears to be, involved in the transaction.

9.12. Section 13 stipulates that, following submission of a suspicious transaction report, the financial institution shall keep on record all information in respect thereto for at least 7 years or for such period as may be specified by the FIU.

9.13. Under Section 13 of the FIAMLA, every financial institution is also required to, as soon as practicable, but not later than 15 working days, to furnish such information as may be requested by the FIU.

9.14. Section 16(1) of the FIAMLA further requires financial institutions and its officers not to disclose to any person that a STR is being or has been filed, or that related information is being or has been requested by, furnished or submitted to the FIU.

9.15. Notwithstanding section 16(1) of the FIAMLA, any supervisory authority may, for the sole purpose of discharging its compliance functions, request the FIU to provide it with a copy of the suspicious transaction report made under section 14(1).

9.16. Section 16(2) of the FIAMLA further provides that no proceedings shall lie against any person for having -

[48] ibid

(a) reported in good faith any suspicion he may have had, whether or not the suspicion proves to be well founded following investigation or prosecution or any other judicial action;

(b) supplied any information to the FIU pursuant to a request made under section 13(2) or (3).

9.17. Section 16(3) of the FIAMLA stipulates that no financial institution and its officers, i.e. a director, employee, agent or other legal representative, who receives or shares a report made that Part shall incur liability for –

(a) any breach of confidentiality for any disclosure made in compliance with this Act, or to assist its supervisory authority in the discharge of its functions under this Act;

(b) any disclosure made for compliance, audit or AML/CFT functions within the financial institution or at group level, provided that adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off, are in place within the group.

9.18. Any person who fails to comply with section 16(1) of the FIAMLA shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

Banking Act 2004

9.19. Section 64(3)(j) of the Banking Act provides that the duty of confidentiality imposed on financial institutions and their employees shall not apply where the financial institution is required to make a report or to provide additional information on a suspicious transaction to the FIU under the FIAMLA.

***Financial Intelligence and Anti-Money Laundering Regulations 2018 (*FIAML Regulations)**

9.20. Under Regulation 26 of the FIAML Regulations, financial institutions are required to appoint a Money Laundering Reporting Officer (MLRO), to whom internal reports of any information or other matter which comes to the attention of any staff handling the transaction and which, in the opinion of the staff gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism. Financial institutions are also required to appoint a Deputy MLRO to perform the duties of MLRO in his absence.

9.21. The MLRO shall be a senior officer[49] and the Deputy MLRO must be sufficiently senior in the organisation of the financial institution or have sufficient experience and authority and have a right of direct access to the board of directors and have sufficient time and resources to effectively discharge his functions.

[49] Please refer to Guidelines on section 46(2) of the Banking Act 2004 – Appointment or Reappointment of Senior Officers issued by the Bank and available at the following link : https://www.bom.mu/financial-stability/supervision/guidelines/guidelines-section-462-banking-act-2004-appointment-or

9.22. Regulation 28 of the FIAML Regulations stipulates that where a person identifies a suspicious or unusual activity in the course of a business relationship[50] or occasional transaction[51], he shall consider obtaining enhanced CDD and make an internal disclosure in accordance with the procedures established under the Regulation 27.

9.23. Regulation 27 of the FIAML Regulations details the reporting procedures to be maintained by financial institutions for internal disclosures of suspicious transactions. The financial institution must, inter alia, establish, document, maintain and operate reporting procedures that shall —

(a) enable all its directors or all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;

(b) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the MLRO;

(c) require reports of internal disclosures to be made to the MLRO of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity;

(d) require the MLRO to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;

(e) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the financial institution; and

(f) enable the information or other matters contained in a report to be provided as soon as is practicable to the FIU where the MLRO knows or suspects that another person is engaged in money laundering or terrorism financing activities.

9.24. In terms of Regulation 28, where a financial institution identifies any unusual activity in the course of a business relationship or occasional transaction the financial institution must –

(a) perform appropriate scrutiny of the activity;
(b) obtain enhanced CDD in accordance with Regulation 12 of the FIAML Regulations and these Guideline; and
(c) consider whether to make an internal disclosure in accordance with the reporting procedures established under regulation 27.

9.25. Pursuant to Regulation 29, where an internal disclosure has been made, the MLRO must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.

---

[50] 'business relationship' means an arrangement between a person and a financial institution, where the purpose, or effect, of the arrangement is to facilitate the carrying out of transactions between the person and the financial institution on a frequent, an habitual or a regular basis. (section 2 of the FIAMLA)

[51] An occasional transaction means any transaction carried out other than in the course of a business relationship. (Regulation 2 of FIAML Regulations)

9.26. Where the MLRO knows or has reason to believe that an internal disclosure may be suspicious, he must forthwith make a report in accordance with section 14 of the FIAMLA to the FlU.

