October 2025

License no: GB25204451

AddUp Markets Ltd

Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (AMLCFTP) Framework

(*an extract*)

Version 1.0

Table of Contents

1. AMLCFTP

1.1 Introduction

AddUp Markets Ltd is a private company, incorporated under the laws of the Republic of Mauritius.

The Company holds a Global Business Licence issued under Section 72 (6) of the Financial Services Act and an Investment Dealer (Full-Service Dealer excluding Underwriting) license issued under Section 29 of the securities Act 2005, Rule 4 of the Securities (Licensing) Rules 2007.

In view of combatting money laundering, the financing of terrorism, and proliferation financing, among other financial crimes described in the FCC Act, the Company must comply with the following primary legislative requirements under Mauritian law, being the FIAMLA 2002, the FIAMLR 2018, FIAMLR 2019, the FSC Handbook, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the FCC Act 2023, the AMLA 2024 among others.

The Board of the Company is required to adopt internal AMLCFTP policies and establish internal procedures; allocate responsibilities to ensure that AMLCFTP policies and procedures that meet AMLCFTP legal obligations are introduced and maintained.

The Company is based in Mauritius with its registered office being located at the Company Administrator's office where primary records are maintained.

1.2 Objectives and scope

The AMLCFTP Framework (hereinafter referred as the 'Framework' or 'Manual') refers to this framework in which, money laundering, terrorism financing, proliferation, and financial crimes, are managed through adequate policies, processes, practices, procedures and plans to discharge the Company's statutory duties, regulatory obligations, professional ethics, and agreed standards.

This manual applies to the Company and outlines its responsibility for:

- Due Diligence exercise
- Know your Customer / Know Your Business / Know Your Transactions / Know Your Employees exercise
- Detection and Prevention of money laundering, terrorism financing, proliferation and financial crimes
- Screening of existing and potential customers, service providers and employees/ officers regarding PEP classifications, enforcement actions, adverse media publications and sanctions among others
- Enterprise-Wide Risk Assessment (Business Risk Assessment and Customer Risk Assessment)
- Third Party Risk Assessment
- Customer identification program and customer acceptance policy
- Transaction Monitoring
- Record-keeping
- Suspicious Transaction Reporting
- AMLCFTP Training
- Implementation of targeted sanctions.

This document shall be read as being part of the Company's risk management framework and may be supplemented with relevant processes which may be amended from time to time.

The Company is the owner of this Framework and the responsibility to ensure that this Framework is up to date and implemented satisfactorily shall lie with the Board of the Company in alignment with its duty to ensure that the Company is managed effectively. The Board is expected to be in the best position to understand and evaluate all potential risks to the financial institution, including those of money laundering, terrorism financing, proliferation and financial crime.

1.3 Legislation in Mauritius

The Mauritian AMLCFTP legislative framework is provided for in the following Acts/Enabling Laws/Regulations/Guidelines[1]:

a) FIAMLA 2002 (and any amendments made/issued thereafter)
b) FIAMLR 2018 (and any amendments made/issued thereafter)
c) FIAMLR 2019 (and any amendments made/issued thereafter)
d) The Financial Services Act 2007 (and any amendments made/issued thereafter)
e) FSC Handbook (and any amendments made/issued thereafter)
f) FSC's Competency Standards (and any amendments made/issued thereafter)
g) Prevention of Corruption Act 2002 (and any amendments made/issued thereafter)
h) Prevention of Terrorism Act 2002 (and any amendments made/issued thereafter)
i) UNSA 2019 (and any amendments made/issued thereafter)
j) FCC Act 2023 (and any amendments made/issued thereafter)
k) AMLA 2024 (and any amendments made/issued thereafter)

The main purpose of the AML legislation is to define and criminalize the laundering of proceeds generated from all serious criminal offences aiming at depriving criminals from the profits of their crimes.

Pursuant to AML legislation, the Company is obliged to apply appropriate policies, controls and procedures that are proportionate to its nature and size to mitigate and effectively manage the risks of money laundering and terrorist financing. Those procedures, which are implemented by the Company, as these are requested by the Law, are the following:

a. Identification and due diligence procedures of the Customers of the Company.

b. Record keeping procedures in relation to Customers' identity.

c. Internal reporting procedures to a competent person (e.g. Anti-Money Laundering Reporting Officer) appointed to receive and consider information that give rise to knowledge or suspicion that a Customer is engaged in money laundering activities.

d. Appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities.

e. Measures for making employees aware of the above-mentioned procedures to prevent money laundering and of the legislation relating to money laundering.

f. Provision of regular training to their employees in the recognition and handling of transactions suspected to be associated with money laundering.

