ANTI-MONEY LAUNDERING
AND
COMBATTING THE FINANCING OF TERRORISM
HANDBOOK

2020

Updated on 31 March 2021

Table of Contents

Foreword

This Anti-Money Laundering and Combatting the Financing of Terrorism (the 'Handbook') consolidates the Financial Services Commission (the 'FSC') guidance on anti-money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction.

This Handbook aims to enhance understanding of FSC's expectations and help financial institutions assess the adequacy of their internal systems and controls and remedy deficiencies with the aim of combatting laundering of criminal proceeds, the financing of terrorism and the financing of proliferation of weapons of mass destruction (henceforth referred to collectively as "ML and TF"). Its objectives are to provide explanation and therefore assist financial institution in complying with the AML/CFT laws.

It is designed to help financial institutions adopt a more effective, risk-based and outcome-focused approach. The Handbook does not include guidance on all the ML and TF risks a financial institution may face. The self-assessment questions and "good or poor practice" examples used in the Handbook are not exhaustive.

The good practice examples present ways, but not the only ways, in which financial institutions might comply with applicable rules and legal requirements. The Handbook is not the only source of guidance on ML and TF. Financial institutions are reminded that other international bodies like the Financial Action Task Force produce guidance that may also be relevant and useful.

Guidance in this Handbook should be applied in a risk-based proportionate way. This includes taking into account the size, nature and complexity of a financial institution when deciding whether a certain example of good or poor practice is relevant to its business.

Chapter 1

1.1. Introduction

The FSC strongly believes that the key to the prevention and detection of money laundering and the financing of terrorism lies in the implementation of, and strict adherence to, effective systems and controls, including sound customer due diligence ('CDD') measures based on international standards.

The Handbook aims at assisting financial institutions in meeting their obligations under the Financial Intelligence and Anti-Money Laundering Act ('FIAMLA') and the Financial Intelligence and Anti-Money Laundering Regulations ('FIAML Regulations 2018').

1.2. Legislative Framework

Mauritius has taken several important steps over the past years to enact legislation that has strengthened the country's money laundering and terrorist financing prevention efforts.

Mauritius brought a number of amendments to its AML/CFT framework through the Finance (Miscellaneous Provisions) Act 2018, Act 11 of 2018, which was gazetted on 9 August 2018 in Government Gazette 71 of 2018. The relevant amendments introduced by the Finance (Miscellaneous Provisions) Act 2018 are in force and aim at strengthening the national AML/CFT framework by, inter alia:

(a) enhancing the existing legal framework for preventive measures that apply to financial institutions and Designated Non-Financial Businesses and Professions ('DNFBPs');
(b) extending the scope of the FIAMLA to include proliferation financing;
(c) establishing a legal framework to support the National Risk Assessment exercise.
(d) providing a general penalty for contravention of those provisions of the FIAMLA for which no specific penalty was set out.

In addition, a new set of regulations namely, the FIAML Regulations 2018 were promulgated on 28 September 2018 and became effective on 01 October 2018. The Regulations 2018 revoked the Financial Intelligence and Anti-Money Laundering Regulations 2003 and address, inter alia, the following FATF requirements:

(a) Customer Due Diligence;
(b) Politically exposed persons;

(c) Correspondent banking;

(d) Money or value transfer services;

(e) New technologies;

(f) Wire transfers;

(g) Reliance on third parties; and

(h) Internal control and foreign branches and subsidiaries.

On 21 May 2019, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 were enacted and both acts came into operation on the 29 May 2019.

The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019enables Mauritius to implement the measures under all the United Nations Security Council Resolutions and deal with other matters of international concern, and to give effect to Article 41 of the Charter of the United Nations.

1.3. Scope of the Handbook

This Handbook is issued to assist financial institutions in complying with the requirements of the relevant legislations (that is, the FIAMLA and FIAML Regulations 2018), pertaining to ML and TF, financial crime and related offences, in order to protect the country's financial system from ML and TF abuses.

This Handbook aims to enhance understanding of FSC's expectations and help financial institutions assess the adequacy of their internal systems and controls and remedy deficiencies with the aim of combatting ML and TF. The purpose of the Handbook is to:

(a) assist financial institutions in understanding their obligations and complying with the requirements of the FIAMLA and FIAML Regulations 2018;

(b) provide guidelines to financial institutions in terms of best practice, in order to uphold the country's reputation as a sound international financial centre;

(c) set the minimum criteria to be followed by all financial institutions in the event that there is knowledge, suspicion or reasonable grounds to suspect ML and TF;

(d) promote the use of a proportionate, risk-based approach to CDD and Enhanced Due Diligence ("EDD") measures;

(e) promote strong internal controls within financial institutions;

(f) ensure compliance with international standards; and

(g) emphasise particular ML/TF risks of certain services and products offered by financial institutions in Mauritius.

This Handbook does not aim to prescribe an exhaustive list of recommended AML/CFT practices. A reasonable, proportionate and intelligent risk-based approach is required. Each financial institution must consider its own particular circumstances. This includes additional measures that may be necessary to prevent its exploitation and that of its products and services, by persons seeking to launder criminal property or to finance terrorism. The self-assessment questions and "good or poor practice" examples used in the Handbook are also non- exhaustive.

The examples of 'good practice(s)' depict situations in which financial institutions might comply with the applicable legal requirements. The Handbook is not the only source of guidance on ML and TF. Financial institutions are reminded that other international bodies like the Financial Action Task Force ('FATF') produce guidance that may also be relevant and useful.

The application of this Handbook should be on a risk-based proportionate way. This includes taking into account the size, nature and complexity of a financial institution when deciding whether good or poor practice exercised by the financial institution is relevant to its business.

Whilst the FSC recognises that financial institutions may already have systems and procedures in place which, although not identical to those outlined in the Handbook, would nevertheless be subject to controls and procedures imposed by the FSC and which are at least equal to if not higher than those contained in the Handbook. This will be taken into account by the FSC when assessing the adequacy of a financial institution's systems and controls.

1.4. Status of the Handbook

This Handbook is designed to provide guidance to all financial institutions. A financial institution is an institution, or a person, licensed or registered or required to be licensed or registered under –

(a) section 14, 77, 77A or 79A of the Financial Services Act;

(b) the Insurance Act;

(c) the Securities Act; or

(d) the Captive Insurance Act 2015.

The FSC issues guides for various purposes, including to illustrate and provide examples of best practice, and assist financial institutions in complying with legislation.

The guidance in this Handbook is not enforceable, but are illustrative to the extent that whoever follows it, would tend to indicate compliance with the legislative provisions (i.e FIAMLA and FIAML Regulations 2018), and vice versa.

1.5. Failure to Comply with FIAMLA and FIAML Regulations 2018

Section 32A and Regulation 33 of the FIAMLA and FIAML Regulations 2018 respectively set out the offences for contravening the requirements of the FIAMLA and FIAML Regulations 2018. Failure to comply with the FIAMLA and FIAML Regulations 2018 may result in regulatory action.

Failure to comply with the minimum requirements of the FIAMLA and FIAML Regulations 2018 may be regarded by the FSC as an indication of:

(a) conduct that is not in the best economic interests, or which damages the reputation of Mauritius; and/or

(b) lack of fitness and propriety.

The level of compliance of a financial institution and any assessment of the fitness and propriety of its controllers and beneficial owners or other key persons (such as Compliance Officer and Money Laundering Reporting Officer) where appropriate will therefore directly impact on the status of its licence.

This may therefore result in regulatory action and depending on the severity of the breach, it may result in revocation of a licence of a business. Actions under the Administrative Penalties Regulatory Framework (approved by the Board of the FSC on 24 July 2019 and issued on 19 August 2019) may also apply as appropriate.

The FSC will take this Handbook into account when assessing the level of compliance with the FIAMLA and FIAML Regulations 2018 while conducting its onsite visits.

1.6. Financial Action Task Force Recommendations

The Financial Action Task Force ('FATF') is an independent inter-governmental body that develops and promotes policies to protect the global financial system against ML, TF and the financing of the proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global standards in respect of AML/CFT.

A link to the 2012 FATF 40 Recommendations, upon which this guidance is based, can be found here.

1.7. Compliance Culture

The FSC recognises that effective AML/CFT policies and procedures can only be delivered through partnership with the industry and, accordingly, expects all financial institutions to ensure that they establish an open and positive approach to compliance and AML/CFT issues amongst all employees.

The board and senior management have a responsibility to ensure that a financial institution's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML/TF.

The board or senior management of a financial institution must establish documented systems and controls which:

(a) undertake risk assessments of its business and its customers;

(b) determine the true identity of customers and any beneficial owners and controllers;

(c) determine the nature of the business that the customer expects to conduct and the commercial rationale for the business relationship;

(d) require identification information to be accurate and relevant;

(e) require business relationships and transactions to be effectively monitored on an ongoing basis with particular attention to transactions which are complex, both large and unusual, or an unusual pattern of transactions which have no apparent economic or lawful purpose;

(f) compare expected activity of a customer against actual activity;

(g) apply increased vigilance to transactions and relationships posing higher risks of ML/TF;

(h) ensure adequate resources are given to the Compliance Officer to enable the standards within this Handbook to be adequately implemented and periodically monitored and tested;

(i) ensure procedures are established and maintained which allow the Money Laundering Reporting Officer ('MLRO') and the Deputy MLRO to have access to all relevant information, which may be of assistance to them in considering suspicious transaction reports ("STRs");

(j) require a disclosure to the Financial Intelligence Unit ("FIU") when there is knowledge or suspicion or reasonable grounds for knowing or suspecting ML and/or TF, including attempted ML and/or TF; and

(k) maintain records for the prescribed periods of time.

Financial institutions must adopt a robust approach and not refrain from asking their customers non-customary questions in circumstances of unusual activity. Any reluctance or failure by the customer to provide credible and verifiable answers should lead the financial institution to investigate the reason for this reluctance, establish any case for suspicion and follow up with appropriate action.

A hierarchical approach within a business may hinder an effective system of AML/CFT control, which financial institutions need to recognise and address. The human element is particularly important since policies and procedures only work if they are understood, followed and enforced by those required to comply with them. The hierarchical relationships between employees within a financial institution and with its customers can face the following damaging barriers:

(a) senior management being unwilling to lead on the concept of the need for sound corporate ethics;

(b) junior employees assuming that their concerns or suspicions are not significant;

(c) employees being unwilling to subject high value (therefore important) customers to effective CDD checks;

(d) management or customer relationship managers outside Mauritius pressurising employees in Mauritius to transact without obtaining all relevant CDD and business relationship information;

(e) employees being unable to understand the commercial rationale for customer relationships and the use of certain products / services, so that potentially suspicious activity is not identified;

(f) lack of time and/or resources to address concerns generating a tendency for line managers to discourage employees from raising concerns; and

(g) conflict between the desire on the part of employees to provide a confidential and efficient customer service and the requirement for employee vigilance in respect of prevention and detection of ML/TF.

1.8. Risk Based Approach

The FATF Recommendations provide for AML/CFT requirements, allowing a business to adopt a risk-based approach towards the prevention and detection of ML and TF.

It is very important to note that FIAMLA and FIAML Regulations 2018 do not prohibit or prevent any type of business, customers or systems from operating, unless they are involved in ML/TF. The legislation only requires that the risks posed by customers, products and systems are identified, mitigated and the mitigating factors/controls documented and reviewed periodically.

The application of a risk based approach provides a strategy for managing potential risks by enabling financial institutions to subject customers to proportionate controls and oversight. Financial institutions should avoid the "tick box" approach at all times, and always have to determine their risks themselves, based on their respective circumstances.

To demonstrate that a financial institution acted reasonably, an assessment of risk should always be documented, reasonably and objectively justifiable and sufficiently robust. Finally, while a risk based approach grants a wide degree of discretion, parameters set by law or regulation may limit that discretion.

1.8.1 What is risk?

Risk can be seen as a function of three factors and ideally, a risk assessment involves making judgments about all three of these elements:

- THREAT - person or group of people, an object or an activity with the potential to cause harm. The threats may vary across customers, countries, geographic areas, products/services and delivery channels
- VULNERABILITY – that which can be exploited by the threat or that may support or facilitate its activities, such as size and volume of the business and client base profile.
- CONSEQUENCE - the impact or harm that ML or TF may cause, such as the impact on reputation and imposition of regulatory sanctions.

1.8.2 What is mitigation?

Financial institutions must then take appropriate steps to mitigate any risks that have been identified. This will involve determining the necessary controls or procedures that need to be in place in relation to a particular part of the business in order to reduce the risk identified. The documented risk assessments that are required to be undertaken by Section 17 of the FIAMLA will assist the business to develop a risk based approach.

Systems and controls may not always prevent and detect all ML/TF. A risk-based approach will, however, serve to balance the cost burden placed on financial institutions and their customers, with a realistic assessment of the threat of a business being used in connection with ML/TF. It focuses effort where it is needed and has most impact.

1.9. Assessing Compliance with a Risk Based Approach

Financial institutions should avoid internal systems of control that encourages the 'tick box' approach rather than involving a thorough thought process, which is counter-productive. Internal systems should require employees to think about the risks posed by individual customers and relationships and to mitigate appropriately and document their thought process. The FSC must be able to see clear, documented rationale of how risks have been assessed and then how these risks have been mitigated or controlled.

In accordance with Regulation 31 of the FIAML Regulations 2018, any risk assessment systems used by the financial institution should be reviewed regularly to ensure an effective system is in place and swift action should be taken to remedy any identified deficiencies. This is further discussed in Chapter 4.

Chapter 2: Overview of Money Laundering, Terrorist Financing, and Proliferation offences

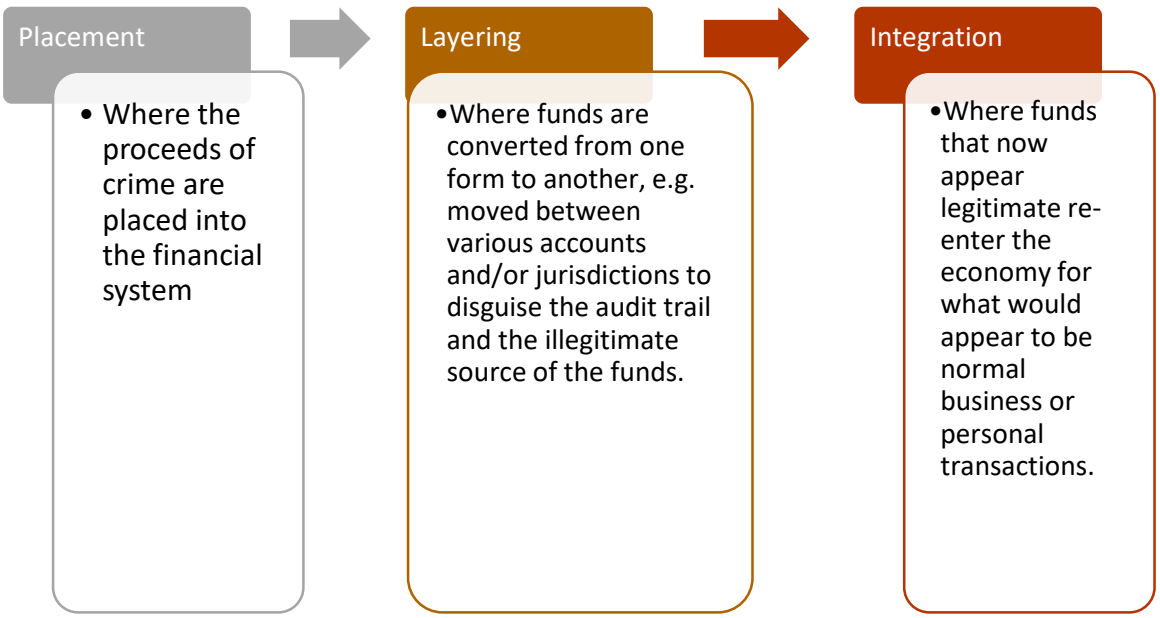
2.1 What is money laundering?

In general terms, ML is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the criminal property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their money or assets back to a crime.

Illegal arms sales, smuggling, and the activities of organised crime, including for example, drug trafficking and prostitution, can generate huge profits. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through ML. When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds or assets to a place where they are less likely to attract attention and disguising ownership and control.

Traditional money laundering model:

ML will often involve a complex series of transactions, traditionally represented in three separate phases.



Rather than getting caught up in trying to establish whether an activity relates to a particular phase of the traditional model, the financial institutions should ask themselves – "*do I know, suspect or have reasonable ground to suspect that the assets in question are derived from criminal activities?"* The assets does not have to be linked or suspected to be linked to a specific act of money laundering.