9.27. Regulation 30 of the FIAML Regulations, requires financial institutions to establish and maintain separate registers of all internal disclosures and all external disclosures. Both registers may be contained in a single document if the following details required to be included in those registers can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

(a) the date on which the report is made;
(b) the person who makes the report;
(c) for internal disclosures, whether it is made to the MLRO or Deputy MLRO; and
(d) information sufficient to identify the relevant papers.

GUIDANCE

Knowledge versus suspicion

9.28. Generally speaking, knowledge is likely to include:

(a) actual knowledge;
(b) knowledge of circumstances which would indicate facts to a reasonable person; and
(c) knowledge of circumstances which would put a reasonable person on inquiry.

Recognition of Suspicious Transactions

9.29. Where there is a business relationship, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognise that a transaction, or series of transactions, is unusual. This underscores the importance of CDD in establishing the client's profile.

9.30. There is no monetary threshold for making a report concerning a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but when taken together, may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering or terrorism financing offence.

9.31. Financial institutions should, from an examination of transactions and ML/TF indicators, determine whether there is a suspicion of ML/TF. Where a transaction or a series of transactions is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, etc., the transaction should be considered as unusual.

9.32. Questions that a financial institution might consider when determining whether an established customer's transaction might be suspicious are, amongst others :

- is the size of the transaction consistent with the normal activities of the customer?
- is the transaction rational in the context of the customer's business or personal activities?
- has the pattern of transactions conducted by the customer changed?
- where the transaction is international in nature, does the customer have any obvious reason for conducting business with the other country involved?

Financial Institutions may refer to the FIU Guidance Note on Suspicious Transaction Report for additional examples of indicators of suspicious transactions.

9.33. Sufficient guidance must be given to staff to enable them to recognise suspicious transactions (see Chapter 11 on "Staff Training"). The type of situations giving rise to suspicions will depend on a financial institution's customer base and range of services and products. Financial institutions might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions from time to time.

Unusual activity

9.34. Financial institutions are required in terms of Regulation 28(2) of the FIAML Regulations to identify any unusual activity in the course of a business relationship or occasional transaction and –

(a) perform appropriate scrutiny of the activity;
(b) obtain enhanced CDD in accordance with regulation 12 of FIAML Regulations and this Guideline; and
(c) consider whether to make an internal disclosure in accordance with the reporting procedures established under regulation 27 of the FIAML Regulations and this Guideline.

9.35. In order to meet its obligations, set out above, it is therefore essential for financial institutions to be able to identify unusual activities.

9.36. While there is no definition of "unusual activity", Regulation 25 of the FIAML Regulations provides an indication of the types of transactions which may constitute such an activity by requiring financial institutions to examine, as far as possible, the background and purpose of all transactions that –

(a) are complex transactions;
(b) are unusually large transactions:
(c) are conducted in an unusual pattern; or
(d) do not have an apparent economic or lawful purpose.

Financial Institutions may refer to the FIU Guidance Note on Suspicious Transaction Report for additional examples of indicators of suspicious transactions.

9.37. A financial institution may also consider anything that causes it to doubt the identity of the customer (including beneficial owner) or anything that causes the relevant person to doubt the good faith of the customer (including beneficial owners) as an unusual activity.

9.38. Such activities are more likely to be detected during ongoing monitoring (for further guidance please refer to Chapter 7 of the Guideline), when receiving an application from a new customer, when receiving an instruction to carry out a transaction or during other communications with the customer.

9.39. Financial institutions may refer to the Guidance Notes issued by the FIU for further guidance on examples of such transactions.

Transaction monitoring

9.40. Financial institutions must have appropriate processes in place that allow for the identification of unusual transactions, patterns and activity that is not consistent with the customer's risk profile. Since these will not all be suspicious, financial institutions should also have processes to analyse transactions, patterns and activity to determine if they are suspicious and meet the reporting threshold.

9.41. Transaction monitoring processes or systems may vary in scope or sophistication depending on the size, volumes and complexity of the business operations. Regardless, the key element of any system is having up-to-date customer information to facilitate the identification of unusual activity.

9.42. Monitoring can be either:

i. In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or

ii. After the event through an independent review of the transactions and/or activities that a customer has undertaken.

9.43. Financial institutions should also have systems and procedures to deal with customers who have not had contact for some time, such as dormant accounts or relationships, to be able to identify future reactivation and unauthorized use.

9.44. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk. Monitoring processes and systems should enable trend analysis of transaction activity including monitoring of transactions with parties in higher risk countries or jurisdictions, to identify unusual or suspicious business relationships and transactions. The monitoring system should enable financial institutions to monitor and report to senior management on significant customer relationships and activity on an individual or consolidated basis across the financial group and identify activity that is inconsistent with the financial institution's knowledge of the customer, their business and risk profile.

The Money Laundering Reporting Officer (MLRO)

9.45. Financial institutions must appoint a MLRO to whom internal reports of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity ('internal disclosures') shall be made and who considers any report to determine whether a STR should be made to the FIU. Chapter 5 of this Guideline provides further guidance on the appointment of the MLRO.

9.46. Every financial institution has a clear obligation to ensure that each relevant employee knows his statutory obligation to report any suspicion or knowledge of money laundering and terrorism financing activity to the MLRO for further investigation. The MLRO shall thus be the central reference point for reporting suspicious transactions.

9.47. The contact details of the MLRO and the procedure to be followed for the internal disclosure of suspicious transactions should be provided to all employees during induction trainings, staff trainings and refresher trainings. Chapter 11 of this Guideline provides further guidance in this respect.

Deputy Money Laundering Reporting Officer

9.48. Financial institutions must also appoint a Deputy MLRO, who shall be sufficiently senior or have sufficient experience and authority, to perform the duties of the MLRO in his absence.

9.49. Hence, financial institutions should ensure that appropriate replacement be provided in case the MLRO is absent. The contact details of the Deputy MLRO must also be disseminated to staff.

REPORTING PROCEDURE

9.50. A financial institution must establish, document, maintain and operate reporting procedures which must–

(a) enable all its directors or all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;

(b) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the MLRO;

(c) require reports of internal disclosures to be made to the MLRO of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity;

(d) require the MLRO to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;

(e) ensure that the MLRO has full access to any other information that may be of assistance and that is available to the financial institution; and

(f) enable the information or other matters contained in a report to be provided as soon as is practicable to the FIU where the MLRO knows or suspects that another person is engaged in money laundering or terrorism financing activities.

Internal Disclosure

9.51. Where a staff identifies a suspicious or unusual activity, he/she should make an internal disclosure to the MLRO or the Deputy MLRO, as appropriate.

9.52. The internal disclosure must be in writing and properly documented and include the full details of the customer and a complete statement of the information giving rise to the suspicion.

9.53. The financial institution may first discuss the matter with the MLRO and then prepare the initial report for the MLRO. It is however emphasised that all internal disclosures should be made in writing and should be documented.

9.54. Once an employee has reported his suspicion to the MLRO, he has fully satisfied and discharged his statutory obligation.

Reporting Chain

9.55. There should be a clear reporting chain under which the internal disclosure is made on to the MLRO.

9.56. The reporting lines for internal disclosures shall be as short as possible, with the minimum number of people between the financial institution and the MLRO and reach the MLRO without undue delay.

Internal Disclosure Report

9.57. The MLRO should consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity.

9.58. Financial institutions should ensure that the MLRO has full access to any other information that may be of assistance and that is available.

9.59. Care should be taken to guard against a report being submitted to the MLRO as a matter of routine without undertaking reasonable internal enquiries to determine that all available information has been taken into account.

9.60. The MLRO should acknowledge receipt of the internal disclosure report and ensure that the internal disclosure report includes sufficient details of the customer and as full a statement as possible of the information giving rise to the suspicion, in order to allow him to further investigate and evaluate the disclosure.

9.61. The MLRO should also remind the staff making the internal disclosure of the obligation not to do anything that may prejudice enquiries, such as tipping off the customer or any other third party.

9.62. When evaluating an internal disclosure report, the MLRO must take reasonable steps to consider all other relevant information available within the financial institution concerning the person or business to whom the initial report relates. This should include making a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and referral to identification records held. It may also include appropriate questioning of the customer.

Tipping Off

9.63. In practice, however, preliminary enquiries in respect of an applicant for business, either to obtain additional information to confirm true identity, or to ascertain the source of funds or the precise nature of the transaction being undertaken, will not trigger a tipping off offence. Great care should, however, be taken where a suspicious transaction has already been reported and it becomes necessary to make further enquiries, to ensure that customers do not become aware that their names have been brought to the attention of the FIU. In cases where the financial institution forms a suspicion of money laundering or terrorist financing, and the financial institution reasonably believes that performing the CDD process will tip-off the customer, the financial institution shall not pursue the CDD process and shall instead file an STR with the FIU.

9.64. The MLRO will be expected to act honestly and reasonably and to make his determinations in good faith. It is vital therefore that all internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the authorities, should be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation in a case on which the MLRO has opted not to report and suspicions are later found to be confirmed. Provided the MLRO or in his absence, the Deputy MLRO, does act in good faith in deciding not to pass on any suspicions, there will be no liability for non-reporting if his judgment is later found to be wrong.

REPORTING OF SUSPICIOUS TRANSACTIONS TO THE FIU (EXTERNAL DISCLOSURES)

Suspicious Transaction Report

9.65. Pursuant to section 14 of the FIAMLA, financial institutions must, as soon as practicable but not later than 15 working days from the day on which it becomes aware of a transaction which it has reason to believe may be a suspicious transaction, make a report to the FIU of such transaction.