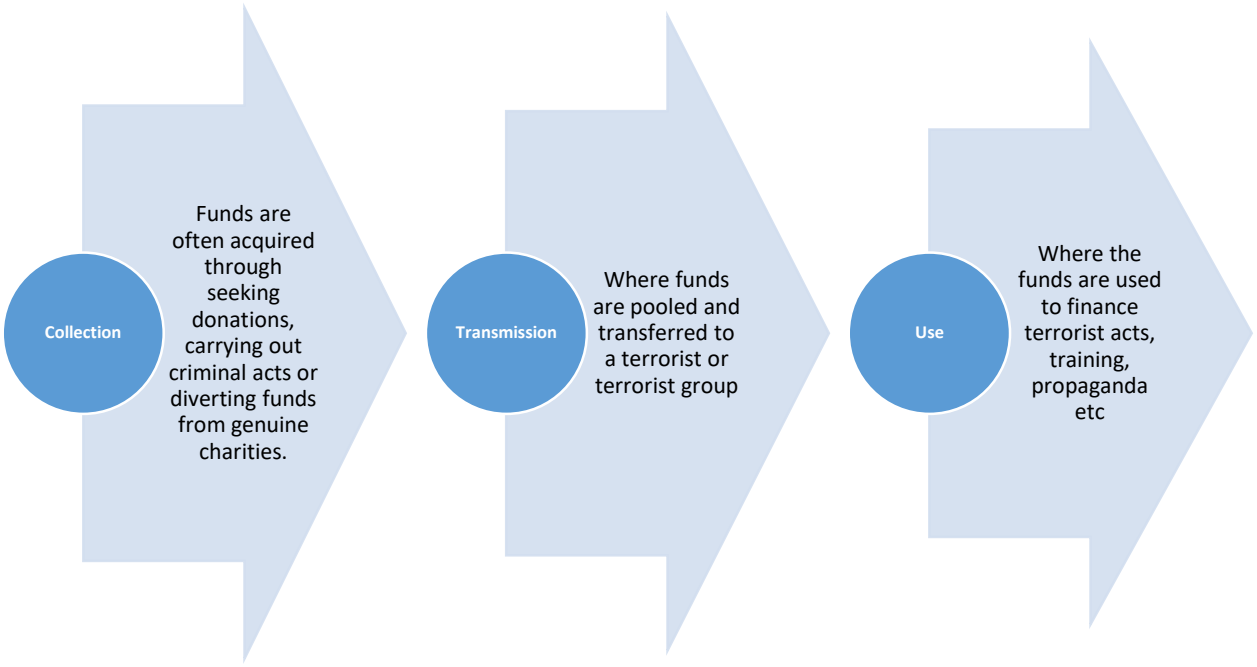
2.2 What is financing of terrorism?

In general terms, TF is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. TF differs from ML in that the source of funds can either be legitimate, such as an individual's salary, or illegitimate, like the proceeds of crimes such as selling pirate DVDs, fraud or drug trafficking.

Usually, the focus of scrutiny for potential terrorist financing activity will be the end beneficiary and intended use of the money or assets. A terrorist financier may only need to disguise the origin of the property if it was generated from criminal activity but in the vast majority of cases they will seek to disguise the intended use i.e. providing support to terrorists or supporting acts of terrorism.

Traditional terrorist financing model:

Terrorist financing often involves a complex series of transactions, generally considered as representing three separate phases and this could be sourced through various means for example through seeking donations, carrying out criminal acts and from genuine charities, as illustrated below



2.3 The consequences of money laundering and terrorist financing

Increased abuse of the financial system by criminal actors leads to increased criminal activity and less safety for everyone in the country and around the world. ML/TF can have serious negative consequences for the economy, national security and society in general. Some of these consequences may include:

(a) reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;

(b) attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;

(c) damaging the legitimate private sector who may be unable to compete against front companies;

(d) weakening of financial institutions which may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.;

(e) economic distortion and instability; or

(f) increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

2.4 What is the financing of proliferation of weapons of mass destruction?

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons, and their delivery systems (such as long range missiles).

Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks may use the international financial system to carry out transactions and business deals. Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology and expertise, providing seemingly legitimate front organisations or acting as representatives or middlemen.

2.5 Summary of Offences Relating to Money Laundering, Terrorist Financing, and Proliferation financing

The FIAMLA and FIAML Regulations 2018 states offences related to ML and TF (as explained above). Some of these offences, as applicable to financial institutions, are listed below for ease of reference:

Section 3 of the FIAMLA states:

(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) In FIAMLA, 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.

Section 4 of the FIAMLA states:

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.

Section 5 of the FIAMLA states:

(1) Notwithstanding section 37 of the Bank of Mauritius Act 2004, but subject to subsection (2), any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.
(2) Subsection (1) shall not apply to an exempt transaction.

Section 8 of the FIAMLA states:

(1) Any person who -
    (a) commits an offence under this Part; or
    (b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a fine not exceeding 2 million rupees and to penal servitude for a term not exceeding 10 years.
(2) Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.
(3) Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.

Section 16(3) (A) of FIAMLA states:
Legal consequences of reporting

Any person who fails to comply with subsection (1) 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.

Section 17(C) (6) of FIAMLA states:
Customer due diligence requirements

Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA 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.

Section 19 of FIAMLA states:
Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request

(1) Any bank, cash dealer, financial institution or member of a relevant profession or occupation or any director, employee, agent or other legal representative thereof, who, knowingly or without reasonable excuse -
    (a) fails to –
        (i) supply any information requested by the FIU under section 13(2) or 13(3) within the date specified in the request;
        (ii) make a report under section 14; or
        (iii)Any person who fails to comply with sections 17 to 17G shall commit an offence and shall, on conviction, be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.
    (b) destroys or removes any record, register or document which is required under FIAMLA or any regulations;
    (c) facilitates or permits the performance under a false identity of any transaction falling within this Part, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

(2) Any person who -
    (a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or
    (b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Section 19E of FIAMLA states:
Duty to provide information

Any person who fails to comply with a request made under subsection (2)(b) shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

FIAML Regulations 2018

Regulation 33 states that any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Chapter 3: Corporate Governance

3.1 Introduction

Good corporate governance should provide proper incentives for the board and senior management to pursue objectives that are in the interest of the firm and its shareholders and should facilitate effective monitoring of the firm for compliance with its AML and CFT obligations.

The presence of an effective corporate governance system, within an individual company and across an economy as a whole, is key to building an environment of trust, transparency and accountability.

3.2 Board Responsibility for Compliance

The Board of financial institutions is responsible for managing the institution effectively and is in the best position to understand and evaluate all potential risks to the financial institution, including those of ML and TF. The Board must therefore take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant.

On the basis of its business risk assessment, the Board must establish a formal strategy to counter money laundering and financing of terrorism. Where a financial institution forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for combatting money laundering and financing of terrorism, and, in particular, responsibilities of the Compliance Officer and MLRO.

The financial institution shall establish and maintain an effective policy, for which responsibility shall be taken by the Board, and such policy shall include provision as to the extent and frequency of compliance reviews. The Board should take a risk-based approach when defining its compliance review policy and ensure that those areas deemed to pose the greatest risk to the firm are reviewed more frequently.

The Board must consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the financial institution occur. Where, as a result of its review, changes to the compliance arrangements or review policy are required, the Board must ensure that the financial institution makes those changes in a timely manner.

As part of its compliance arrangements, the financial institution is responsible for appointing a Compliance Officer (‘CO’) who is responsible for the implementation and ongoing compliance

of the financial institution with internal programmes, controls and procedures in accordance with the requirements of the FIAMLA and FIAML Regulations 2018.

In addition to appointing a CO, an independent audit function to test the ML and TF policies, procedures and controls of the financial institution should be maintained.

The Board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the financial institution, including the risks identified in the business risk assessments. The policy must include a requirement for sample testing of the effectiveness and adequacy of the financial institution's policies, procedures and controls.

The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for ML and TF, and, in particular, responsibilities of the MLRO and Compliance Officer.

3.3 Foreign Branches and Subsidiaries

In accordance with Regulations 23(2) of the FIAML Regulations 2018, the financial institution shall ensure that any of its branch offices and, where it is a body corporate, any body corporate of which it is the majority shareholder or control of which it otherwise exercises, which, in either case, is a specified business in any country or territory outside Mauritius (collectively "its subsidiaries"), complies there with:

(i) the requirements of Regulations 23(2) of the FIAML Regulations 2018, and

(ii) any requirements under the law applicable in that country or territory which are consistent with the FATF Recommendations

The financial institution must be aware that the inability to observe appropriate AML/CFT measures is particularly likely to occur in countries or territories which do not, or insufficiently apply the FATF Recommendations. In such circumstances the financial institution must take appropriate steps to effectively deal with the specific ML and TF risks associated with conducting business in such a country or territory.

3.4 Key Persons

3.4.1. Compliance Officer

In accordance with Regulations 22 (1) (a) of FIAML Regulations 2018, the financial institution shall designate a Compliance Officer at senior management level and approved as officer under Section 24 of the FSA. The Compliance Officer ('CO') is 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 2018. Senior management is defined under the FIAML Regulations 2018 as an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

The CO appointed by the financial institution must:

(a) be a natural person;
(b) be of at least senior management level as defined under FIAML Regulations 2018;
(c) be an approved officer under Section 24 of the FSA; and
(d) have the appropriate qualification knowledge, skill and experience to fulfil a compliance role within the financial institution;

The financial institution must ensure that the CO:

(a) has timely and unrestricted access to the records of the financial institution;
(b) has sufficient resources to perform his or her duties;
(c) has the full co-operation of the financial institution staff;
(d) is fully aware of his or her obligations and those of the financial institution; and
(e) reports directly to, and has regular contact with, the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and FIAML Regulations 2018, and this Handbook are being met and that the financial institution is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

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

(a) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the financial institution and senior management;
(b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;
(c) regular reporting, including reporting of non-compliance, to the Board and senior management; and

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

While it is not anticipated that the CO will personally conduct all monitoring and testing, the expectation is that the CO will have oversight of any monitoring and testing being conducted by the financial institution.

The circumstances of the financial institution may be such that, due to the small number of employees, the CO holds additional functions or is responsible for other aspects of the financial institution's operations. Where this is the case, the financial institution must ensure that any conflicts of interest between the responsibilities of the CO role and those of any other functions are identified, documented and appropriately managed. The CO however should be independent of the core operating activities of the financial institution and should not be engaged in soliciting business.

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

3.4.2. Money Laundering Reporting Officer

In accordance with Regulations 26(1) of FIAML Regulations 2018, the financial institution shall appoint a MLRO to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

Regulation 26(4) of the FIAML Regulations 2018 states the MLRO shall:

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

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

The MLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required.

A financial institution should appoint a Deputy Money Laundering Reporting Officer ("DMLRO") in order to exercise the functions in the MLRO's absence. The DMLRO should

be of similar status and experience to the MLRO. Where this Handbook refers to the MLRO it implies the DMLRO in the MLRO's absence.

The MLRO appointed by the financial institution must:

(a) be a natural person;
(b) be an approved officer under Section 24 of the FSA; and
(c) have the appropriate knowledge, skill and experience in accordance with the Competency Standards issued by the FSC in October 2014;

The financial institution must ensure that the MLRO:

(a) is the main point of contact with the FIU in the handling of disclosures;
(b) has unrestricted access to the CDD information of the financial institution's customers, including the beneficial owners thereof;
(c) has sufficient resources to perform his or her duties;
(d) is available on a day-to-day basis;
(e) reports directly to, and has regular contact with, the Board or equivalent of the financial institution; and
(f) is fully aware of both his or her personal obligations and those of the financial institution under FIAMLA and FIAML Regulations 2018 and this Handbook.

Where the same person acts as MLRO on multiple financial institutions, he/ she should ensure that in accordance with FIAML Regulations 2018, he/ she has sufficient time and resources to effectively discharge his/ her functions. The FSC may require financial institutions to demonstrate the allocation of time and resources by the MLRO at onsite/ offsite reviews and failure to effectively and satisfactorily show the above may indicate non-compliance to Regulation 26(4) (b) of FIAML Regulations 2018.

Chapter 4: Risk Based Approach

4.1 Introduction

This chapter is designed to assist financial institutions in taking a risk-based approach to preventing its products and services from being used for the purposes of ML and TF. The three main sections are:

(a) Risk-Based Approach - which provides a high-level overview of the risk-based approach;

(b) Business Risk Assessments - which details the relevant requirements of Section 17(1) of the FIAMLA which states that financial institutions should take appropriate steps to identify, assess and understand the money laundering and terrorist financing risks for customers, countries or geographic areas and products, servicers, transactions or delivery channels; and

(c) Risk Factors - which provides for guidance and are provided as examples of factors that the financial institution might consider when undertaking a risk assessment of their relationship with their customers.

4.2 Risk-Based Approach

A risk-based approach towards the prevention and detection of ML and TF aims to support the development of preventative and mitigating measures that are commensurate with the ML and TF risks identified by the financial institution. This approach also aims to deal with those risks in the most cost-effective and proportionate way.

Section 17 of the FIAMLA provides for a duty for the financial institution to identify, assess and understand its money laundering and terrorism financing risks. Furthermore, section 17A of the FIAMLA requires a financial institution 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. In this respect the financial institution should:

(a) understand its ML and TF risks; and

(b) have in place effective policies, procedures and controls to:

  (i) identify,

  (ii) assess,

  (iii) understand

(iv) mitigate,

(v) manage, and

(vi) review and monitor, those risks in a way that is consistent with the requirements of section 17 of the FIAMLA and the requirements of this Handbook.

A risk-based approach starts with the identification and assessment of the risk that has to be managed. A risk-based approach requires the financial institution to assess the risks of how it might be involved in ML and TF, taking into account its customers (and the beneficial owners of customers), countries and geographic areas, the products, services and transactions it offers or undertakes, and the delivery channels by which it provides those products, services and/or transactions.

In determining how the risk-based approach should be implemented, the financial institution should analyse and seek to understand how the identified ML and TF risks affect its business. This determination should take into account a range of information, including (amongst others) the type and extent of the risks that the financial institution is willing to accept in order to achieve its strategic objectives (its "risk appetite"), its AML and CFT experience and the public version of the Mauritius National Risk Assessment ('NRA') Report which can be found at the following link: https://www.fscmauritius.org/en/being-supervised/amlcft/national-money-laundering-and-terrorist-financing-risk-assessment-of-mauritius-nra-report

Through the business risk assessments and determination of a risk appetite, the financial institution can establish the basis for a risk-sensitive approach to managing and mitigating ML and TF risks. It should be noted, however, that a risk-based approach does not exempt the financial institution from the requirement to apply enhanced measures where it has identified higher risk factors, as detailed in Chapter 6 of this Handbook.

A risk-based approach prescribes the following procedural steps to manage the ML and TF risks faced by the financial institution:

(a) identifying the specific threats posed to the firm by ML and TF and those areas of the firm's business with the greatest vulnerability;

(b) assessing the likelihood of those threats occurring and the potential impact of them on the financial institution;

(c) mitigating the likelihood of occurrence of identified threats and the potential for damage to be caused, primarily through the application of appropriate and effective policies, procedures and controls;

(d) managing the residual risks arising from the threats and vulnerabilities that the financial institution has been unable to mitigate; and

(e) reviewing and monitoring those risks to identify whether there have been any changes in the threats posed to the financial institution which necessitate changes to its policies, procedures and controls.

In applying a risk-based approach and taking the steps detailed above, it is crucial that, regardless of the specific considerations and actions of the financial institution, clear documentation is prepared and retained to ensure that the board and senior management can demonstrate their compliance with the requirements of Section 17 of the FIAMLA.

By adopting a risk-based approach the financial institution should ensure that measures to prevent or mitigate ML and TF are commensurate with the risks identified. In this respect, the business risk assessments will also serve to enable the financial institution to make decisions on how to allocate its resources in the most efficient and effective way and to determine its appetite and tolerance for risk.

No system of checks will detect and prevent all ML and TF risks. A risk-based approach will, however, serve to balance the cost burden placed upon the financial institution and its customers with a realistic assessment of the threat of the financial institution being used in connection with ML and/or TF. It focuses the effort where it is needed and has most impact.

4.2.1 Identification and Mitigation of Risks

Regulation 31 of the FIAML Regulations 2018 requires that a financial institution should establish and maintain appropriate procedures for monitoring and testing compliance with the Anti-Money Laundering or Combatting the Financing of Terrorism requirements, while ensuring it has robust and documented arrangements for managing the risks identified by the business risk assessment conducted, in accordance with Section 17 of the FIAMLA.

The financial institution's policies, procedures and controls must take into account the nature and complexity of its operations, together with the risks identified in its business risk assessments, and must be sufficiently detailed to demonstrate how the conclusion of each risk assessment with respect to relationships with customers has been reached.

4.2.2 Business Risks

Risk can be seen as a function of three factors and a risk assessment involves making judgements about all three of the following elements:

(a) threat – a person or group of persons, an object or an activity with the potential to cause harm;

(b) vulnerability – an opportunity that can be exploited by the threat or that may support or facilitate its activities; and

(c) consequence – the impact or harm that ML and TF may cause.

Having identified where it is vulnerable and the threats that it faces, the financial institution should take appropriate steps to mitigate the opportunity for those risks to materialise. The threats specific to the business can be identified by going through typology reports, notices published by the FSC, the FIU or other regulatory bodies, media articles, and other information that may be available internally at the financial institution. This will involve determining the necessary controls or procedures that need to be in place in order to reduce the risks identified. The documented risk assessments that are required to be undertaken by Section 17 of the FIAMLA, will assist the financial institution in developing its risk-based approach.

Retaining documentation on the results of the financial institution's risk assessment framework will assist the financial institution to demonstrate how it:

(a) identifies and assesses the risks of being used for ML and TF;

(b) adopts and implements appropriate and effective policies, procedures and controls to

(c) manage and mitigate ML and TF risk;

(d) monitors and improves the effectiveness of its policies, procedures and controls; and

(e) ensures accountability.

4.2.3 Accumulation of Risks

In addition to the individual consideration of each risk factor, the financial institution must also consider all such factors holistically, to establish whether their concurrent or cumulative effect might increase or decrease the financial institution's overall risk exposure and the dynamic that this could have on the controls implemented by the financial institution to mitigate risk.

Such an approach is relevant not only to the financial institution in its consideration of the risks posed to its business as part of undertaking its business risk assessments, but also in the consideration of the risk that individual business relationships or occasional transactions pose.

There are also other operational factors which may increase the overall level of risk and should therefore be considered in conjunction with the financial institution's ML and TF risks. An example of such factor could be the use of on-line or web-based services and cyber-crime risks which may be associated with those service offerings.

4.2.4 Weightage of Risk Factors

In considering the risk of a business relationship or occasional transaction holistically, the financial institution may decide to weigh risk factors differently depending on their relative importance. When weighting risk factors, the financial institution should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction.

This will likely result in the financial institution allocating varying 'scores' to different factors; for example, the firm may decide that a customer's personal links to a country, territory or geographic area associated with higher ML and/or TF risk is less relevant in light of the features of the product they seek.

Ultimately, the weight given to each risk factor is likely to vary from product to product and customer to customer (or category of customer). When weighting risk factors, the financial institution should ensure that:

(a) weighting is not unduly influenced by just one factor;

(b) economic or profit considerations do not influence the risk rating;

(c) weighting does not lead to a situation where it is impossible for any business relationship or occasional transaction to be classified as a high risk relationship;

(d) the provisions of Regulation 12(1) of FIAML Regulations setting out the situations which will present a high risk (for example, the involvement of PEPs or in event of suspicious activity) cannot be over-ruled by the financial institution's weighting; and

(e) it is able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

Where the financial institution uses automated IT systems to allocate overall risk scores to business relationships or occasional transactions and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score. The financial institution should be satisfied that the scores allocated reflect its understanding of ML and TF risk and it should be able to demonstrate this.

4.3 Business Risk Assessment

A financial institution must, under Section 17(1) of the FIAMLA identify, assess, understand and monitor that person's money laundering and terrorism financing risks.

While performing business, Management, Compliance and Risk Management should all work together on performing the Business Risk Assessment. Primarily, responsibility for the quality and execution of the risk analyses lies with the first line of defence. This is the business, as risks manifest themselves first there. The role of Compliance is process monitoring, facilitating and testing. Other functions or departments such as Audit can also provide the necessary input. The ultimate responsibility for the Business Risk Assessment lies with the board of directors.

As explained at Section 1.8.1 and 4.2.2 of this Handbook, a risk assessment involves making a judgement of a number of elements including threat, vulnerability and consequence.

It should also consider the extent of its exposure to risk by reference to a number of additional factors which are explained in this section. The examples provided are not exhaustive and other factors may need to be considered depending on the nature of the business and its activities.

A key component of a risk-based approach involves the financial institution identifying areas where its products and services could be exposed to the risks of ML and TF and taking appropriate steps to ensure that any identified risks are managed and mitigated through the establishment of appropriate and effective policies, procedures and controls.

The business risk assessments are designed to assist the financial institution in making such an assessment and provide a method by which the financial institution can identify the extent to which its business and its products and services are exposed to ML and TF. Good quality business risk assessments are therefore vital for ensuring that the financial institution's policies, procedures and controls are proportionate and targeted appropriately.

The financial institution must record and document its risk assessment in order to be able to demonstrate its basis. The assessment must be undertaken as soon as reasonably practicable

after the financial institution commences business and regularly reviewed and amended to keep it up to date. It is expected that this risk assessment is reviewed at least annually and in case of trigger events and this review should be documented to evidence that an appropriate review has taken place.

Risk management requires a systematic approach, it is a cyclical process. This means that a financial institution is expected to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at regular intervals. This is because risks are not static. Risks to financial institutions may change as a result of both internal and external factors. The financial institution's activities may for instance be expanded or changed, specific trends may emerge in the financial and economic world, or laws and regulations may be amended.

Since the risks of ML/FT vary from business to business and are not static, it is the responsibility of the financial institution to identify the vulnerabilities and risks faced, maintain an up to date understanding of these risks, and develop and implement appropriate strategies to mitigate and control those identified risks. This includes adjustment of such mitigation when needed. The appropriate strategy in order to manage and control those risks is to have an effective internal compliance culture under the board of directors' ultimate responsibility.

Any risks that have been identified should be properly mitigated by policies, procedures and controls. The financial institution should also document the mitigating factors and controls put in place to provide an audit trail of how the assessed risks have been mitigated.

Section 17(2) of the FIAMLA requires businesses to assess 6 key areas when undertaking the business risk assessment amongst other risk factors:

(i) the nature, scale and complexity of the financial institution's activities;

(ii) the products and services provided by the financial institution's;

(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.

As per Section 17(2) (b) of the FIAMLA, financial institutions shall take into account the findings of the National Risk Assessment ('NRA') and any guidance issued in their business risk assessment.

Each of the areas specified by the FIAMLA, and examples of what factors a financial institution should consider as a part of assessing these areas, are detailed as follows:

4.3.1 The nature, scale and complexity of its activities

- Consider the services provided by the business and how those services might be abused for ML/TF.

- Actively involve all members of senior management in determining the risks (threats and vulnerabilities) posed by ML/TF within those areas for which they have responsibility.
- Consider any organisational factors that may increase exposure to the risk of ML/TF e.g. business volumes and outsourcing aspects of regulated activities or compliance functions.
- Consider the nature, scale and complexity of its business including the diversity of its operations, the volume and size of its transactions, and the degree of risk associated with each area of its operation. Large volume and more complex transactions may pose higher risk of money laundering than less complex and voluminous transactions. However, this will also depend on the assessment of the area of operations and nature of business. As a whole, factors need to be considered together in order to have a more comprehensive assessment.
- Consider the jurisdictions in which the business operates, any particular threats from those jurisdictions, any particular vulnerabilities within the organisation in those jurisdictions. Regulation 24(1) of the FIAML Regulations 2018 states how high risk third countries should be identified.

➢ Risk factors that the financial institution can consider when identifying the effectiveness of a country's or territory's AML and CFT regime include:

(a) Has the country or territory been identified by a mutual evaluation as having strategic deficiencies in its AML and CFT regime? In accordance with Regulation 12(1)(c) of FIAML Regulations 2018, EDD measures shall be applied where a customer or an applicant for business is from a high risk third country.

(b) Is there information from more than one credible and reliable source about the quality of the country's or territory's AML and CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight? Examples of possible sources include mutual evaluation reports by the FATF or FATF-style regional bodies (in particular Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund ("IMF") assessments and Financial Sector Assessment Programme reports. The financial institution should note that membership of the FATF or a FATF-

style regional body does not, of itself, mean that the country's or territory's AML and CFT regime is adequate and effective.

- Consider the scale on which the services are provided and linked to this, any vulnerabilities in the level of compliance resources available.
- Consider whether the business model provides for complex structures and what risks this poses to the business.
- Consider the findings of the NRA in relation to the business sector.

4.3.2 The products and services provided by the financial institution

- Consider the vulnerabilities of the services or products offered and how they could be abused for ML/TF. Certain characteristics of the products and whether there are any increased vulnerabilities such as high volumes of cash, virtual currencies or untraceable/anonymous medium.
- Whether payments to any unknown or un-associated third parties are allowed. Such payments would entail higher risks.
- Whether the products/services/structure are of particular, or unusual complexity.

➢ When identifying the risk associated with the way in which the customer obtains the products or services they require, the financial institution should consider the risk related to:

(a) the extent to which the business relationship is conducted on a non-face-to-face basis; and

(b) any introducers of business or other intermediaries the financial institution might use and the nature of their relationship with the financial institution.

4.3.3 The persons to whom and the manner in which the products and services are provided

- Consider the threats posed by the types of customers. Some examples include, politically exposed persons ("PEPs"); high net worth individuals, those from or operating in a higher risk jurisdiction; and non-face-to-face business.
- The type of product should be considered, the higher risk products or services are more likely to be those with high values and volumes; where unlimited third party funds can

be freely received and those where funds can regularly be paid to third parties without CDD on the third parties being obtained.

- The speed with which products and services can be delivered or transactions undertaken.

Factors as above can be considered collectively such as the risk of provision of a service in a non-face-to-face manner to a PEP or risk imposed by a client dealing in securities in a high risk jurisdiction. Proper assessment would be effective when a comprehensive list of factors that is most relevant is taken into consideration as touchstones.

4.3.4 The nature, scale, complexity and location of the customer's activities

- Whether the customer base has any involvement in those businesses which are likely to be most vulnerable to corruption, such as oil, construction or arms sales.
- Consider jurisdictional factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect ML/TF in countries where it may have customers.
- The countries, territories and geographic areas with which customers (and the beneficial owners of customers) have a relevant connection.

➢ Risk factors the financial institution can consider when identifying the level of TF risk associated with a country or territory include:

(a) Is there information (for example, from law enforcement or credible and reliable open media sources) suggesting that a country or territory provides funding or support for terrorist activities or that groups committing terrorist offences are known to be operating in the country or territory?

(b) Is the country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU?

➢ Risk factors that the financial institution can consider when identifying the risk associated with the level of predicate offences to ML in a country or territory include:

(a) Is there information from credible and reliable public sources about the level of predicate offences to ML in the country or territory, for example, corruption, organised

crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UN Office on Drugs and Crime World Drug Report.

(b) Is there information from more than one credible and reliable source about the capacity of the country's or territory's investigative judicial system effectively to investigate and prosecute these offences?

- The complexity of customer and beneficial ownership structures.
- The complexity of legal persons and legal arrangements.
- The number of customers and beneficial owners which are charities or non-profit organisations ("NPOs") and their associated countries or geographic areas.

4.3.5 Reliance on third parties for elements of the customer due diligence process

Under Regulation 21 of the FIAML Regulations 2018, a financial institution may rely on a third party to introduce business or to perform the CDD measures. When reliance is placed on third parties, the following may be considered:

- Consider how reliance on third parties is prompted and agreed on.
- Consider who these third parties are, including any reputational issues, the quality of relationships with such third parties and previous experiences.
- Consider the extent and type of any reliance placed or to be placed on third parties.
- Consider the extent of the information being provided by the third party and who has actually met the customer face-to-face (chains of information).
- Consider any jurisdictional issues in connection with reliance placed on third parties.
- Consider the results of any testing undertaken on the third party's procedures and the responses to any previous requests for documentation.
- Consider the extent of any outsourcing undertaken.
- Consider the quality of the provider for any outsourced functions including any reputational issues, previous experiences with the provider, results of any audits, assessments or inspections where the material generated as a result of outsourcing has been reviewed.

The financial institution should also establish procedures to be satisfied that:

(i) the third party applies CDD measures and keeps records to a standard equivalent to the FATF Recommendations;

(ii) the third party will provide, immediately upon request, relevant copies of identification data in accordance with Regulation 21(2)(b) of the FIAML Regulations 2018; and

(iii) the quality of the third party's CDD measures is such that it can be relied upon.

4.3.6 Technological developments

Under Section 17(3) of the FIAMLA and Regulation 19(1) of the FIAML Regulations 2018, a financial institution should 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.

The financial institution should assess the use of developing technologies for both new and pre-existing products such as:

- digital information storage including cloud computing;
- digital or electronic documentation storage;
- electronic verification of documentation;
- data and transaction screening systems; or
- the use of virtual or digital currencies.

For completeness, the assessment should consider the operational risks, reputational risks and legal risks posed by the use of new technologies in the context of ML/TF. Appropriate action should be taken to mitigate the risks that have been identified.

4.3.6.1 Operational risks

Operational risks arise from the potential loss that could be incurred due to significant deficiencies in system reliability or integrity. Operational risks will also increase in proportion to the amount of reliance placed on outside service providers and external experts to implement, operate, and support portions of electronic systems.

Also, the rapid pace of technological change carries risk in itself. For example, staff may not fully understand the nature of new technology, resulting in operational problems with new or updated systems. Channels for distributing software updates could pose risks in that criminal or malicious individuals could intercept and modify the software.

It will have to be considered whether any of the factors above would have any impact in relation to the relevant person continuing to meet the AML/CFT requirements.

4.3.6.2 Reputational risks

Reputational risk may arise when systems or products do not work as expected and cause negative public reaction and when there are large AML/CFT failures as a result of unmitigated technology risks. In particular, if this affected systems were involved with the collection or maintenance of customer information, this may lead to serious reputational concerns. The event of this happening would have to be assessed by the financial institution and any risk should be mitigated. Testing of the systems is also recommended.

4.3.6.3 Legal risks

Legal risks arise from violations or non-compliance with legislation such as the FIAMLA and FIAML Regulations 2018. Financial institution may also face increased difficulty in applying traditional crime prevention and detection methods because of the remote access by customers of the systems.

It is recognised that where financial institution may be part of a larger group, the parent may introduce new products, systems or procedures without input from the Mauritius based branch. The financial institution should identify and mitigate any risks arising from the proposed system.

The above risk factors are non-exhaustive list and it is for the financial institution to assess and decide what is appropriate and relevant in the circumstances of the business. In cases, where not all the risk elements have been considered when conducting the business risk assessment, the financial institution has to demonstrate how effective and robust its business risk assessment is in line with its inherent risks and vulnerabilities and the Commission will assess to what extent the business risk assessment conducted reflect residual risks faced by the financial institution.

4.4 Customer Risk Assessments

The customer risk assessment estimating the risk of ML/TF must be undertaken prior to the establishment of a business relationship or carrying out an occasional transaction, with or for, that customer. This risk assessment must be documented in order to be able to demonstrate its basis. The customer risk assessment may have to take into account that not all CDD and relationship information might have been collected yet. It should be a living document that is revisited and reviewed, as and when more information about the customer and relationship is obtained. The customer risk assessment can be done on categories of clients (risk buckets), and it is not necessary to individually risk rate each client should the financial institution deem it appropriate.

The initial risk assessment of a particular customer will help determine:

- the extent of identification information to be sought;
- any additional information that needs to be requested;
- how that information will be verified; and
- the extent to which the relationship will be monitored on an ongoing basis.

Due care should be exercised under a risk-based approach. Being identified as carrying a higher risk of ML/TF does not automatically mean that a customer is a money launderer or is financing terrorism. Similarly, identifying a customer as carrying a lower risk of ML/TF does not mean that the customer presents no risk at all.

In order to complete a meaningful risk assessment, it is recommended that information should be gathered prior to the assessment, although this may not always be possible. Upon completion of the risk assessment any additional information, evidence or clarification should be sought in the event that circumstances remain unclear.

It should be noted that the FSC has no objection to a financial institution having higher risk customers, provided that they have been adequately risk assessed and any mitigating factors documented. If the customer is assessed as presenting a higher risk, EDD (as per Chapter 6 of this Handbook) must be obtained.

The following diagram sets out the basic risk assessment process:

When assessing the risks posed by a customer, the financial institution should consider all risk factors that are known and ensure that all of these factors are included into the customer's risk profile, taking care that any mitigating factors are fully documented. A financial institution must be able to objectively and reasonably justify a risk assessment classification and document those justifications. The financial institution should also ensure that its internal sign off procedure in relation to customer risk assessments is appropriate.

The FSC would expect a financial institution to avoid a tick box approach when assessing risks and consider each customer on a case by case basis or in group risk- rated buckets based on their profiles, looking at any risks they pose along with any mitigating factors. The customers may be risk rated using a risk matrix as follows:

	Nature, Scale, Complexity	***Products and Services***	***Clients***	***Geography***	***Delivery Channels***	***Total Risk Rating***
Client 1/ Bucket 1 e.g Fintech	Low	Medium	Medium	Low	Low	Low
Client 2/ Bucket 2	Medium	High	High	Medium	High	High
Client 3/ Bucket 3	Medium	Medium	High	Low	Low	Medium

Factors used should be documented and details should be provided on how any risks identified would be mitigated. The FSC would have no objection to templates or forms being used during the risk assessment, however it should be carefully considered how these work, what the scoring system is and how the score is reviewed / overridden. It should also be ensured that the score only takes into account factors relevant to ML/TF.

As with business risk assessments, customer risk assessments must be reviewed on a regular basis to ensure they remain up to date and to assess any changes of the risk profile due to changes in the customer's circumstances. It is expected that the review of the risk assessment is documented to evidence that an appropriate review has taken place.

Regarding frequency of the reviews, customer risk assessments should be reviewed:

- at least annually for higher risk customers or whenever a transaction with a high risk country or high risk customer occurs;
- at least every 3 years for standard risk customers subject to sector specific guidance; and
- at the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

The above are only examples of suggested review frequency, financial institution may decide to different frequency level should their business and client risk assessments merit same. However, in cases where the financial institution determine different schedules for reviews, this should be justified and properly documented.

4.5 Risk Factors

The risk factors included within the following sections are purely for guidance and are provided as examples of factors that the financial institution might consider when undertaking a risk assessment of the relationship they have with their customers. The following factors are not exhaustive and are not prescribed as a checklist. It is for the financial institution to assess and decide what is appropriate in the circumstances of the business relationship and it is not expected that all factors will be considered in all cases.

If it is determined, through a relationship risk assessment, that there are types of customer, activity, business or profession that are at risk of abuse from ML and/or TF, then the financial institution should apply higher AML and CFT requirements as dictated by the relevant risk factor(s).

4.5.1 Customer Risk Factors

When identifying the risk associated with its customers, including the beneficial owners of customers, the financial institution can consider the risk related to:

(a) the customer's (and beneficial owner's) business or professional activity;

(b) the customer's (and beneficial owner's) reputation; and

(c) the customer's (and beneficial owner's) nature and behaviour.