9.66. The MLRO must therefore forthwith make a report in accordance with section 14 of the FIAMLA to the FIU where he knows or has reason to believe that an internal disclosure may be suspicious.

9.67. Regulation 27(f) of the FIAML Regulations further requires financial institutions to maintain such reporting procedures that would enable the information or other matters contained in a report of internal disclosures to be provided as soon as is practicable to the FIU where the MLRO knows or suspects that another person is engaged in money laundering or terrorism financing activities.

9.68. If, after completing this review, it is decided that there are no facts that would negate the suspicion, the MLRO must report that suspicious transaction to the FIU.

9.69. Reporting to the FIU should not only be made following internal disclosure reports. The MLRO should not be a passive recipient of ad hoc reports of suspicious transactions.

9.70. The MLRO should play an active role in the identification and reporting of suspicious transactions. This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff. Should make mention of ongoing monitoring and the enhanced monitoring of higher risk clients as part of the process to identify suspicions.

Incidence of reporting on risk assessment of customer

9.71. If an FI is reporting multiple suspicious financial transactions involving the same client(s) or account(s), it should periodically re-assess their level of risk and apply the appropriate measures determined by its risk-based approach.

Contents of Suspicious Transactions Reports

9.72. It is mandatory for every report which a financial institution submits with the FIU to contain the following information[52] –

(a) the identification of the party or parties to the transaction;

(b) the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;

(c) the business relationship of the suspect to the bank, financial institution, cash dealer or member of relevant profession or occupation, as the case may be;

(d) where the suspect is an insider, any information as to whether the suspect is still affiliated with the bank, financial institution, cash dealer, or member of a relevant profession or occupation, as the case may be;

(e) any voluntary statement as to the origin, source or destination of the proceeds;

(f) the impact of the suspicious activity on the financial soundness of the reporting institution or person; and

(g) the names of all the officers, employees or agents dealing with the transaction.

Method of Reporting

9.73. The use of a standard format in the reporting of suspicious transactions is important. A format has been devised by the FIU and is available on the website of the FIU[53]. The FIU will, forthwith, upon receipt of a report, acknowledge receipt of same.

9.74. All reports of suspicious transactions whether in relation to money laundering or terrorist financing should be made in such form and manner as may be specified by the FIU and addressed to:

The Director
Financial Intelligence Unit
10th Floor, SICOM Tower
Wall Street
Ebène Cybercity, 72201
Ebène
Republic of Mauritius

Telephone: (230) 454 1423
Fax: (230) 466 2431
Email: fiu@fiumauritius.org

Other reports to the FIU

9.75. The FIAMLA also provides for the following reports to be made to the FIU. The relevant regulations, however, have not yet promulgated and accordingly the following requirements are not operative.

[52] Section 15(2) of the FIAMLA
[53] www.fiumauritius.org

Cash Transaction Report

9.76. Under section 14A of the FIAMLA, every financial institution should report to the FIU, in such matter and within such time as may be specified, particulars of any cash transaction in excess of the prescribed amount.

Report of Electronic transfer of money to or from Mauritius

9.77. Section 14B of the FIAMLA further requires every financial institution, which sends or receives money in excess of the prescribed amount from outside Mauritius on behalf, or on the instruction of, another person, to report the transfer, together with the prescribed particulars, to FIU within the prescribed time.

Currency transaction reports

9.78. Under section 17G of the FIAMLA, every financial institution has an obligation to submit to the FIU, within the prescribed time limit, a report on any currency transaction in an amount equal to or above the prescribed amount, whether conducted as a single transaction or several transactions that appear to be linked.

REGISTER OF REPORTS

9.79. Pursuant to Regulation 30 of the FIAML Regulations, financial institutions are required to establish and maintain separate registers of all internal disclosures and all external disclosures.

9.80. These registers may be contained in a single document if the details maintained in the registers can be presented separately for internal disclosures and external disclosures upon request by a competent authority[54].

9.81. The registers must include details of –

(a) the date on which the report is made;

(b) the person who makes the report;

(c) for internal disclosures, whether it is made to the MLRO or Deputy MLRO; and

(d) information sufficient to allow the papers relevant to the disclosures to be located.

9.82. A template for the registers is provided in Annex 1A and 1B of the Chapter which may be used by financial institutions. Financial Institutions should however ensure that the name of the customer who is subject to the STR is not listed in the register to ensure confidentiality of the report.

[54] "competent authorities" has been defined in the FIAML Regulation as (a) meaning a public authority to which responsibility to combat money laundering or terrorist financing is designated; and (b) including a supervisory authority, regulatory body and an investigatory authority;

Appendix 9.1A

Register of Internal Disclosures

This template, based on Regulation 30(3) of the FIAML Regulations, is for guidance purposes only. Financial institutions may make use of document as is or with such adaptations as they may deem fit provided that these are in compliance with the prevailing legislation.