- Risk factors that may be relevant when considering the risk associated with a customer's or beneficial owner's business or professional activity may include:

(a) Does the customer or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the extractive industries or public procurement?

(b) Does the customer or beneficial owner have links to sectors that are associated with higher ML and/or TF risk, for example, certain money service providers ("MSPs"), casinos or dealers in precious metals?

(c) Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

(d) Where the customer is a legal person or legal arrangement, what is the purpose of their establishment? For example, what is the nature of their business?

(e) Does the customer have political connections, for example, are they a PEP, or is the beneficial owner a PEP? Does the customer or beneficial owner have any other relevant

links to a PEP, for example, are any of the customer's directors PEPs and, if so, do these PEPs exercise significant control over the customer or beneficial owner? In line with Regulation 12(1) of FIAML Regulations 2018, where a customer or the applicant for business is a PEP, the financial institution shall apply EDD measures.

(f) Does the customer or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? For example, are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision-makers?

(g) Is the customer a legal person subject to enforceable disclosure requirements that ensure reliable information about the customer's beneficial owner is publicly available, for example, public companies listed on stock exchanges that make such disclosure a condition for listing?

(h) Is there evidence that the customer has been subject to supervisory sanctions or enforcement for failure to comply with AML and CFT obligations or wider conduct requirements in recent years?

(i) Is the customer a public administration or enterprise from a country or territory with high levels of corruption?

(j) Is the customer's or the beneficial owner's background consistent with what the firm knows about their former, current or planned business activity, their business's turnover, the source of funds and the customer's or beneficial owner's source of wealth?

- The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owners' reputation:

(a) Are there adverse media reports or other relevant sources of information about the customer, for example, are there any allegations of criminality or terrorism against the customer or the beneficial owner? If so, are these reliable and credible? The financial institution should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations.

(b) Has the customer, beneficial owner or anyone publicly known to be closely associated with them, had their assets frozen due to administrative or criminal proceedings or

allegations of terrorism or TF? Does the firm have reasonable grounds to suspect that the customer or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?

(c) Does the firm know if the customer or beneficial owner has been the subject of an internal or external disclosure in the past?

(d) Does the firm have any in-house information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?

- The following risk factors may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour. The financial institution should note that not all of these risk factors will be apparent at the outset, they may emerge only once a business relationship has been established:

(a) Does the financial institution has any doubts about the veracity or accuracy of the customer's or beneficial owner's identity?

(b) Are there indications that the customer might seek to avoid the establishment of a business relationship? For example, does the customer look to carry out one transaction or several one-off transactions where the establishment of a business relationship might make more economic sense?

(c) Is the customer's ownership and control structure transparent and does it make sense? If the customer's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?

(d) Does the customer issue bearer shares or does it have nominee shareholders?

(e) Is the customer a legal person or legal arrangement that could be used as a personal asset holding vehicle?

(f) Is there a sound reason for changes in the customer's ownership and control structure?

(g) Does the customer request transactions that are complex, unusual or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale? Are there grounds to suspect that the customer is trying to evade specific thresholds, such as those subject to mandatory reporting, either in Mauritius or the customer's home country or territory?

(h) Does the customer request unnecessary or unreasonable levels of secrecy? For example, is the customer reluctant to share identification data, or do they appear to want to disguise the true nature of their business?

(i) Can the customer's or beneficial owner's source of funds or source of wealth be easily established, for example, through their occupation, inheritance or investments?

(j) Does the customer use the products and services they have taken out as expected when the business relationship was first established?

(k) Is the customer an NPO whose activities could be abused for TF purposes?

4.5.2 Countries and Territories Risk Factors

When identifying the risk associated with countries and territories, the financial institution can consider the risk related to those countries and territories with which the customer or beneficial owner has a relevant connection. These are detailed at 3.2.1 and 3.2.4. Additionally, the following can be considered:

The financial institution should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors.

For example:

(a) Where the funds used in the business relationship or occasional transaction have been generated abroad, the level of predicate offences to ML and the effectiveness of a country's or territory's legal system will be particularly relevant.

(b) Where funds are received from, or sent to, countries or territories where groups committing terrorist offences are known to be operating, the financial institution should consider to what extent this could be expected to, or might give rise to, suspicion based on what the financial institution knows about the purpose and nature of the business relationship or occasional transaction.

(c) Where the customer or beneficial owner is a legal person or legal arrangement, the firm should take into account the extent to which the country or territory in which the customer or beneficial owner is registered effectively complies with international tax transparency standards.

- Risk factors that the financial institution can consider when identifying a country's or territory's level of transparency and tax compliance include:

(a) Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards? Is there evidence that relevant rules are effectively implemented in practice?

Examples of possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the OECD, which rate jurisdictions for tax transparency and information sharing purposes; assessments of the country's or territory's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 of the FATF Recommendations by the FATF or FATF-style regional bodies; and IMF assessments (for example, IMF staff assessments of offshore financial centres).

(b) Has the country or territory committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?

(c) Has the country or territory put in place reliable and accessible beneficial ownership registers?

- Risk factors the firm should consider when identifying the risk associated with the level of predicate offences to ML in a country or territory include:

(a) Is there information from credible and reliable public sources about the level of predicate offences to ML in the country or territory, for example, corruption, organised crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the UN Office on Drugs and Crime World Drug Report.

(b) Is there information from more than one credible and reliable source about the capacity of the country's or territory's investigative judicial system effectively to investigate and prosecute these offences?

4.5.3 Products, Services and Transactions Risk Factors

- When identifying the risk associated with its products, services or transactions, the financial institution can consider the risk related to:

(a) the level of transparency, or opaqueness, the product, service or transaction affords;

(b) the complexity of the product, service or transaction; and

(c) the value or size of the product, service or transaction.

- Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency include:

(a) To what extent do products or services allow the customer or beneficial owner structures to remain anonymous, or facilitate hiding their identity? Examples of such products and services include bearer shares, fiduciary deposits, personal asset holding vehicles, and legal entities such as foundations that can be structured in such a way as to take advantage of anonymity and allow dealings with shell companies or companies with nominee shareholders.

(b) To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example, in the case of certain correspondent banking relationships?

- Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity include:

(a) To what extent is the transaction complex and does it involve multiple parties or multiple countries or territories, for example, in the case of certain trade finance transactions? Are transactions straightforward, for example, are regular payments made into a pension fund?

(b) To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected? Where third party payments are expected, does the firm know the third party's identity, for example, is it a state benefit authority or a guarantor?

(c) Does the financial institution understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?

- Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size include:

(a) To what extent are products or services cash intensive, for example, many payment services and certain current accounts?

(b) To what extent do products or services facilitate or encourage high-value transactions?

(c) Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML and TF purposes?

Chapter 5 - Customer Due Diligence ('CDD')

Financial institutions must identify their customers, and where applicable, their beneficial owners and then verify their identities, which is essential to the prevention of money laundering and combatting the financing of terrorism. CDD is the means by which financial institutions achieve such knowledge and is a key element of any internal AML/CFT system.

This chapter sets out the minimum CDD requirements and establishes a framework by which a financial institution should develop a risk-based approach to deciding the type and extent of CDD measures to apply to different types of customers, products and services.

Identification and verification refers to establishing and verifying a customer's identity. Verification refers to the verification of elements of the identification information, by using independent reliable sources, which may include material obtained from the customer such as a passport to verify the customer's name. It is essentially the concept of the financial institution satisfying itself that its customer is who they say they are.

The inadequacy or absence of satisfactory CDD measures can subject a financial institution to serious customer and counterparty risks, as well as reputational, operational, legal and regulatory risks, any of which can result in significant financial cost to its business.

Effective CDD measures are vital because they:

(a) help to protect the financial institution and, more widely, the integrity of the financial system of the jurisdiction and globally, by reducing the likelihood of the financial institution's business becoming a vehicle for, or a victim of, financial crime;

(b) assist law enforcement agency, by providing it with relevant information ascertained via CDD in the event of a suspicious transaction report ('STR'); and

(c) constitute an essential part of sound risk management, for example by providing the basis for identifying, limiting and controlling the risk posed by particular customers or classes of customers.

Financial institutions must routinely consider the risks that all such relationships pose to them and the manner in which those risks can be limited. To do so, financial institutions must be able to demonstrate the effective use of documented CDD information. CDD information is also a vital tool for the MLRO and business employees when examining unusual or higher risk activity or transactions, in order to determine whether a STR will be appropriate.

CDD measures that should be undertaken by the financial institution under the relevant legislation include:

(a) identifying and verifying the identity of each applicant for business;

(b) identifying and verifying the identity of individuals connected to the account or transaction, such as the customer's beneficial owner(s)[1];

(c) obtaining information on the purpose and intended nature of the business relationship (the inability for employees of the financial institution to understand the commercial rationale for business relationship may result in the failure to identity non-commercial and therefore potential money laundering and financing of terrorism activity);

(d) conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout the course of that relationship, to ensure that the transactions in which the customer is engaged are consistent with the financial institution's knowledge of the customer and its business and risk profile (including the source of funds). Further reference can be made to Chapter 9;

(e) achieving each of the above measures by using reliable, independently sourced documents, data or information (this is intended through the use of commercial databases and public information); and ensuring that all material collected under the CDD process is kept relevant and up to date (for example undertaking reactive reviews in response to trigger events, and by undertaking regular planned reviews of existing records at intervals determined by risk rating, with higher risk customers warranting more frequent reviews).

If a financial institution forms a suspicion that one or more actual or proposed transactions relates to money laundering or terrorist financing, it should take into account the risk of tipping off when performing the CDD process. If the financial institution reasonably believes that performing the CDD process will tip off the customer or potential customer, it should stop the CDD process and will need to file a STR in such circumstances. This should be included in the employee training programme as described in Chapter 12.

An applicant for business may be an individual acting on his own behalf or for others (for example, a trustee of an express trust), or a legal body or legal arrangements seeking to enter into or having entered into a business relationship or to conduct a one-off transaction, as principal or on behalf of a third party.

[1] The FSC considers the beneficial owner(s) as the natural person(s) who ultimately owns or has control over a customer or the person(s) on whose behalf a transaction is being conducted. This also includes those natural person who exercise ultimate control over a legal person or arrangement and such other persons as may be specified in Regulations 6 and 7 of FIAML Regulations 2018.

A financial institution is required to take reasonable measures at the time of establishing a business relationship to determine whether the applicant for business is acting on behalf of a third party. If the financial institution determines that the applicant is acting for a third party, then it must keep a record setting out –

(a) the identity of the third party (and any beneficial owners or associated persons as required);

(b) the proofs of identity required under Regulation 3 of the FIAML Regulations 2018; and

(c) the relationship between the third party and the applicant for business.

Where CDD measures are required to be undertaken, financial institutions must apply the CDD measures listed above in order to enable a customer profile to be prepared.

In applying CDD measures, financial institutions will be expected to follow a risk-based approach as provided in Chapter 4 of this Handbook while meeting the standards set out in legislation. A risk-based approach to CDD is one that involves a number of steps in assessing the most effective and proportionate way to manage the money laundering and financing terrorism risk faced by a financial institution.

In light of the information obtained, a financial institution must carry out and maintain a risk assessment of the applicant, taking into account all the relevant factors. The financial institution will allocate a risk rating based on the client profile, geography and other factors that the financial institution deemed necessary on a risk based approach. Further guidance is provided under Chapter 4.

The risk assessment of a particular applicant will determine the extent of identification information (and other CDD information) that will be requested, how that information will be verified, and the extent to which the resulting relationship will be monitored. Chapter 4 provides further guidance on the above.

Systems and controls will not detect and prevent all instances of money laundering or the financing of terrorism. A risk-based approach will, however, serve to balance the cost burden placed on a financial institution and on applicants and customers with the risk that the business may be used in money laundering or to finance terrorism by focusing resources on higher risk areas.

Care nevertheless has to be exercised under a risk-based approach. Being identified as carrying a higher risk of money laundering does not automatically mean that a customer is a money launderer or is financing terrorism and vice versa.

The extent of customer relationship information sought in respect of a particular applicant, or type of applicant, will depend upon the jurisdictions with which the applicant is connected, the

characteristics of the product or service requested, how the product or service will be delivered, as well as factors specific to the applicant and the associated risk ratings.

Financial institutions must keep and maintain customer relationship information with respect to all its customers as detailed in the CDD measures listed above. This would include scrutinising the source of funds and the source of wealth. The source of funds normally refers to the origin of the particular funds or assets which are the subject of the business relationship between the financial institution and its client and the transactions the financial institution is required to undertake on the client's behalf (e.g. the amounts being invested, deposited or remitted). The source of funds requirement refers to where the funds are coming from in order to fund the relationship or transaction. This does not refer to every payment going through the account, however the financial institution must ensure it complies with the ongoing monitoring provisions as laid out in Chapter 9 of this Handbook.

The source of wealth is distinct from source of funds and describes the origins of a customer's financial standing or total net worth i.e. those activities which have generated a customer's funds and property. A financial institution is required to hold sufficient information to establish the source of wealth and this information must be obtained for all higher risk customers (including higher risk domestic PEPs) and all foreign PEPs and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile.

For express trusts the CDD information should provide the type of trust (e.g. discretionary), the structure of any underlying legal bodies (if applicable) and nature of activities undertaken by the trust and any underlying legal bodies. And this should also include the classes of beneficiaries and classes within an expression of wishes.

A financial institution must periodically update relevant CDD information and its risk assessment throughout the business relationship with each customer as provided in Chapter 9 of this Handbook. In the event of any material change (for example, in beneficial ownership or control of the applicant / customer or the third parties on whose behalf the applicant/customer acts, or an adverse change in the financial institution's perception of the reliability of the CDD information it already holds), then reasonable further measures should be taken to verify identity of the applicant/customer.

Financial institution s must ensure that there is consistency between the information they hold on the applicant /customer and the nature of transactions or proposed transactions. Where there is any indication of abnormal or potentially suspicious activity within the context of the product or service being provided, or any other event occurs to cast doubt on the CDD held by the financial institution, then the financial institution must take additional measures to verify the information already obtained and to obtain such further information as may be necessary.

5.1 Identification and verification

A financial institution must, on the basis of the relevant CDD information collected, make an analysis of the information provided and make such appropriate verification using external database or source, and consider whether it is appropriate to collect further CDD information. CDD information comprises both identification and verification information and customer relationship information.

Regulation 3(1) of the FIAML Regulations 2018 imposes an obligation for a financial institution to identify his customer whether permanent or occasional and verify the identity of his customer. Financial institutions should note that failure to identify and verify customers is an offence under the FIAMLA.

Financial institutions must have in place clear, documented procedures governing how they will:

(a) identify and verify the identity of their applicants for business and existing customers on a risk based approach (including identifying and verifying the identity of any connected individuals such as beneficial owners and controllers of the applicant);

(b) determine whether or not an applicant for business is acting or intending to act for a third party; and

(c) where the financial institution is unable to determine whether the applicant is acting for a third party or not, make a suspicious activity report pursuant to section 14 of the FIAMLA to the Financial Intelligence Unit.

These procedures must be brought to the knowledge of and be readily available to all relevant staff for the creation of an effective internal compliance culture and all staff will be aware of the reporting chain and procedures to follow.

All relevant employees must receive ongoing training that is tailored to their role and responsibilities within the business as detailed in Chapter 12 of the Handbook.

5.2 Natural Persons

Regulation 4 of the FIAML Regulations 2018 lays down specific requirements for natural persons (applicants or beneficial owners/controllers of applicants).

A financial institution must collect the identification data on a natural person, and verify that data, in accordance with the following:

(a) The data to be collected applies to both standard and high risk applicants for business.

(b) The appropriate number of methods for verifying the data will vary depending on whether the customer is standard or high risk.

5.3 Identification and Verification data for natural persons

TABLE 1

Data to be collected:	Permissible methods for verifying data:
1. Legal name (including any former names, aliases and any other names used) 2. Sex 3. Date of birth 4. Place of birth 5. Nationality	• current valid passport • current valid national identity card • current valid driving licence (where the Financial institution is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence) In each case, the document must incorporate photographic evidence of identity. Where the legal person with which the natural person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However where the legal person is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
6. Current residential address. PO Box addresses are not acceptable 7. Permanent residential address (if different to current residential address)	• any of the identity sources listed above; • a recent utility bill issued to the individual by name; • a recent bank or credit card statement; or • a recent reference or letter of introduction from (i) a financial institution that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or (iii) a branch or subsidiary of a group headquartered in a well-regulated overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the

		application of, and compliance with, such standards. 'recent' means within the last three months.
8.	Any public position held and, where appropriate, nature of employment (including self-employment) and name of employer	A letter or other written confirmation of the individual's status from the public body in question and or any enhanced CDD; a letter or other written confirmation of employment.
9.	Government issued personal identification number or other government issued unique identifier	The relevant government document.

Where a particular aspect of an individual's identity changes (such as change of name, nationality, or any other forms as approved), a financial institution must take reasonable measures to re-verify that particular aspect of identity of the individual using the same methods prescribed by the table above. In case of high risk customers, further verification should take place either using a newly issued replacement for the expired document.

5.4 Applicants for business who are Legal Persons or Legal Arrangements

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

For customers that are legal persons, financial institutions should identify and verify the identity of beneficial owners by obtaining information on –

(a) the identity of all the natural persons who ultimately have a controlling ownership[2] interest in the legal person;

(b) where there is doubt under subparagraph (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 effective control of the legal person; and

[2] A controller is person who is able to control or exert significant influence (through shareholding interest or otherwise) over, the business or financial operations of a company whether directly or indirectly

(c) where no natural person is identified under subparagraph (a) and (b), the identity of the natural person who holds the position of senior managing official[3].

Where the underlying shareholders are not natural persons, financial institutions must 'drill down' to establish the identity of the natural persons ultimately owning or controlling the business. A legal person may have one or more methods of data verification as provided in the right column and the method of data verification will apply according to the legal status of the person to be identified.

5.5 Identification and verification data for legal person

TABLE 2

Person to be identified	Data to be identified	Method of data verification
Underlying persons who are individuals.	As per the requirements for natural person Where the individual persons are such by virtue of their status as members of the board of directors of a relevant legal person (or equivalent – for examples partners in a partnership [4], or council members in a foundation), financial institutions are required to identify and verify the identity of all such persons.	As per the requirements for natural person Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However where the legal person is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary

[3] "senior management" includes an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

[4] Including the General Partner(s) and Limited Partners under a Limited Partnership.

Private companies Partnerships Sociétés Foundations Other legal persons	1. Legal status of body 2. Legal name of body 3. Any trading names 4. Nature of business 5. Date and country of incorporation / registration 6. Official identification number (for example, company number) 7. Registered office address 8. Mailing address (if different) 9. Principal place of business / operations (if different) 10. Any other data which the financial institution considers to be reasonably necessary for the purposes of establishing the true identity of the legal person.	• Certificate of incorporation (or other appropriate certificate of registration or licensing); • Memorandum and Articles of Association (or equivalent); • Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; • Latest audited financial statements or equivalent; • Annual report or equivalent; • Personal visit to principal place of business; • Partnership deed or equivalent; • Charter of Foundation; • *Acte de société;* • Certificate of good standing from a relevant national body; • Reputable and satisfactory third party data, such as a business information service • Any other source of information that to verify that the document submitted is genuine.

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

Where a financial institution intends to use data held by a third party organisation, such data must be satisfactory and the organisation reputable. Such criteria will be likely to be satisfied where the organisation:

(a) accesses a wide range of information sources; and

(b) has transparent processes that enable a financial institution to know what checks have been carried out, what the results of these checks were and to be able to determine the level of satisfaction provided by those checks.

5.6 Legal arrangements

For customers that are legal arrangements, financial institution s should identify and verify the identity of beneficial owners–

(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.

A financial institution must collect the identification data concerning a legal person listed in the left-hand column of the table below, and verify that data in accordance with the following:

(a) The data to be collected applies to low, standard and high risk applicants for business. Potential methods of data verification are listed in the right-hand column of the table.

(b) The appropriate number of methods for verifying the data will vary depending on the status of the person to be identified and the risk rating:

  (i) For low risk legal persons, verification of each piece of the required data may take place using one of the methods identified.

  (ii) For standard and high risk legal persons, verification of each item of the required data must take place using at least two such methods wherever practicable.

5.7 Identification and verification data for legal arrangement

TABLE 3

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

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

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

5.8 Acquisition of a business or block of customers

Where a financial institution takes on a business which has established business relationships or a block of customers, a financial institution shall undertake sufficient enquiries to determine:

(a) whether the business's CDD policies, procedures, controls and systems are in line with current AML/CFT legislative requirements;

(b) the level and the appropriateness (having regard to risk) of identification data held in relation to the customers and business relationships which are to be acquired.

In deciding whether to acquire the business, a financial institution may rely on the identification data held where:

(a) The business relationships were established in jurisdictions that have equivalent AML/CFT legislation or meets the FATF Standards;

(b) The business' CDD policies, procedures and controls are in line with the AML/CFT legislative framework;

(c) The financial institution has obtained identification data for each customer acquired.

Where deficiencies in the identification data held are identified, either at the time of transfer/acquisition or subsequently, the financial institution must determine and implement a programme to remedy any such deficiencies, prioritised according to its assessment of the risks.

5.9 Individuals acting on behalf of applicants for business and customers

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

with financial institution s – for example, persons authorised to instruct the financial institution to transfer funds on the customer's behalf. Such authority may derive from a number of possible sources: for example, a power of attorney, or an authorised signatory mandate form, or a trust instrument.

Financial institution s must have in place appropriate policies, procedures and controls to ensure that they are able to identify and verify the identity of all persons purporting to act on behalf applicants for business or existing customers, and to confirm the authority of such persons to act.

Financial institution s must, in the case of individuals acting on behalf of applicants for business or existing customers, obtain identification data and verify that data in accordance with the Table 1 above.

Where a particular aspect of the above identification data subsequently changes or expires, a financial institution must take reasonable measures to re-verify that particular aspect of identity of the individual.

5.9.1 Third party reliance

A financial institution may rely on relevant third parties to complete certain customer due diligence ("CDD") measures, provided that there is a contractual arrangement in place with the third party and the third party provides all CDD information to the financial institution (but the document can be provided at a later stage and upon request) and undertakes to provide to the firm any CDD documents obtained as soon as practicable upon request pursuant to section 17D of the FIAMLA. Where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the financial institutions relying on the third party. Further guidance is provided in Chapter 8.

5.10 Electronic identification and verification

Where a financial institution adopts a system providing for the electronic verification of natural person identity, the financial institution must assess the veracity of the controls inherent within the system in order to determine whether the financial institution can place reliance on the results produced, or if additional steps are necessary to complement the existing controls.

The additional steps undertaken by the financial institution could include requiring a representative of the financial institution or a designated third party for example a lawyer, a notary or an accountant to be present with the natural person when the on-boarding software is being used.

Whilst the use of electronic verification can help to reduce the time and cost involved in gathering information and identification data for a natural person, the financial institution should be mindful of any additional risks posed by placing reliance on an electronic method or system. This should include understanding the method and level of review and corroboration within the system and the potential for the system to be abused.

Knowledge and understanding of the functionality and capabilities of a system can help provide assurance of its suitability. In particular, there should be certainty of the methods applied to corroborate identification data. The use of more than one confirmatory source to match data enhances the assurance of authenticity. A process whereby the images taken are independently verified, either by a suitably trained individual or computer system, to confirm the authenticity of the identification data used to verify identity (for example, that the identification data has not been fraudulently altered, is listed on a missing/stolen documents list, etc.). The corroboration of biometric information (for example, finger prints, voice identification, etc.) and/or geotagging/geolocation (i.e. the inclusion of geographical identification metadata to confirm the location in which the user interacted with the system) could be done.

In all circumstances, the financial institution should adopt a risk based approach to satisfy itself that the documents received adequately verify that the customer is who they say they are and that the financial institution is comfortable with the authenticity of these documents. The financial institution could check the type of file and ensure it is tamper resistant, it could check the email address it is being received from to ensure it seems legitimate and relates to the customer sending in the documentation, if the document has been certified that it is a suitable certifier etc.

Where the financial institution is unsure of the authenticity of the documents based on electronic means of collection, or that the documents actually relate to the customer, a cumulative approach should be taken and additional measures or checks undertaken to gain comfort. If still unsatisfied with the verification of identity or address the business relationship must proceed no further, the financial institution must terminate the business relationship and consideration be given to making an internal disclosure.

Chapter 6: Enhanced Due Diligence

Regulation 12 of the FIAML Regulations 2018 provides that financial institutions shall implement internal controls and other procedures to combat money laundering and financing of terrorism, including EDD procedures with respect to high-risk persons, business relations and transactions and persons established in jurisdictions that do not have adequate systems in place to combat money laundering and financing of terrorism.
Where the ML/TF risks are identified to be higher, a financial institution shall take EDD measures to mitigate and manage those risks.

Financial institutions must assign a high risk rating to the applicant for business where a high risk of ML/TF has been identified. This is explained in details in the risk based approach and customer due diligence chapters of this Handbook.

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

(a) requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;
(b) obtaining additional information on the intended nature of the business relationship and the source of fund/wealth;
(c) obtaining information on the intended or performed transactions;
(d) obtaining the approval of senior management to commence or continue the business relationship;
(e) conducting close monitoring of the business relationship;
(f) any other measures a financial institution may undertake with relation to a high risk relationship.

In case where a financial institution is unable to perform the required Enhanced CDD requirements, the latter shall terminate the business relationship and file a suspicious transaction report under section 14 of the FIAMLA.

6.1 PEPs

PEPs are individuals who are or who have been entrusted with prominent public functions foreign, domestic and international organisation PEP, as well as the close relatives and associates of such persons. (Refer to the definition section of the FIAML Regulations 2018).

Business relationships with PEPs pose a greater than normal money laundering risk to financial institutions, by virtue of the possibility for them to have benefitted from proceeds of corruption,

as well as the potential for them (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

6.2 Non face-to-face relationships or occasional transactions

The FSC recognises that business conducted by financial institutions may also be conducted on a non- face-to-face basis, i.e. where there is no face to face contact with the customer or connected persons such as beneficial owners or controllers. Examples might be where identification information is provided through a trustee about persons who are connected with a trust, or by a legal body about the persons who are its beneficial owners and controllers or through identification documents received through electronic means. A further example may be where, although there is face-to-face contact with a customer, the supporting identification and verification documentation is provided at a time when the customer is not present.

Financial institutions must apply appropriate enhanced CDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is unable to be identified and when the financial institution is unsure of the authenticity of the documents in non-face-to-face relationships.

6.3 Connected persons that are PEPs

'Connected persons' will include underlying principals such as beneficial owners and controllers.

Financial institutions must apply appropriate EDD measures on a risk-sensitive basis where an applicant for business or customer (or any connected person, such as a beneficial owner or controller) is a PEP, and must ensure that they operate adequate policies, procedures and controls to comply with this requirement.

Financial institutions must:

(a) develop and document a clear policy on the acceptance of business relationships or one-off transactions with such persons, and ensure that this is adequately communicated;

(b) obtain and document the approval of senior management prior to establishing relationships with such persons;

(c) where such persons are discovered to be so only after a relationship has commenced, thoroughly review the relationship and obtain senior management approval for its continuance; and

(d) apply EDD measures to establish the source of funds and source of wealth of such persons.

Chapter 7: Simplified Due Diligence

In general, the full range of CDD measures should be applied by financial institutions. However, simplified CDD measures can be implemented in cases where lower risks have been identified and this corresponds to the situations outlined in Regulation 11 of the FIAML regulations and where the CDD measures are commensurate with the lower risk factors or any guidance issued. The possibility of applying simplified CDD measures does not remove from the financial institution its responsibility to adopt CDD measures, it only allows for application of reduced measures. The ultimate decision rests with the financial institution and there may be instances, depending on the level of risk and all the known circumstances (a high risk relationship e.g. PEP will be dealt with more caution rather than the routine CDD measures), where it is inappropriate to adopt these simplified measures. An example of simplified CDD measure could be not requiring CDD documentation for beneficial owner of publicly listed entities. The financial institution could obtain and retain documentary evidence of the existence of the public company and of its listed status, together with a copy of its annual report to verify that the individuals who purport to act on behalf of such entity have the necessary authority to do so.

Under all circumstances, financial institutions must keep the client risk assessment up to date and review the appropriateness of CDD obtained even if simplified CDD measures are adopted. Financial institutions are required to keep the risk assessment and level of CDD requirements under review and the level of risk of the CDD measures should be consistent with the risk of the relationship.

Financial institutions can apply simplified CDD measures where –

(a) Lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors;

(b) There is a low level of risk, financial institutions shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment carried out, whichever is most recently issued;

Where a financial institution decides to adopt the simplified measures in respect of a particular applicant, it must:

(a) document that decision in a manner which explains the factors which it took into account (including retaining any relevant supporting documentation) and its reasons for adopting the measures in question; and

(b) keep the relationship with the applicant (including the continued appropriateness of using the simplified measures) under review, and operate appropriate policies, procedures and controls for doing so.

Simplified CDD shall never 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 where there are other indicators of ML/TF risk.

Where simplified CDD measures are adopted, financial institutions should apply a risk-based approach to determine whether to adopt the simplified CDD measures in a given situation and/or continue with the simplified measures, although these clients' accounts are still subject to transaction monitoring obligations.

Chapter 8: Third Party Reliance

A financial institution may rely on relevant third parties to complete certain CDD measures, provided that there is a contractual arrangement in place with the third party. Where reliance is placed on a third party for elements of CDD, the financial institution must ensure that the identification information sought from the third party is adequate and accurate. The CDD information has to be submitted immediately in line with section 17D of the FIAMLA upon onboarding although the documents can be provided upon request at a later date. Where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the financial institutions relying on the third party.

In a third party reliance scenario, the third party should be regulated, supervised and monitored and subject to CDD in line with section 17C of the FIAMLA and record keeping requirements pursuant to section 17F of the FIAMLA and Regulation 21 of the FIAML Regulations 2018 which provides for third party reliance. When reliance is placed on a third party that is part of the same financial group, the financial institution must ensure that the group applies the measures as applicable to regulation 21(4) of the FIAML Regulations 2018.

Moreover, the financial institution needs to be aware on the level of the country risk when determining in which country (ies) the third party can be based, countries with strategic deficiencies in the fight against money laundering and the financing of terrorism, e.g those identified by the FATF as having strategic deficiencies. A high risk country can also be those countries that are vulnerable to corruption and which are politically unstable, the above examples are not exhaustive.

An example of a third party reliance arrangement is in the context of investment fund (fund), a third party reliance arrangement between the fund or its administrator and a relevant third party that acts as a fund distributor for its underlying investors is very common.

In order to ensure that these arrangements meet the FSC's expectations, an investment fund and its administrator should ensure that:

- there is a signed agreement between the fund or its administrator and the relevant third party, in which the third party consents to being relied upon for these purposes and undertakes;
- to provide any CDD information obtained immediately upon onboarding;
- the signed agreement contains clear contractual terms in respect of the obligations of the third party to obtain and maintain the necessary CDD records and to provide the CDD documents upon request;

- the signed agreement does not contain any conditional language, whether explicit or implied, which may result in the inability of the third party to provide the CDD documents. For example, language which qualifies the obligation to provide the CDD documents, such as "to the extent permissible by law" or "subject to regulatory request", is not acceptable. This is of particular relevance where reliance is placed on a third party based in a jurisdiction that is subject to secrecy laws or similar restrictive rules; and
- policies and procedures are in place which set out an approach with regard to the identification, assessment, selection and monitoring of third party relationships, including the frequency of testing performed on such third parties to deliver the necessary CDD documents when requested.

Reliance may only be placed on third parties to carry out CDD measures in relation to the identification and verification of a customer's identity and the establishment of the purpose and intended nature of the business relationship. Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a customer, including identifying the source of wealth or source of funds.

The FSC recommends that regular assurance testing is carried out in respect of the third party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient pursuant to section 17(2)(v) of the FIAMLA.

Financial institutions should take steps to ensure that any existing third party reliance arrangements comply with the applicable AML/CFT legislation in this regard. It is suggested that, where third party reliance arrangements are in place, reporting entities (e.g. funds) receive a report from the administrator about the arrangements that meets those requirements and that the report details the outcome of the testing carried out.

8.1 Introduced Business

There are occasions where applicants for business are introduced to financial institutions by ‘introducers’ pursuant to Regulation 21 of the FIAML Regulations 2018, a form of third-party reliance.

Financial institution should subject third-party introducers to the full identification and verification CDD measures for identification and verification as provided under Regulations 3(a), (c) and (d) of the FIAML Regulations 2018.

The financial institution should at the time of establishing the introducer relationship should carry out a risk analysis of this relationship and monitor the introducer relationship.

In line with the third-party reliance obligations, when individual applicants, or applicants which are body corporate, are introduced to a financial institution by an introducer, the financial institution should:

(a) obtain and maintain documentary evidence that the introducer is regulated for the purposes of preventing money laundering and terrorist financing; and
(b) be satisfied that the procedures laid down by the introducer meet the requirements specified in the FIAMLA and FIAML Regulations 2018.

Financial institutions should at all times bear in mind that the ultimate responsibility to ensure the completion of satisfactory CDD measures rests with them and not with the introducer.

Where it is proposed to rely on the introducer to carry out any of the CDD requirements, financial institutions must adopt a risk-based approach and must:

(a) obtain explicit written assurance from the introducer that it will carry out the requirements for CDD;
(b) satisfy themselves independently (and have clear procedures for doing so) that the procedures followed by the introducer are sufficiently robust to ensure that the introducer complies with the requirements of the AML/CFT legislation; and
(c) obtain evidence that the introducer is regulated/ supervised.

Where CDD identification data and other documentation is to be retained by the introducer rather than the financial institution, there must be a clear written understanding between the financial institution and the introducer that -

(a) such data will be retained by the introducer and will not be disposed of without the financial institution ’s consent,
(b) the financial institution will have timely access to such data (including inspection of documents) upon request, and
(c) such data will be promptly transferred to the custody of the financial institution, if the introducer ceases to act in that capacity.

Financial institutions’ boards of directors or equivalent senior management must ensure that periodic testing of the above arrangements are conducted by the financial institution, to ensure that the financial institution is complying with the current legislative framework with respect to the above provision.

Chapter 9: Monitoring Transactions and Activity

9.1 Introduction

The regular monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing CDD measures.

It is vital that the financial institution understands a customer's background and is aware of changes in the circumstances of the customer and beneficial owner throughout the life-cycle of a business relationship. The financial institution can usually only determine when it might have reasonable grounds for knowing or suspecting that ML and/or TF is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular business relationship.