[Name and logo of Financial Institution]

Register of Internal Disclosure Reports on Money Laundering and Financing of Terrorism made to the MLRO or Deputy MLRO

Date on which the report is made	*Person who made the report*	*Whether the report is made to the MLRO or Deputy MLRO*	*Information sufficient to identify the relevant papers*

* financial institutions may, if they so wish, include an additional column on any action taken regarding the internal disclosure, which may assist them in promptly determining whether an internal disclosure has been reported to the FIU.

Appendix 9.1B

Register of External Disclosures

This template, based on Regulation 30(3) of the FIAML Regulations, is for guidance purposes only. Financial institutions may make use of document as is or with such adaptations as they may deem fit provided that these are in compliance with the prevailing legislation.

[Name and logo of Financial Institution]

Register of External Disclosures on Money Laundering and Financing of Terrorism made to the FIU

Date on which the report is made	*Person who made the report*	*Information sufficient to identify the relevant papers*

* financial institutions may, if they so wish, include additional columns on any action taken regarding the external disclosure as well as any reference number provided to them by the FIU after submission of the STR.

---

10 RECORD-KEEPING

INTRODUCTION

10.01 Record keeping is an essential component of the combat against money laundering and the financing of terrorism in the sense that an audit trail is established. Otherwise, an authority investigating a case relating to money laundering or the financing of terrorism would not be able to follow the movement of the funds through the financial system thus rendering inquiry and confiscation of those funds difficult. Financial institutions often play an important role in a money laundering or financing of terrorism investigation by providing the relevant records, particularly where a complex web of transactions specifically for the purpose of confusing the audit trail has been used.

STATUTORY REQUIREMENTS

Financial Intelligence and Anti-Money Laundering Act

10.02 Section 17F of the Financial Intelligence and Anti-Money Laundering Act requires financial institution to maintain, and keep for the specified period, all books and records with respect to his customers and transactions as set out hereunder :

(a) all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis undertaken in accordance with this Act, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended;

(b) records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders, which shall be maintained for a period of 7 years after the completion of the transaction; and

(c) copies of all suspicious transaction reports made pursuant to section 14 of the Financial Intelligence and Anti-Money Laundering Act or other reports made to FIU in accordance with that Act, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

10.03 Pursuant to section 13(5) of the Financial Intelligence and Anti-Money Laundering Act, where a report of a suspicious transaction has been made by a financial institution to the FIU under section 14 of the Act, the Director of the FIU may, not later than 15 days before the end of the 7th year following the completion of the transaction to which the suspicious transaction report relates, by written notice, require the financial institution to keep the records in respect of that suspicious transaction for such period as may be specified in the notice.

Financial Intelligence and Anti-Money Laundering Regulations 2018

10.04 Regulation 6(2) of the Financial Intelligence and Anti-Money Laundering Regulations 2018 requires financial institutions to keep records of actions taken to verify the identity of the beneficial owner of their customers which are legal persons pursuant to Regulation 6(1), as well as any difficulties encountered during the verification process.

10.05 Regulation 6(1) provides that where the customer is a legal person, the financial institution shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information on –

(a) the identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;

(b) where there is doubt under paragraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control of the legal person through other means as may be specified by relevant regulatory body or supervisory authority; and

(c) where no natural person is identified under subparagraph (a) or (b), the identity of the natural person who holds the position of senior managing official.

10.06 Pursuant to Regulation 14 –

(i) A financial institution must keep and maintain all necessary records relating to transactions in such a form which enables the prompt reconstruction of each individual transaction.

(ii) In addition, where a financial institution is responding to a request from the FIU under section 13(2) of the Financial Intelligence and Anti-Money Laundering Act or to a request from the Bank, it shall provide for each transaction record -

(a) the full name of the party making a payment; and

(b) the full name of the party receiving a payment.

(iii) Financial institutions must also ensure that all CDD information and transaction records are kept in such a manner that they are swiftly made available to the FIU or the Bank or the other competent authority upon request.

10.07 Regulation 20(7) further stipulates that where technical limitations prevent the required originator or beneficiary information accompanying a cross border wire transfer from remaining with a related domestic wire transfer, the intermediary financial institution shall keep a record, for at least 7 years, of all the information received from the ordering financial institution or another intermediary financial institution.

Banking Act

10.08 Section 33 of the Banking Act 2004 further requires every financial institution, for the purposes of the banking laws[55], to keep in relation to its activities, a full and true written record of every transaction it conducts.