There are two strands to effective ongoing monitoring:

(a) The first relates to the transactions and activity which occur on a day-to-day basis within a business relationship and which need to be monitored to ensure they remain consistent with the financial institution's understanding of the customer and the product or service it is providing to the customer.

(b) The second relates to the customer themselves and the requirement for the financial institution to ensure that it continues to have a good understanding of its customers and their beneficial owners. This is achieved through maintaining relevant and appropriate CDD and applying appropriate ongoing screening.

This Chapter deals with the requirement for the financial institution to monitor business relationships on an ongoing basis, including the application of scrutiny to large and unusual or complex transactions or activity so that ML and TF may be identified and prevented as required under Regulation 3(1)(e) of the FIAML Regulations 2018.

9.2 Objectives

A key prerequisite to managing the risk of a business relationship is understanding the customer, and beneficial owner, and where changes to those parties occur. It is also important to maintain a thorough understanding of the business relationship and to appropriately monitor transactions in order to be in a position to detect, and subsequently report, suspicious activity.

The type of monitoring applied by the financial institution will depend on a number of factors and should be developed with reference to the financial institution's business risk assessments

and risk appetite. The factors forming part of this consideration will include the size and nature of the financial institution's business, including the characteristics of its customer-base and the complexity and volume of expected transactions or activity.

The monitoring of business relationships should involve the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions or activity, to ensure that such transactions and activity are consistent with the financial institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds.

Particular attention should be paid to high risk relationships (for example, those involving PEPs), high risk countries and territories and high risk transactions.

An unusual transaction or activity may be in a form that is inconsistent with the expected pattern of activity within a particular business relationship, or with the normal business activities for the type of product or service that is being delivered. For example, unusual patterns of transactions with no apparent or visible economic or lawful purpose.

The nature of the monitoring in any given case will depend on the business of the financial institution, the frequency of activity and the types of business. Monitoring may include reference to: specific types of transactions; the relationship profile; a comparison of activities or profiles with that of a similar customer or peer group; or a combination of these approaches.

9.3 Obligations

Under Regulation 3(1) (d) of the FIAML Regulations 2018, financial institutions should understand and obtain adequate and relevant information on the purpose and intended nature of a business relationship or occasional transaction. Further, in accordance with Regulation 3(1) (e) of the FIAML Regulations 2018, financial institutions should 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 CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

Regulation 12(2)(f) of the FIAML Regulations 2018 states that EDD measures that may be applied for higher risk business relationships including conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Regulation 15(1)(d) of the FIAML Regulations 2018 requires a financial institution to conduct enhanced ongoing monitoring on foreign PEPs, whether as customer or beneficial owner, in addition to performing the CDD measures. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP. Examples of the additional monitoring arrangements for high risk relationships could include:

(a) undertaking more frequent reviews of high risk relationships and updating CDD
(b) information on a more regular basis;
(c) undertaking more regular reviews of transactions and activity against the profile and
(d) expected activity of the business relationship;
(e) applying lower monetary thresholds for the monitoring of transactions and activity;
(f) reviews being conducted by persons not directly involved in managing the relationship,
(g) for example, the CO;
(h) ensuring that the financial institution has adequate MI systems to provide the board and CO with the timely information needed to identify, analyse and effectively monitor high risk relationships and accounts;
(i) appropriate approval procedures for high value transactions in respect of high risk
(j) relationships; and/or
(k) a greater understanding of the personal circumstances of high risk relationships, including an awareness of sources of third party information.

The financial institution should also consider the possibility for legal persons and legal arrangements to be used as vehicles for ML and TF.

9.4 PEP Relationships

The system of monitoring used by the financial institution must provide for the ability to identify where a customer or beneficial owner becomes a PEP during the course of the business relationship and whether that person is a foreign PEP, domestic PEP or international organisation PEP.

In accordance with Regulation 15(1) (b) of FIAML Regulations 2018, where a customer or beneficial owner becomes a foreign PEP during the course of an existing business relationship, as part of the EDD measures subsequently applied the financial institution shall obtain senior management approval to continue that relationship. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organisation PEP.

It is not expected that the financial institution will have a thorough knowledge of, or fully research, a family connection. The extent to which a connection is researched should be based upon the size, scale, complexity and involvement of the person in the context of the business relationship and the profile of the business relationship, including its asset value.

It is possible that family members and/or associates may not inform the financial institution, or even be aware, of their PEP status and therefore independent screening and monitoring should be conducted. It is also possible that an individual's PEP status may not be present at take-on, for example, where that person takes office during the life of a business relationship. It is therefore important that ongoing monitoring exists in order to identify changes of status and risk classification.

9.5 High Risk Transactions or Activity

When conducting ongoing monitoring, the following are examples of red flags which may indicate high risk transactions or activity within a business relationship:

(a) an unusual transaction in the context of the financial institution's understanding of the business relationship (for example, abnormal size or frequency for that customer or peer group, or a transaction or activity involving an unknown third party);
(b) funds originating from, or destined for, an unusual location, whether specific to an individual business relationship, or for a generic customer or product type;
(c) transactions or activity unexpectedly occurring after a period of dormancy;
(d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;
(e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the customer or their business;
(f) the involvement of charitable or political donations or sponsorship; or
(g) a relevant connection with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

Financial institutions must remain conscious that under the FIAMLA, they have an obligation to prevent and detect ML and TF.

A customer who is, or may be, attempting to launder money may frequently structure his instructions in such a way that the economic or lawful purpose of the instruction is not apparent or is absent entirely. When asked to explain circumstances or transactions, the customer may be evasive or may give explanations which do not stand up to reasonable scrutiny.

Where a financial institution is suspicious, or has knowledge of, money laundering or terrorist financing, it should not unquestioningly carry out instructions as issued by the customer.

If a financial institution unquestioningly carries out unreasonable instructions in this manner, it may mean that it is failing in its duty to prevent and detect ML/TF.
When faced with unreasonable customer instructions that lead the relevant person to know or suspect ML/TF, the financial institution must file a suspicious transaction report and also consider taking legal advice. Please refer to Chapter 10 of the Handbook for further guidance on internal and external disclosures.

9.6 Handling Cash Transactions

The use of cash and monetary instruments as a means of payment or method to transfer funds can pose a higher risk of ML/TF than other means, such as wire transfer, cheques or illiquid securities. Unlike many other financial products with cash and monetary instruments there will likely be no clear audit trail and it may be unclear where the funds have originated from. Section 5 of the FIAMLA states that any person who makes or accepts any payment in cash in excess of 500,000 rupees or an equivalent amount in foreign currency, or such amount as may be prescribed, shall commit an offence.

Therefore, where cash and monetary instrument transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, financial institution must approach such situations with caution and make relevant further enquiries.

In relation to cash transactions, the financial institution should consider factors such as the amount of cash, currency, denominations and the age of the notes in determining whether the activity is 'normal' for the customer along with a comparison with the customer's expected activity.

Financial institutions should be especially robust when dealing with requests for frequent or unusually large amounts of cash and monetary instrument by customers, especially where the customer is resident in jurisdictions where tax evasion is a known problem.

Financial institutions should be vigilant for explanations given by customers which do not stand up to scrutiny.

Where the financial institution has been unable to satisfy itself that the transaction is legitimate activity, and therefore considers it suspicious, an internal disclosure must be made.

9.7 Real-Time and Post-Event Transaction Monitoring

Monitoring procedures should involve a combination of real-time and post-event monitoring.

Real-time monitoring focuses on transactions and activity where information or instructions are received before or as the instruction is processed. Post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.

Real-time monitoring of activity can be effective at reducing exposure to *ML*, *TF* and predicate offences such as bribery and corruption, whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

In this respect, regardless of the split of real-time and post-event monitoring, the over-arching purpose of the monitoring process employed should be to ensure that unusual transactions and activity are identified and flagged for further examination.

Financial institutions should ensure that the flags / alerts raised are examined within the shortest delay and properly documented prior to closure.

9.8 Automated and Manual Monitoring

The financial institution's monitoring processes should be appropriate with respect to its size, activities and complexity, together with the risks identified within its business risk assessments.

While bigger financial institutions with large volumes of transactions will likely favour an automated system, the financial institution may conclude that a manual real-time and/or post-event monitoring process is sufficient given the size and scale of its business.

Notwithstanding the method of monitoring used, the financial institution should adapt the parameters of its processes, in particular the extent and frequency of monitoring, on the basis of materiality and risk, including, without limitation, whether or not a business relationship is a high risk relationship.

The rationale for deciding upon either a manual or automated method of monitoring, together with the criteria in defining the parameters of that monitoring, should be based on the conclusions of the financial institution's business risk assessments and risk appetite.

Where an automated monitoring method is used, whether specific to the financial institution or a group-wide system, the financial institution must:

(a) understand how the system works and how to use the system (for example, making full use of guidance);

(b) understand when changes are to be made to the system (including the nature and extent of any changes);

(c) understand the system's coverage (including the extent of the transactions, activity and/or parties monitored);

(d) understand the sources of data used (including both the source(s) of internal data fed into the system and the source(s) of external data to which it is compared);

(e) understand the nature of the system's output (exceptions, alerts etc.);

(f) set clear procedures for dealing with potential matches, driven on the basis of risk rather than resources; and

(g) record the basis for discounting alerts (for example, false positives) to ensure there is an appropriate audit trail.

Where the financial institution is a branch office or subsidiary of an international group and uses group-wide systems for transaction and activity monitoring, the ability for the financial institution to dictate the particular characteristics of the monitoring conducted by the system may be limited. Where this is the case, notwithstanding the group-wide nature of the system, the financial institution must be *satisfied* that it provides adequate mitigation of the *risks* applicable to the business of the financial institution.

The financial institution should be aware that the use of computerised monitoring systems does not remove the requirement for relevant employees to remain vigilant. It is essential that the financial institution continues to attach importance to human alertness. Factors such as a person's intuition; direct contact with a customer either face-to-face or on the telephone; and the ability, through practical experience, to recognise transactions and activities which do not seem to have a lawful or economic purpose, or make sense for a particular customer, cannot be automated.

9.9 Examination

In accordance with Regulation 25(1) of FIAML Regulations 2018, where within a business relationship there are complex, or large and unusual transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, the financial institution shall examine the background and purpose of those transactions.

As part of its examination, the financial institution should give consideration to the following:

(a) reviewing the identified transaction or activity in conjunction with the relationship risk assessment and the CDD information held;

(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by the

financial institution as to whether the transaction or activity has a rational explanation and economic purpose;

(c) reviewing the appropriateness of the relationship risk assessment in light of the unusual transaction or activity, together with any supplemental CDD information obtained; and

(d) considering the transaction or activity in the context of any other connected business relationships and the cumulative effect this may have on the risk attributed to those relationships.

For the purposes of Regulation 25(1) of FIAML Regulations 2018, what constitutes a large and unusual or complex transaction will be based on the particular circumstances of a business relationship and will therefore vary from customer to customer.

The financial institution must ensure that the examination of any large and unusual, complex, or otherwise higher risk transaction or pattern of transactions or other activity is sufficiently documented and that such documentation is retained in a readily accessible manner in order to assist the FSC, the FIU, other domestic competent authorities and auditors.

The financial institution must ensure that procedures are maintained which require reporting of internal disclosures to be made to the MLRO in accordance with the requirements of Regulations 27 (c) of FIAML Regulations 2018 and Chapter 10 of this Handbook where any information or other matters that come to the attention of the file handler and his opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity.

Following the conclusion of its examination, the financial institution should give consideration to whether follow-up action is necessary in light of the identified transaction or activity. This could include, but is not limited to:

(a) applying EDD measures where this is considered necessary or where the financial institution has reassessed the business relationship as being high risk as a consequence of the transaction or activity;

(b) considering whether further employee training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;

(c) considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or

(d) applying increased levels of on-going monitoring for particular relationships.

9.10 Ongoing CDD

In accordance with Regulation 3(1) (e) (ii), the requirement to conduct ongoing CDD will ensure that the financial institution is aware of any changes in the development of a business relationship. The extent of the financial institution's ongoing CDD measures must be determined on a risk-sensitive basis. However, the financial institution must be aware that as a business relationship develops, the risks of ML and TF may change.

It should be noted that it is not necessary to re-verify or obtain current identification data unless an assessment has been made that the identification data held is not adequate for the assessed risk of the business relationship or there are doubts about the veracity of the information already held. Examples of such could include a material change in the way that the business of the customer is conducted which is inconsistent with its existing business profile, or where the financial institution becomes aware of changes to a customer's or beneficial owner's circumstances, such as a change of address.

In order to reduce the burden on customers and other key principals in low risk relationships, trigger events (for example, the opening of a new account or the purchase of a further product) may present a convenient opportunity to review the CDD information held.

The review must take account of the CDD and EDD obtained on the customer, whether there have been any changes to the customer's activity / circumstances. Where the basis of a relationship has changed the relevant person should consider whether the risk rating of the customer needs amending and carry out further CDD procedures to ensure that the revised risk rating and basis of the relationship is fully understood. Ongoing monitoring procedures must take account of these changes. If the risk changes significantly it should be remembered that EDD may be required. The review should include considering the customer's location in relation to the high risk third countries and sanctions list.

Financial institutions 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. That information must be available to the MLRO.

Failure to adequately monitor customers' activities could expose a business 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 business.

9.11 Customer screening

When obtaining CDD or carrying on ongoing monitoring, it is likely that a financial institution will perform searches against its customer's name, and in the case of non-personal customers, against the names of the beneficial owners, controllers, beneficiaries etc. These searches can be performed using a wide variety of risk management systems or public domain searches.

When conducting searches against the name of an individual or entity, financial institutions should consider "negative press" in addition to whether the individual or entity is named on a sanctions or PEP list.

Negative press is the term given to any negative information, whether alleged or factual. This could be anything from an allegation of fraud by a disgruntled former customer to an article in a newspaper relating to a criminal investigation.

Consideration should be given to the credibility of the information source, the severity of the negative press, how recent the information is and the potential impact the negative press would have on the business relationship with that customer.

The FSC would expect the financial institution to document:

- the source and date of the search;
- actions taken to confirm or discount any potential match;
- details of the negative press;
- any actions taken to verify or disprove the claims; and
- any additional actions taken as a result of this information such as treating the customer as high risk and/or seeking proof of source of wealth/funds etc.

9.12 Oversight of Monitoring Process by Compliance Officer

The CO should have access to, and familiarise his or her self with, the results and output from the financial institution's monitoring processes. Such output should be reviewed by the CO who in turn should report regularly to the board, providing relevant management information such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

The board should consider the appropriateness and effectiveness of the financial institution's monitoring processes as part of its annual review of the financial institution's business risk assessments and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and risk as set out in the business risk assessments.

Where the financial institution identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner.

Chapter 10: Reporting suspicious transactions

10.1 Introduction

Financial institutions have the opportunity to observe the day to day transactions of their customers. Law enforcement agencies do not have unlimited resources to monitor every transaction performed in the financial system by every individual or business, but do have access to confidential information relating to known or suspected criminals and terrorists.

Communication between the financial institutions and the law enforcement agencies is therefore fundamental with the aim of preventing money laundering and terrorist financing. Financial institutions have a critical responsibility in determining transactions which give rise to reasonable ground to suspect any potential link to money laundering and terrorist financing.

Under the FIAMLA, a suspicious transaction has been 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, terrorist financing or by proscribed organisations, whether or not the funds represent the proceeds of a crime;

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

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

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

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

A transaction includes:

(a) opening an account, issuing a passbook, renting a safe deposit box, entering into a fiduciary relationship or establishing any other business relationship, whether electronically or otherwise; and

(b) a proposed transaction or an attempted transaction.

Given the above, financial institutions should also be able to report transactions which are planned for the future and give rise to suspicion and/or transactions which have been endeavoured. The predicate offence need not be known or suspected, reasonable grounds to suspect should suffice.

10.2 Role of the Money Laundering Reporting Officer

Regulation 26(1) of the FIAML Regulations 2018 requires a financial institution to appoint a Money Laundering Reporting Officer, to whom an internal report shall be made of any information or other matter which comes to the attention of any person handling a transaction and which, in the opinion of the person, gives rise to knowledge or reasonable suspicion that another person is engaged in money laundering or the financing of terrorism.

Further Regulation 26(2) of the FIAML Regulations 2018 requires a financial institution to appoint a Deputy Money Laundering Reporting Officer to perform the duties of the Money Laundering Reporting Officer in his absence.

According to Regulation 26(4) of the FIAML Regulations 2018, the Money Laundering Reporting Officer and the Deputy Money Laundering Officer must be:

(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.

The MLRO/ DMLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required.

The DMLRO should be of similar status and experience to the MLRO.
In this Handbook, reference to the MLRO implies the DMLRO in the MLRO's absence.

The responsibilities of the MLRO will normally include, as stated in the FIAML Regulations 2018:

(a) undertaking a review of all internal disclosures in the light of all available relevant information and determining whether or not such internal disclosures have substance and require an external disclosure to be made to the FIU;

(b) maintaining all related records;

(c) giving guidance on how to avoid tipping off the customer if any disclosure is made;

(d) liaising with the FIU and if required the FSC and participating in any other third party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance; and

(e) providing reports and other information to senior management.

10.3 Unusual activity

According to Regulation 28(2) of the FIAML Regulations 2018, where a financial institution identifies any unusual activity in the course of a business relationship or occasional transaction the financial institution should:

(a) perform appropriate scrutiny of the activity;

(b) obtain EDD in accordance with regulation 12 only if this will not tip off the client; and

(c) consider whether to make an internal disclosure in accordance with the reporting procedures established under regulation 27.

Reference can also be made to Chapter 9 on Monitoring Transactions and activity, where unusual activity has been briefly discussed.

Unusual activity includes, but not limited to, any activity or information relating to a business relationship, occasional transaction or an attempted transaction where there is no apparent economic or lawful purpose, including transactions that are –

(i) complex;

(ii) both large and unusual; or

(iii) of an unusual pattern.

Unusual activity also includes, but not limited to, anything that causes the financial institution to doubt the identity of the customer (including beneficial owners and controllers or introducer, where appropriate) or anything that causes the financial institution to doubt the good faith of the customer (including beneficial owners and controllers or introducer, where appropriate).

Situations that are likely to appear unusual include, inter alia:

(a) transactions or instructions which have no apparent legitimate purpose and appear not to have a commercial rationale;

(b) transactions, instructions or activity that involve apparent unnecessary complexity;

(c) where the transaction being requested by the customer is out of the ordinary range;

(d) where the size or pattern of transactions is out of line with expectations for that customer;

(e) where the customer is not forthcoming with information about their activities, reason for a transaction, source of funds, CDD documentation etc.;

(f) where the customer who has entered into a business relationship uses the relationship for a single transaction or for only a very short period of time where that was not expected;

(g) the extensive use of offshore structures where the customer's needs are inconsistent with the use of such services;

(h) transfers to or from high risk jurisdictions which are not consistent with the customer's expected activity;

(i) unnecessary routing of funds through third party accounts;

(j) unusual investment transactions with no discernible purpose; and

(k) extreme urgency in requests from the customer, particularly where they are not concerned by large transfer fees, early repayment fees etc.

Please note that this is not an exhaustive list. Unusual activity is likely to be detected during ongoing monitoring (see Chapter 9 of the Handbook), when receiving an application from a new customer, when receiving an instruction to carry out a transaction or during other communications with the customer.

Where a financial institution identifies unusual activity, Regulation 28(2) requires the financial institution to perform 'appropriate scrutiny' of the activity and to obtain EDD. Appropriate scrutiny of the activity may involve making enquiries of the customer and asking the questions as per the circumstances. Relevant processes should be in place to ensure that unusual activity alerts or incidences are reviewed and analysed promptly so that an internal disclosure can be filed as soon as possible. For further detail on how to conduct 'appropriate scrutiny', please refer to part 9 below.

10.4 Suspicious transaction reporting procedures

According to Regulation 28(1) of the FIAML Regulations 2018, where a financial institution identifies any suspicious activity or has reasonable ground to suspect that a transaction is suspicious in the course of a business relationship or occasional transaction, the financial institution should

(a) consider obtaining EDD in accordance with Regulation 12 of the FIAML Regulations 2018; and

(b) make an internal disclosure in accordance with the procedures established under Regulation 27 of the FIAML Regulations 2018.

The reporting procedures as above must also apply to prospective customers and transactions that were attempted but that did not take place. The MLRO should then consider the internal disclosure to assess whether an external disclosure need to be made to the FIU.

Regulation 27 of the FIAML Regulations 2018 requires a financial institution to have documented reporting procedures in place that will:

(a) enable all its directors, management and all appropriate employees to know to whom they should report any knowledge or suspicion of ML/TF activity;
(b) ensure that there is a clear reporting chain to the MLRO;
(c) require reports to be made to the MLRO ("internal disclosures") 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 ML/TF activity;
(d) require the MLRO to then consider these reports in the light of all other relevant information available to determine whether or not it gives rise to any knowledge or suspicion of ML/TF activity;
(e) ensure that the MLRO has full access to any other available information that may be of assistance; and
(f) enable the information or other matters contained in a report ("external disclosure") to be provided as soon as is practicable the Financial Intelligence Unit if the MLRO knows or suspects that another is engaged in ML/TF activity.

The recording of internal and external disclosures are covered further at 10.6 and 10.7 of this Chapter.

10.5 Potential Red Flags

The following is a non-exhaustive list of possible ML and TF red flags that the financial institution should be mindful of when dealing with a business relationship or occasional transaction:

(a) The deposit or withdrawal of unusually large amounts of cash from an account;
(b) Unwillingness to provide CDD documentation on beneficial owners/ controllers;
(c) Deposits or withdrawals at a frequency that is inconsistent with the financial institution's understanding of that customer and their circumstances.
(d) Transactions involving the unexplained movement of funds, either as cash or wire transfers.
(e) Payments received from, or requests to make payments to, unknown or un-associated third parties.

(f) Personal and business related money flows that are difficult to distinguish from each other.

(g) Financial activity which is inconsistent with the legitimate or expected activity of the customer.

(h) An account or business relationship becomes active after a period of dormancy.

(i) The customer is unable or reluctant to provide details or credible explanations for establishing a business relationship, opening an account or conducting a transaction.

(j) The customer holds multiple accounts for no apparent commercial or other reason.

(k) Bank drafts cashed in for foreign currency.

(l) Early surrender of an insurance policy incurring substantial loss.

(m) Frequent early repayment of loans.

(n) Frequent transfers indicated as loans sent from relatives.

(o) Funds transferred to a charity or NPO with suspected links to a terrorist organisation.

(p) High level of funds placed on store value cards.

(q) Insurance policy being closed with a request for the payment to be made to a third party.

(r) Large amounts of cash from unexplained sources.

(s) Obtained loan and repaid balance in cash.

(t) Purchase of high value assets followed by immediate resale with payment requested via cheque.

The above list is not exhaustive and its content is purely provided to reflect examples of possible red flags. The existence of one or more red flag does not automatically indicate suspicion and there may be a legitimate reason why a *customer* has acted in the manner identified.

10.6 Internal disclosures

Where suspicious activity is identified, an internal disclosure must be made to the MLRO in accordance with Regulation 28(1) of the FIAML Regulations 2018. It is the responsibility of the MLRO (or if appropriate, the Deputy MLRO) to consider all internal disclosures he/she receives in the light of full access to all relevant documentation, this may include reviewing CDD, transaction patterns and other connected accounts / relationships. The evaluation process should be fully documented. All relevant persons must ensure that the MLRO receives full cooperation from all staff and full access to all relevant documentation so that he/she is in a position to decide whether there are reasonable grounds to suspect money laundering or terrorist financing. The predicate offence need not be known or suspected, reasonable grounds to suspect should suffice.

Failure by the MLRO to diligently consider all relevant material may lead to vital information being overlooked and the suspicious transaction or activity not being externally disclosed to the FIU in accordance with the requirements of the legislation. As a result, the MLRO must document internal disclosures made by employees to record the results of the assessment of each disclosure.

Financial institutions must ensure that all employees are made aware of the identity of the MLRO and his/her Deputy, and the procedures to follow when making an internal disclosure report to the MLRO. Reporting lines should be as short as possible with the minimum number of people between the employee with suspicion and the MLRO. This ensures speed, confidentiality and accessibility to the MLRO. All disclosure reports must reach the MLRO without any undue delay. Under no circumstances should reports be filtered out by supervisors or managers such that they do not reach the MLRO.

All suspicions reported to the MLRO must be documented (in urgent cases this may follow an initial discussion by telephone). The report must include the full details of the customer and as full a statement as possible of the information giving rise to the suspicion.

The MLRO should acknowledge receipt of the internal disclosure and at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries, such as tipping off the customer or any other third party.

10.7 External disclosures (Suspicious Transaction Reports)

Regulation 29(1) of the FIAML Regulations 2018 requires the MLRO, in the event of an internal disclosure being made, to assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/TF.

Regulation 29(2) of the FIAML Regulations 2018 and Section 14 of the FIAMLA requires the MLRO to make an external disclosure (in the form prescribed in Section 15 of the FIAMLA) as soon as practicable but not later than 15 working days from the day on which it becomes aware of a transaction

if the MLRO-

(a) knows; or

(b) has reasonable grounds to believe, that an internal disclosure may be suspicious.

10.8 Recording of internal and external disclosures

Regulation 30 (1)(a) of the FIAML Regulations 2018 requires the financial institution to establish and maintain a register of all ML/TF internal disclosures made to the MLRO or Deputy MLRO. The register must include details of:

- the date the report was made;
- the person who made the report;
- whether the report was made to the MLRO or Deputy MLRO; and;
- information to allow the papers and relevant documentation to be located.

Regulation 30 (1)(b) of the FIAML Regulations 2018 requires the relevant person to establish and maintain a register of all ML/TF external disclosures made to the FIU. The register must include details of:

- the date of the disclosure;
- the person making the disclosure; and
- information to allow the papers relevant to the disclosures to be located.

Regulation 30(2) of the FIAML Regulations 2018 states that the registers of internal and external disclosures may be contained in a single document if the details included in the registers can be presented separately for internal and external disclosures upon request by a competent authority.

10.9 Unusual Activity-Conducting "appropriate scrutiny" of unusual activity

Regulation 28(2) of the FIAML Regulations 2018 requires the relevant person to conduct 'appropriate scrutiny' of any unusual activity and to obtain EDD. The activity should be looked at in detail in conjunction with additional information such as the customer's CDD, expected activity, an explanation of the activity from the customer, supporting documentary evidence or information from independent data sources. CDD provides the basis for recognising unusual activity therefore it is imperative that CDD is satisfactory on all customers and that business relationships are monitored appropriately.

The aim of conducting 'appropriate scrutiny' is to enable the financial institution to determine whether the activity is in fact suspicious and, if so, make a disclosure. If the activity is not deemed to be suspicious but still appears unusual or risky, the relevant person should consider

other actions such as reviewing and updating the customer's risk assessment, arranging further ongoing monitoring or considering whether they have the risk appetite to continue doing business with the customer.

When conducting 'appropriate scrutiny', other connected customers, accounts or relationships may need to be examined. Connectivity can arise though commercial connections e.g. linked accounts, introducers etc., or through connected individuals e.g. third parties, controllers, signatories etc. The need to search for information concerning connected accounts or relationships should not delay making an external disclosure to the FIU.

The nature and scale of the scrutiny required will vary greatly depending on the type of activity, the risk factors involved and the size and scope of the activity. Regardless of the methods adopted, it is essential that the investigation and outcome are clearly documented in a prompt and timely manner.

The following are likely to cause suspicion after conducting appropriate scrutiny:

(a) the customer is unable or refuses to provide a reasonable explanation for the activity and this is perceived as being an attempt to conceal criminal conduct rather than the customer being awkward, unhelpful or secretive for personal reasons;
(b) the explanation does not "sit right" or does not make economic sense. For example a bank's customer sending repeat small amounts on a regular basis overseas despite transfer fees incurred with no reasonable explanation;
(c) documentation supplied appears to be fraudulent, incomplete or doctored;
(d) independent data sources reveal negative information on the customer or related parties such as allegations of corruption; or
(e) activity appears consistent with known ML/TF typologies.

Please note that the above list is non-exhaustive.

10.10 Appropriate scrutiny tips

The following tips should be borne in mind when conducting 'appropriate scrutiny':

(a) Investigate until you feel comfortable with the activity or have sufficient information to submit a disclosure.
(b) Consider using a broad range of data sources – e.g. companies registers, address verification sites, social networks, news.

(c) Obtain an understanding of the relationships between the customer and any related parties.

(d) Find out if the customer is or was acting on behalf of another person. If so, who and why?

(e) Compare the customer's explanation with publicly available information. For example, if a large credit supposedly relates to the sale of a house, consider checking the address and average prices in that area.

(f) Consider the information held against known typologies and high risk indicators - transaction type, customer background, location and currency.

(g) By checking the customer's historic activity you may be able to detect a pattern. For example a local business may always see a surge in cash deposits in June due to tourism.

(h) If requesting information or documentation from a customer, allow a reasonable timeframe for them to respond and communicate by phone, email, online messaging and fax wherever possible to expedite the process. It should be noted that further CDD should not be pursued if it may tip off the client.

(i) If appropriate, use this as an opportunity to gain a better understanding of what activity to expect going forward.

10.11 Tipping Off

Section 16(1) of the FIAMLA states that no person directly or indirectly involved in the reporting of a suspicious transaction shall inform any person involved in the transaction or an unauthorised third party that the transaction has been reported or that information has been supplied to the FIU pursuant to a request made under section 13(2) or (3) of the FIAMLA

Reasonable enquiries of a customer, conducted in a discreet manner, regarding the background to a transaction or activity which has given rise to the suspicion is prudent practice, forms an integral part of CDD and on-going monitoring, and should not give rise to tipping off. If the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead the financial institution should immediately file an STR with the FIU.

10.12 Terminating a Business Relationship

Whether or not to terminate a *business relationship* is a commercial decision, except where required by law, for example, where the financial institution cannot obtain the required *CDD* information and EDD as applicable (Regulations 12(3) and 13(b) of the FIAML Regulations 2018). The financial institution should in these cases consider the following points when interacting with its customer:

(a) it will become apparent to criminals that elements of their criminal activity is known to the financial institution, if it begins to ask probing questions regarding certain activities or if it seeks to terminate the relationship or decline entering into a business relationship without a meaningful pretext. The financial institution is therefore encouraged to carefully consider the wording of any statements made to customers explaining their decision; and

(b) the more information is included in the STR, the more valuable it will be to the FIU.

Chapter 11: Record keeping

Financial institutions are expected to have appropriate and effective policies, procedures and controls in place to ensure that records including transactions are maintained during and after the course of the business relationship, either in the form of original documents or copies.

The books and records shall include

(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/assessment undertaken in accordance with the FIAMLA, 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 or other reports made to FIU in accordance with the FIAMLA, including any accompanying documentation, which shall be maintained for a period of at least 7 years from the date the report was made.

Where a financial institution destroys or removes any record (which includes register or document as per section 17F of the FIAMLA); or fails to warn or inform the owner of any funds of any report required to be made in respect of any transaction or any action to be taken with respect to any transaction; or facilitates or permit a transaction to be carried out under a false identity commits an offence and on conviction is liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Records shall include account records of the customer during the course of the relationship and shall be kept as long as prescribed under the relevant legislation and will also include any audit report of the different functions of the financial institution. The following information should be kept for every transaction carried out in the course of a business relationship or one-off transaction:

(a) the name and address of the customer;

(b) if a monetary transaction, the kind of currency and the amount;

(c) if the transaction involves a customer's account, the number, name or other identifier for the account;

(d) the date of the transaction;

(e) details of the counterparty, including account details;

(f) the nature of the transaction; and

(g) details of the transaction.

Customer transaction records must provide a clear and complete transaction history of incoming and outgoing funds or assets.

Financial institutions are requested to keep sufficient records to demonstrate that their CDD measures are appropriate in view of the risk of money laundering and terrorist financing and are required to demonstrate that records of customer identification and verification can be retrieved quickly and without delay in line with the relevant legislative framework.

Financial institutions must maintain records of all transactions undertaken on behalf of the customer during the course of a business relationship, either in the form of original documents or copies. Where copies of the original identification documents (passports, national ID, drivers licence or any acceptable form of identification) are maintained, these copies should be duly certified in accordance with the CDD measures in place.

Regardless of the form in which the financial institution chooses to keep records, correspondence records must be sufficiently detailed to enable a transaction to be readily reconstructed at any time. Transaction records must adequately identify the nature and date of the transaction, who initiated the transaction (instructions can be given through various means – emails, regular instructions, etc), the type and amount of currency, the type and number of any account with the financial institution, and the name and address of the financial institution and the responsible officer, employee or agent.

In the case of negotiable instruments other than currency, records must include particulars of the name of the drawer and the payee (if any), the financial institution on which it was drawn, the amount, date, and number (if any) of the instrument, and any endorsement details.

Financial institutions must not enter into outsourcing arrangements or place reliance on third parties to retain records where access is likely to be impeded by confidentiality or data protection restrictions. Records held by third parties are not considered to be in a readily retrievable form unless the financial institution is reasonably satisfied that the third party is itself an institution which is able and willing to keep and disclose such records when so required.

Financial institutions must maintain records of all AML/CFT training delivered to employees. These records must include:

(a) the dates on which the training was provided;

(b) the nature of the training, including its content and mode of delivery; and

(c) the names of the employees who received the training.

Moreover, records should also include any assessment/audit carried out by the financial institution.

Where the records are being held electronically, the financial institution should ensure that the working documents should be legible and in a usable filing system, so that they can be retrieved/found without undue delay and produced on a timely basis especially where the originals are not to be retained.

Where a financial institution chooses to implement an electronic storage system, the financial institution should carry out an assessment of the risk, this risk assessment should be documented. Based on the risk assessment the financial institution may determine whether it is appropriate to retain the originals.

Where a financial institution is aware that a request for information or an enquiry is being conducted by a competent authority, the financial institution must retain the relevant records for as long as required by the competent authority.

Chapter 12: Employee Screening and Training

12.1 Introduction

One of the most important tools available to financial institutions, to assist in the prevention and detection of financial crime, is to have appropriately screened employees who are alert to the potential risks of ML and TF and who are well trained with respect to the CDD requirements and the identification of unusual activity, which may prove to be suspicious.

The effective application of even the best designed systems, policies, procedures and controls can be quickly compromised if employees lack competence or probity, are unaware of, or fail to apply, the appropriate policies, procedures and controls or are not adequately trained.