---

[55] "banking laws" –

(a) means this Act, the Bank of Mauritius Act, the Convention for the Suppression of Financing of Terrorism Act, the Financial Intelligence and Anti-Money Laundering Act, the Prevention of Terrorism Act, the Prevention of Terrorism (International Obligations) Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019; and

(b) includes such other enactment as may be prescribed;

10.09 The records required to be kept by financial institutions under section 33 of the Banking Act include –

(a) accounting records exhibiting clearly and correctly the state of its business affairs, explaining its transactions and financial position so as to enable the central bank to determine whether the financial institution has complied with all the provisions of the banking laws;

(b) the financial statements;

(c) account files of every customer, business correspondences exchanged with every customer and records showing, for every customer, at least on a daily basis, particulars of its transactions with or for the account of that customer, and the balance owing to or by that customer;

(d) proper credit documentation; and

(e) such other records as the central bank may determine.

10.10 The above records shall be kept –

(a) in written form or kept on microfilm, magnetic tape, optical disk, or any other form of mechanical or electronic data storage and retrieval mechanism as the central bank may agree to;

(b) for a period of at least 7 years after the completion of the transaction to which it relates;

(c) at the principal office of the financial institution, or at such other place as may be approved by the central bank; and

(d) for identification purposes, in chronological order or sequential order, as appropriate, in batches of convenient size.

GENERAL

10.11 A financial institution should maintain all books and records with respect to its customers and transactions that are necessary and sufficient to meet the record-keeping requirements under Financial Intelligence and Anti-Money Laundering Act, banking laws, this Guideline and other regulatory requirements.

10.12 Financial institutions must ensure that all CDD information and transaction are kept in such a manner that they are swiftly made available to the Bank of Mauritius, the FIU or other competent authority upon request.

CDD RECORDS

10.13 All CDD documentation required by financial institutions to identify and verify the identity of customers and of beneficial owners in accordance with this Guideline must be retained for a period of not less than 7 years after the completion of the transaction to which it relates, closure of the account or cessation of the business relationship with the customer concerned. Likewise, records of the measures taken to verify the identity of beneficial owners as well as any

difficulties encountered during the verification process should be properly documented and retained for a similar period.

10.14 Financial institutions should update information on existing customers and clients on a risk sensitive basis. The existing records of documents data or information collected under the CDD process, particularly for higher risk categories of customers must be reviewed and kept up to date and relevant by financial institutions at least on an annual basis. Financial institutions may determine the frequency at which higher and lower risk clients will be subject to updating of information, provided that for higher risk client such an update is carried out at least on an annual basis and whenever the circumstances so warrant (for e.g. change of CDD information or where the financial institution comes across any information which warrants for the customer information to be updated.

TRANSACTION RECORDS

10.15 Transaction records, in whatever form they are used, e.g. credit/debit slips, cheques etc. need to be maintained for a period of not less than 7 years after the completion of the transactions concerned, in such a manner to enable competent authorities to compile a satisfactory audit trail for suspected laundered and terrorist money and establish a financial profile of any suspect account and should include the following –

(i) the volume of funds flowing through the account

(ii) the source of the funds, including full remitter details

(iii) the form in which the funds were offered or withdrawn i.e. cash, cheques, etc.

(iv) the identity of the person undertaking the transaction and of the beneficiary

(v) counterparty details

(vi) the destination of the funds

(vii) the form of instruction and authority

(viii) the date of the transaction.

(ix) the type and identifying number of any account involved in the transaction.

10.16 All necessary records relating to transactions, both domestic and international must be kept and maintained in such a form that permits the prompt reconstruction of each individual transaction for both account holders and non-account holders.

Reports made to and by the MLRO

10.17 Records of all internal reports made to the MLRO and also all reports made by the MLRO to the FIU should be retained for a period of not less than 7 years after the date on which the report was made.

10.18 Any analysis or findings relating to the background and purpose of complex, unusual or suspicious transactions should also be retained for a period of not less than 7 years after the date on which the finding was made.

Records Relating to Ongoing Investigations

10.19 Where the records relate to ongoing investigations, they should be retained until it is confirmed by the authorities that the case has been closed.

Electronic Records

10.20 Records of electronic payments and messages must be treated in the same way as any other records and kept for the period mentioned in paragraph 10.10 above.

10.21 A comprehensive set of identification documents in respect of each customer should be kept in an orderly manner and produced to the Bank of Mauritius on request.

10.22 It is lawful to electronically record any matter and a personal identification mark on the electronically recorded document is as good as a signature.

Report of a suspicious transaction

10.23 A report of a suspicious transaction made under section 14 of the FIAMLA, including any accompanying documentation should be maintained for a period of at least 7 years from the date the report was made.

10.24 Where a report of a suspicious transaction is made under section 14 of the FIAMLA, the Director of the FIU can, by written notice, not later than 15 days before the end of the 7th year following the completion of the transaction to which the suspicious transaction report relates, require the financial institution to keep the records in respect of that suspicious transaction for such period as may be specified in the notice.

Records kept by intermediaries

10.25 All originator and beneficiary information that accompanies a cross border wire transfer must be retained by an intermediary financial institution. A record of all the information received from an ordering financial institution or another intermediary financial institution must be retained for at least 7 years by an intermediary financial institution where technical limitations have prevented the required originator or beneficiary information accompanying a cross border wire transfer from remaining with a related domestic wire transfer.