12.2 Obligations

The financial institution is required, under Regulation 22(1)(b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees. Furthermore, Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against money laundering and terrorism financing should also be in place to include ongoing training programme for the directors, officers and employees of the financial institution, 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).

12.3 Board Oversight

The Board must be aware of the obligations of the financial institution in relation to employee screening and training.

The financial institution must ensure that the training provided to officers and employees is comprehensive and ongoing and that the officers and employees are aware of ML and TF, the associated risks and vulnerabilities of the financial institution, and their corresponding obligations.

The financial institution must establish and maintain mechanisms to measure the effectiveness of the AML and CFT training provided to relevant employees and on a risk based approach.

In order to measure the effectiveness of AML and CFT training, the financial institution could consider it appropriate to incorporate an exam or some form of assessment into its on-going

training programme, either as part of the periodic training provided to employees or during the intervening period between training.

Regardless of the methods utilised, the board should ensure that it is provided with adequate information on a sufficiently regular basis in order to satisfy itself that the financial institution's employees are suitably trained to fulfil their personal and corporate responsibilities.

12.4 Screening Requirements

In order to ensure that employees are of the required standard of competence, which will depend on the role of the employee, the financial institution must give consideration to the following prior to, or at the time of, recruitment:

(a) obtaining and confirming details of employment history, qualifications and professional memberships;

(b) obtaining and confirming appropriate references;

(c) obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;

(d) obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and

(e) screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions

The financial institution should also carry out periodic ongoing of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

12.5 Methods of Training

While there is no single or definitive way to conduct training, the critical requirement is that training is adequate and relevant to those being trained and that the content of the training reflects good practice.

The guiding principle of all AML and CFT training should be to encourage directors, officers and employees, irrespective of their level of seniority, to understand and accept their responsibility to contribute to the protection of the financial institution against the risks of ML and TF.

The precise approach adopted will depend upon the size, nature and complexity of the financial institution's business. Classroom training, practical exams, videos and technology-based

training programmes can all be used to good effect, depending on the environment and the number of directors, officers and employees to be trained.

Training should highlight to directors, officers and employees the importance of the contribution that they can individually make to the prevention and detection of ML and TF. There is a tendency, in particular on the part of more junior employees, to mistakenly believe that the role they play is less crucial than that of more senior colleagues. Such an attitude can lead to failures in the dissemination of important information because of mistaken assumptions that the information will have already been identified and dealt with by more senior colleagues.

12.6 Frequency and Scope of Training

The financial institution must provide the appropriate level of AML and CFT induction training, or a written explanation, to all new employees, board members and senior management, before they become actively involved in the operations of the financial institution.

Consideration should be given by the financial institution to establishing an appropriate minimum period of time by which, after the start of their employment, new employees should have completed their AML and CFT induction training. Satisfactory completion and understanding of any mandatory induction training should be a requirement to the successful completion of an employee's probation period.

The financial institution must provide basic AML/CFT training to all employees at least every year. Some categories of employees should receive additional, specialized training according to their roles. Please refer to Section 12.8 of this Chapter for information.

Training will also need to be carried out more frequently to meet the requirements of FIAML Regulations 2018, if new legislation or significant changes to this Handbook are introduced, or where there have been significant technological developments within the financial institution or with the introduction of new products, services or practices.

12.7 Content of Training

In providing the training required, pursuant to Regulation 22(1)(c) of FIAML Regulations 2018 and this Handbook, the financial institution must:

(a) provide appropriate training to directors, officers and employees to enable them to competently analyse information and documentation, so as to enable them to form an opinion on whether the transactions and actions may be linked to money laundering or terrorism financing;

(b) detail procedures that need to be followed if any links to money laundering or terrorism financing have been identified;

(c) prepare and provide to employees a copy, in any format, of the financial institution's policies, procedures and controls manual for AML and CFT; and

(d) ensure employees are fully aware of all applicable legislative requirements.

In accordance with Regulation 22(1)(c) of FIAML Regulations 2018, the ongoing training provided by the financial institution shall cover:

(a) the FIAMLA, FIAML Regulations 2018, any AML/CFT Code issued by the FSC and this Handbook;

(b) the implications of non-compliance by employees to requirements of FIAMLA, FIAML Regulations 2018, any AML/CFT Code issued by the FSC and this Handbook; and

(c) the financial institution's policies, procedures and controls for the purposes of foreseeing, preventing and detecting ML and TF.

The financial institution must ensure that the ongoing training provided to directors, officers and employees also covers, to a minimum:

(a) the requirements for the internal and external disclosing of suspicion;

(b) the criminal and regulatory sanctions in place, both in respect of the liability of the financial institution and personal liability for individuals, for failing to report information in accordance with the policies, procedures and controls of the financial institution;

(c) the identity and responsibilities of the MLRO, CO and Deputy MLRO;

(d) dealing with business relationships or occasional transactions subject to an internal disclosure, including managing the risk of tipping off and handling questions from customers;

(e) those aspects of the financial institution's business deemed to pose the greatest ML and TF risks, together with the principal vulnerabilities of the products and services offered by the financial institution, including any new products, services or delivery channels and any technological developments;

(f) new developments in ML and TF, including information on current techniques, methods, trends and typologies;

(g) the financial institution's policies, procedures and controls surrounding risk and risk awareness, particularly in relation to the application of CDD measures and the management of high risk and existing business relationships;

(h) the identification and examination of unusual transactions or activity outside of that expected for a customer;

(i) the nature of terrorism funding and terrorist activity in order that employees are alert to transactions or activity that might be terrorist-related;

(j) the vulnerabilities of the financial institution to financial misuse by PEPs, including the effective identification of PEPs and the understanding, assessing and handling of the potential risks associated with PEPs; and

(k) UN, EU and other sanctions and the financial institution's controls to identify and handle natural persons, legal persons and other entities subject to sanction.

The list included above is non-exhaustive and there may be other areas the financial institution may deem appropriate to include, based on the business of the financial institution and the conclusions of its business risk assessments.

12.8 Additional Training requirement

The financial institution shall also identify employees who, in view of their particular responsibilities, should receive additional and ongoing training, appropriate to their roles, and it shall provide such additional training.

This section set out those categories of employee who are to be provided with additional training, together with the particular focus of the additional training provided. The categories below are not exhaustive and the financial institution may identify other employees who it considers require additional training.

12.8.1 The Board and Senior Management

The Board and senior management must receive adequate training to ensure they have the knowledge to assess the adequacy and effectiveness of policies, procedures and controls to counter the risk of ML and TF.

The additional training provided to the Board and senior management must include, at least, a clear explanation and understanding of:

- offences and penalties arising for non-reporting or for assisting money launderers or those involved in terrorist financing;
- requirements for CDD including verification of identity and retention of records; and
- in particular, the application of the financial institution's risk-based strategy and procedures.

12.8.2 The Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer

Ongoing professional development, including participating in professional associations and conferences, is vital for MLROs/ DMLROs. In addition, MLROs and DMLRO should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to:

(a) AML/CFT legislative and regulatory requirements;
(b) the international standards and requirements on which the Mauritius' strategy is based, namely the FATF 40 Recommendations and ML/TF typology reports that are relevant to their business;
(c) the identification and management of ML/TF risk;
(d) the design and implementation of internal systems of AML/CFT control;
(e) the design and implementation of AML/CFT compliance testing and monitoring programs;
(f) the identification and handling of suspicious activity and arrangements and suspicious attempted activity and arrangements;
(g) the money laundering and terrorist financing vulnerabilities of relevant services and products;
(h) the handling and validation of internal disclosures;
(i) the process of submitting an external disclosure;
(j) liaising with law enforcement agencies;
(k) money laundering and terrorist financing trends and typologies; and
(l) managing the risk of tipping off.

12.8.3 The Compliance Officer

The CO is responsible for ensuring continued compliance with the requirements of FIAMLA and FIAML Regulations 2018 and having an overall oversight of the program for combatting money laundering and terrorism financing amongst others (Regulation 22(3) of FIAML Regulations 2018).

The CO should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to, addressing the monitoring and testing of compliance systems and controls (including details of the financial institution's policies and procedures) in place to prevent and detect ML and TF.

Chapter 13: Independent Audit

13.1 Introduction

This chapter is designed to assist financial institutions in meeting their regulatory and legal requirements through independent compliance audit.

Regulation 22(1) (d) of the FIAML Regulations 2018 requires that financial institutions shall have in place an audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA and FIAML Regulations 2018.

An AML/CFT independent audit is a vital element of any effective compliance programme for financial institutions. By virtue of the FIAMLA and FIAML Regulations 2018, there is a statutory obligation on every financial institution to have in place an audit function which will allow the reporting entity to evaluate its AML/CFT programme and to ascertain whether the established policies, procedures, systems and controls are adapted with the money laundering and terrorism financing risks identified. The objective of an independent audit is to form a view of the overall integrity and effectiveness of the AML programme, including policies, procedures and processes.

Conducting a successful independent audit enables a financial institution to ensure that its policies, procedures and controls remain up to date, recognise deficiencies in regulatory compliance system and develop ways to remediate the breaches in order to be compliant with the prevailing legislation.

13.2 Scope of independent audit

In line with international best practices, the independent audit exercise should be risk-based. Independent audit is the financial institution's final line of defence, therefore, it is vital to ensure that the AML/CFT independent audit is tailored to the financial institution's risks.

The scope of the independent audit exercise is mainly a verification of the AML/CFT risk faced by the financial institution.

Typically, every independent audit should mandatorily test compliance in the following non-exhaustive areas:

- AML/CFT policies and procedures;
- Internal Risk Assessment;
- Risk Assessment on the use of third-party service providers (Outsourcing);
- Compliance Officer function and effectiveness;
- MLRO function and effectiveness;
- Implementation and Effectiveness of Mitigating Controls, including customer due diligence and enhanced measures;
- AML/CFT Training;
- Record Keeping Obligations;
- Targeted Financial Sanctions; and
- Suspicious Transaction Monitoring and Reporting.

If a financial institution relies on automated systems or manual processes to implement its AML/CFT programme, the reliability of these systems and processes should also be considered during the independent audit on a risk-basis.

13.3 Choosing the Audit Professional

Regulation 22 (1) (d) of the FIAML Regulations 2018 requires the audit process to be carried out independently. This implies that the person or firm conducting the audit should be independent and must not be involved in the development of a financial institution's AML/CFT risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme.

The audit function should therefore be independent of, and separate from the operational and executive team dealing with the AML/CFT processes of the financial institution. An independent audit review may be conducted by an internal or external audit professional.

The person or firm conducting the audit should have the necessary skills, qualifications, relevant experience of the audit process, have a proper understanding of the FIAMLA and its supporting regulations as well as sufficient knowledge of the financial institution industry. In order to ensure that the audit is properly conducted as required under the FIAMLA and FIAML

Regulations 2018, the audit professional needs to provide quality recommendations, so that the financial institution can use the findings and recommendations to improve upon deficient areas.

13.3.1 Assessing the "independence" of the audit professional.

In all cases, the financial institution must be satisfied and able to demonstrate that the person or the firm undertaking the audit is adequately independent from the area of the business function responsible for risk assessment and AML/CFT programme, and ensure that there are no conflicts of interest. Therefore, the independent audit may be conducted by an in-house audit professional not involved in the development and implementation of the AML/CFT programme or outsourced to external accountants or independent consultants duly regulated or registered by relevant competent authorities.

When sourcing an external audit professional to conduct the audit, the financial institution should conduct some level of due diligence as listed in Section 13.3 to confirm the proposed or selected professional candidate has the requisite competence. The criteria considered by the financial institution when assessing the independence and relevant experience of the external audit professional to effectively perform the audit, should be properly documented and shall be made available to the Commission upon request.

In order to assess the independence of the audit professional, the financial institution should ensure that the following non-exhaustive pertinent areas are addressed:

- Was the audit professional involved in the development of the entity's risk assessment? Or the creation, implementation or maintenance of the AML/CFT programme?
- Does the audit professional have financial interest in the business? If yes, would their interests be harmed by the results of the audit, or could there be influence over the audit outcome?
- Does the audit professional have any relationship with any shareholder, director, senior management and or employees?

13.4 Frequency of the Independent Audit

The frequency and extent of the review should be commensurate with the licensee's size, nature, context, complexity and internal risk assessment.

All financial institutions should consider the appropriateness and effectiveness of its compliance arrangements and its policy for the review of compliance at a minimum annually, or whenever material changes to the financial institution or legislative and regulatory obligations occur. However, the financial institutions can determine for themselves the frequency to have their audits conducted. The greater the AML risk of the financial institution, and of the rate of change of the financial institution's business, the greater should be the frequency of audit.

For any business that does not have clients during the reporting period, the financial institution must ascertain the frequency to conduct its independent audit. It may be appropriate that the audit cycle be extended if the financial institution has no clients and no clients have been onboarded or exited since the previous independent audit is conducted.

For a financial institution that is in process of being wound up, it is recommended that at least one final independent audit is carried out until the financial institution is no more considered as a reporting entity under the FIAMLA.

The basis for the audit frequency must be clearly articulated in the financial institution's audit policy and scope.

13.5 Key components of the AML/CFT programme

The independent audit report must express views on whether the AML/CFT risk assessment and the AML/CFT programme comply with the requirements of FIAMLA and supporting legislations and whether the programme is functioning effectively in practice as required and intended, and has been over the course of the period. The independent audit will involve obtaining a good understanding of the financial institution's business, reviewing relevant core documents, file testing, testing of the live application of policies and procedures, and interviewing a cross-section of players. The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

Within the framework of the AML/CFT programme itself, the independent audit shall inter alia:

- address the adequacy of AML/CFT risk assessment, including whether it addresses the specific business activities of that particular financial institution;
- test compliance of the financial institutions' AML/CFT programme, policies and procedures with the FIAMLA, FIAML Regulations 2018, and the AML/CFT

Handbook and a general review of the effectiveness of the compliance function considering the risks identified through the risk assessment;

- assess the employees' adherence to the AML policies and procedures;
- assess employees' knowledge of the AML/CFT laws, regulations, guidance, and policies & procedures;
- examine the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures and processes, and whether they comply with higher-level internal requirements in the financial institution. This may include considering the adequacy of onboarding paperwork and considering the adequacy of enhanced measures against the findings of the risk assessment;
- conduct appropriate customer file testing, with particular emphasis on high risk operations (products, service, customer and geographical locations);
- examine the adequacy of the policies and procedures as well as the processes for identifying and reporting suspicious transactions promptly;
- if an automated system is not used to identify or aggregate large transactions, the audit should include sample test of how the compliance officer conducts monitoring;
- conduct appropriate transaction file testing, 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;
- examine the adequacy of the policies and procedures as well as the processes for screening for targeted financial sanctions as well as implementing prohibitions, freezing assets, and reporting to competent authorities;
- review how the financial institution is screening for targeted financial sanctions without delay when onboarding clients or conducting transactions and when the lists are updated (within hours), and the appropriateness of periodic screening frequency;
- conduct appropriate testing of TFS screening records, including a review of false positives, to determine the adequacy, completeness and effectiveness of the TFS process;
- examine the integrity and the accuracy of the management information systems use in the AML compliance programme; and
- assess training adequacy including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

Overall, the audit professional should decide whether the audit coverage and frequency are appropriate to the risk profile of the financial institution.

13.6 Audit outcome, report and recommendations

The audit will result in a signed and dated written report by the audit professional to ensure that the audit programme:

- covers all relevant components of the compliance programme as required under FIAMLA and relevant regulations;
- was adequate and effective throughout a specified period;
- identifies areas where the financial institution did not meet minimum legal or regulatory standards, and include actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effectiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a recommended course of action.

A key element of the whole audit process is effective follow-up. Failure to address recommendations and findings of previous audits should be red flagged to the board or audit committee and will be in any regulatory inspection. The findings of the independent audit report, highlighting recommendations and deficiencies, should be reported to senior management and to the board of directors.

It is the responsibility of the board of directors of the financial institutions to take appropriate corrective actions to remediate any issues identified in the independent audit report within the specified timelines.

13.7 Filing to the Commission

Financial institutions are not required to file their independent audit report with the Commission periodically. However, the financial institution shall file its independent audit report for a specified period, upon the request of the Commission.

All independent audit documentation, including, *inter alia*, work plan, audit scope, transaction testing, should also be properly documented and shall be made available to the Commission upon request.

The Commission may *inter-alia*, request the following information:

(i) whether the financial institution has adequate policies and procedures in place for independent audit exercise;

(ii) what AML/CFT issues have been identified;

(iii) what are the controls and procedures in place to ensure that all risks identified are remediated in a timely manner;

(iv) when the financial institution has conducted its last independent audit;

(v) when the next independent audit exercise would be scheduled;

(vi) whether, from a corporate governance perspective, the financial institution is considering of rotating the audit professional after performing audit after a specific number of years, as it deems appropriate.

Annex 1: List of Acronyms

Acronyms	Full Terms
AML	Anti - Money Laundering
AML/CFT	Anti - Money Laundering and Combatting of Terrorism Financing
CDD	Customer Due Diligence
CFT	Combatting Financing of Terrorism
CO	Compliance Officer
DMLRO	Deputy Money Laundering Reporting Officer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIAMLA	The Financial Intelligence and Anti - Money Laundering Act
FIAML Regulations 2018	The Financial Intelligence and Anti - Money Laundering Regulations 2018
FIU	Financial Intelligence Unit
FSC	Financial Services Commission
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
TF	Terrorism Financing