Record-keeping in case of reliance on third party

10.26 A financial institution must immediately obtain the required CDD information and records from the third party on which the financial institution is relying to perform CDD measures. The financial institution must ensure that all necessary CDD data and documentation will be made available by the third party upon request and without delay and that the third party has measures in place to comply with all the record-keeping requirements under the banking and FIAMLA laws including regulations made thereunder. Arrangements should be made for the records to be retained for the same period as stated in paragraph 10.10 above.

10.27 In any event, the responsibility for complying with record keeping requirements lies with the financial institution, as opposed to the third party.

Record-keeping requirements for subsidiary or affiliates

10.28 Financial institutions which have subsidiaries, branches or affiliates outside Mauritius should ensure that records held by their subsidiary, branch or affiliate outside Mauritius at a minimum, comply with the requirements of the banking laws, FIAMLA as well as the Regulations made thereunder and this Guideline.

Record-keeping requirements for outsourced activities

10.29 Where a financial institution has outsourced any of its activities to a company in another jurisdiction then it must be satisfied that the relevant records will be maintained in accordance with banking laws, FIAMLA as well as the Regulations made thereunder and this Guideline and will be available to the Bank of Mauritius, the FIU or other competent authority on request.

Record-keeping requirements following mergers or acquisition

10.30 When a financial institution either merges with or acquires another financial institution, it should ensure that the records required to be kept under the banking laws, FIAMLA as well as the Regulations made thereunder and this Guideline can be readily retrieved.

11 STAFF TRAINING

INTRODUCTION

11.01 Ongoing staff training is an integral element of an effective AML/CFT system to prevent and detect potential illicit transactions pertaining to money laundering, terrorist or proliferation financing activities. It is therefore important for every financial institution, in order to combat money laundering and the financing of terrorism and proliferation in an efficient and effective manner, implement an ongoing training programme for its employees in order to discharge part of its statutory duty to take reasonable measures in that regard.

STATUTORY REQUIREMENT

Banking Act

11.02 Section 64A(1)(b) of the Banking Act requires financial institutions to implement programmes against money laundering and terrorism financing, which are commensurate with the money laundering and terrorism financing risks to which it is exposed and the size of its business. These programmes shall include ongoing training programmes for its directors and officers.

Financial Intelligence and Anti-Money Laundering Regulations 2018

11.03 Regulation 22(1)(c) of the Financial Intelligence and Anti-Money Laundering Regulations 2018 further requires financial institutions to implement programmes against money laundering and terrorism financing having regard to the money laundering and terrorism financing risks identified and the size of its business, which at a minimum shall include internal policies, procedures and controls for an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to –

(i) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and

(ii) instruct them in the procedures to be followed where any links have been identified under subparagraph (i) above.

STAFF TRAINING

11.04 The main objection of providing ongoing training is to ensure that directors, officers and employees of the financial institution are adequately trained to enable them to perform their obligation in respect of AML/CFT requirements.

11.05 Financial institutions must take appropriate measures to make its directors, officers and employees aware of:

i. an understanding of ML/TF risk related to clients, products, services, delivery channels and geography, how the monitoring of these risks should occur and what mitigation measures should be applied when these risks are identified.

ii. policies and procedures put in place to prevent money laundering and the financing of terrorism including those for identification, record-keeping, the recognition and handling of suspicious transactions and internal reporting.

iii. the legal requirements contained in the 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 the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and Regulations, guidelines and instructions made thereunder.

iv. their own personal statutory obligations, and the fact that they can personally be liable for failure to report information in accordance with internal procedures.

v. new developments, including information on current money laundering and financing of terrorism techniques, methods and trends.

vi. The procedures to follow when working with law enforcement or the FIU on an investigation

vii. The completion of unusual and suspicious transaction reports; Treatment of incomplete or declined transactions

11.06 At a minimum, a financial institution is required to:

i. ensure that directors, officers and employees understand ML/TF risk, how to monitor risk and corresponding risk mitigation strategies;
Develop an appropriately tailored training and awareness programme consistent with the financial institution's size, resources and type of operation to enable relevant employees to be aware of the risks associated with ML and TF and how to monitor risk and corresponding risk mitigation strategies. The training should also ensure employees understand how the institution might be used for ML or TF; enable them to recognize and handle potential ML or TF transactions; and to be aware of new techniques and trends in money laundering and terrorist financing; The training program should most importantly be tailored and proportional to the risks that have been identified by the FI;

ii. Document, as part of their AML/ CFT policy document, their approach to training, including the frequency, delivery channels and content;

iii. Sensitise its directors, officers and employees as to the importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures and all AML/ CFT preventive measures (record keeping, policies, procedures, risks, PF, etc.);

iv. Ensure that all employees are aware of the identity and responsibilities of the MLRO to whom they should report unusual or suspicious transactions;

v. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile, for the different types of training required for:

a) new employees;
b) operations employees;
c) agents;

d) supervisors;
e) board and senior management; and
f) MLRO, audit and compliance employees.

vi. Obtain an acknowledgement from each employees on the training received;

vii. Assess the effectiveness of training; and

viii. Provide all relevant employees with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

11.07 Scope and Frequency of training / Refresher Training

While training should be imparted to all relevant employees, the scope and frequency of training should be tailored to the specific risks faced by the financial institution and to the nature of their responsibilities.

It will be necessary to make arrangements for refresher training at regular intervals to ensure that staff do not forget their responsibilities and are kept abreast with legislative and regulatory changes. In all cases, the refresher training must be done at least once every 2 years and when a legislative or regulatory change has been implemented or the FI risk assessment has been updated.

DIFFERENT REQUIREMENTS FOR DIFFERENT CATEGORIES OF STAFF

11.08 All staff should be trained generally on all AML/CFT procedures. However, specific guidance should be provided to the following positions.

11.09 Account Opening Personnel

Those members of staff responsible for account opening and acceptance of new customers must receive training in respect of the need to verify a customer's identity and on the internal opening and customer verification procedures available in the institution. They should also be familiarised with the recognition and handling of suspicious transactions and internal suspicious transaction reporting procedures. Training on how to establish the client's ML/TF risk profile and how the risk profile will determine whether enhanced CDD should be applied should also be provided to Account Opening Personnel.

11.10 Front Line Staff

All front line staff who are dealing directly with the public are the first point of contact with potential money launderers and terrorists or their agents. They have to be trained to know the true identity of the customer and the need to, at the outset, know enough of the type of business activities expected of the customer to know what might constitute suspicious activities at a future date. They should be alert to any change in the pattern of a customer's transactions or circumstances that might constitute criminal conduct. They should be provided with training on the recognition and handling of suspicious transactions and on the procedures to be adopted when a transaction is regarded as suspicious. Training should also be provided on how to update

the client's risk profile and what mitigation strategies should be applied when higher risk have been identified.

11.11 Global Trade Services Staff

Financial institutions shall provide AML/CFT training, with special emphasis on trade-based money laundering and terrorist financing, to their global trade services departments and personnel. Training should also be provided on how to update the client's risk profile and what mitigation strategies should be applied when higher risk have been identified.

11.12 New Employees

New employees must, as soon as may be reasonably practicable, but not later than 1 month after they are employed, be given a broad appreciation of the general background to the combating of money laundering and the financing of terrorism, how to implement a risk based approach and the internal suspicious transactions reporting procedures. They should be made aware of the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place for the reporting of suspicious transactions. In all cases, new employees must be subject to AML/CFT training prior to interacting with customers.

11.13 Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the penalties arising under the Act for non-reporting, ensuring that the ML/TF risks are properly understood and that risk mitigation strategies are adequately implemented. assisting money launderers and 'tipping off'; internal reporting procedures; and the requirements for the verification of identity and retention of records.

11.14 MLROs, internal audit and Compliance employees

Emphasis should be placed on the continuous training of the Compliance Officer as well as the compliance and audit employees given their critical role in sensitizing the broader employees complement to AML/CFT issues and ensuring compliance with established AML/ CFT policies and procedures.

In-depth training concerning all aspects of the 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, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and Regulations, guidelines and instructions applicable to those legislations, the internal policies applicable in their institutions and the recognition of suspicious transactions, will be required for the MLRO, internal auditor and Compliance Officer. In addition, the MLRO, internal auditor and Compliance Officer will require extensive initial and ongoing instruction on the validation and reporting of suspicious transactions, understanding of ML/TF risk, how

to conduct risk monitoring, how to adequately implement risk mitigation, on feedback arrangements, and on new trends and patterns of criminal activity.

11.15 Assessing the Effectiveness of the Training Programme

The effectiveness of the institution's training programme may be assessed by:

i. Testing employees' understanding of the policies and procedures to combat ML/TF, the understanding of their statutory and regulatory obligations, and also their ability to recognize suspicious transactions and understanding of ML/TF risk; and

ii. Monitoring the compliance of employees with the AML/CFT procedures as well as the quality and quantity of internal reports so that further training needs may be identified and adequate implementation of risk mitigation strategies and appropriate action can be taken.

11.16 Records of training imparted

Financial institutions should keep a record of all anti-money laundering and combating the financing of terrorism training delivered to their employees for the statutory requirement of at least 7 years.

The records, at a minimum, should include:

i. Details of the content of the training programmes provided;

ii. The names of employees who have received the training;

iii. The date on which the training was delivered;

iv. The results of any testing carried out to measure employees understanding of the anti-money laundering requirements; and

v. An on-going training plan.