The Company shall take appropriate measures to identify and assess the risks of money laundering and terrorist financing, taking into account risk factors, including those relating to the Customers, countries or geographical areas, products, services or channels. These measures should be in proportion to the nature and size of the Company. These risk assessments shall be documented, updated.

1.4 Definition of Money Laundering

Money laundering is defined broadly and includes all forms of handling or possessing criminal property, including possessing the proceeds of one's own crime, and facilitating any handling or possession of criminal property. Criminal property may take any form, including money, securities, tangible property and intangible property.

[1] As per the definition of provided in AMLA 2024, "guidelines" include codes, guidance notes, practice notes and other similar instruments issued by a supervisory body.

Illegal profits can be generated for example through drug trafficking, illegal arms sales, smuggling, insider trading, embezzlement, corruption & bribery, prostitution, and internet fraud schemes and any other criminal offence punishable in the Republic by a term imprisonment exceeding one year.

Businesses and individuals need to be alert of the risk of clients, their counterparties and others laundering money in any of its possible forms. The business or its client does not have to be a party to money laundering for a reporting obligation to arise.

Money laundering is not only about cash transactions. Money laundering can be achieved through virtually every medium and financial institution or business.

For the purpose of this Manual, money laundering is also taken to encompass activities related to terrorist financing, including handling or possessing funds to be used for terrorist purposes as well as proceeds from terrorism.

1.5 Stages for Money Laundering

There is no single method of laundering money. Despite the variety of methods employed, the laundering process is accomplished in three basic stages which may comprise transactions by the launderers that could alert a financial institution to criminal activity:

a) Placement – The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.

b) Layering – The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's cheques, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewellery. All these transactions are designed to disguise the audit trail and provide anonymity.

c) Integration – The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used. If the layering process is successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

The three basic steps may occur as separate and distinct phases or may occur simultaneously or, more commonly, they may overlap. How the basic steps are used depends on the available laundering mechanisms and requirements of criminal organizations.

1.6 General Examples of Money Laundering Situations

Significant cash transactions: If a person is making thousands of dollars is small change a week from a business (something which is not unusual for a store owner) and wishes to deposit that money in a bank, it cannot be done without possibly drawing suspicion. In the United States, for example, cash transactions and deposits of more than a certain dollar amount are required to be reported as "significant cash transactions" to the Financial Crimes Enforcement Network (Fin CEN), along with any other suspicious financial activity which is identified as "suspicious activity reports". In other jurisdictions suspicion- based requirements are placed on financial services employees and firms to report suspicious activity to the authorities.

Irregular funding: One method of keeping this small change private would be for an individual to give money to an intermediary who is already legitimately taking in large amounts of cash. The intermediary would then deposit that money into an account, take a premium, and write a check to the individual. Thus, the individual draws no attention to himself, and can deposits his check into a bank account without drawing suspicion. This works well for one- off transactions, but if it occurs on a regular basis then the check deposits themselves will form a paper train and could raise suspicion.

Captive business: Another method involves establishing a business whose cash inflow cannot be monitored and passing the small change into this business and paying taxes on it. All bank employees however are trained to be constantly on the lookout for any transactions which appear to be an attempt to get around the currency reporting requirements. Such shell companies should deal directly with the public, perform some service- related activity as opposed to providing physical goods, and reasonably accept cash as a matter of business. Dealing directly with the public ensures plausible anonymity of source. An example of a legitimate business displaying plausible anonymity of source would be a hairstylist. Since it would be unreasonable for them to keep track of the identity of their clients, a record of their transaction amounts must be accepted as primary evidence of actual financial activity. Service- related business have the advantage of anonymity of resources. A business that sells computers has to account for where it actually got the computers, whereas a plumbing company merely has to account for labor, which can be falsified.

Corrupt politicians and lobbyists also launder money by setting up personal accounts to move money between trusted organizations, so that donations from inappropriate sources may be illegally used for personal gain.

Structuring (“smurfing”): Smurfing is possibly the most commonly used money laundering method. It involves many individuals who deposit cash into bank accounts to avoid the reporting threshold.

Bank Complicity: Bank complicity occurs when a bank employee is involved in facilitating part of the money laundering process.

Money Services and Currency Exchanges: Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the company. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers’ cheques, and traveler’s cheques.

Asset Purchases with Bulk Cash: Money launderers may purchase high value item such as cars, boats or luxury items such as jewelry and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate’s name.

Electronic Funds Transfer: Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.

Postal Money Orders: The purchase of money orders for cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.

Credit Cards: Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchases high value items or to convert the credit balance into cheques.

Casinos: Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.

Refining: This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.

Legitimate Business/ Co- mingling of funds: Criminal groups or individual may take over or invest in business that customarily handles a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase business that commonly receive cash payments, including restaurants, bars, night clubs, hotels, currency exchange shops, and vending machine companies. They will then insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.

Value Tempering: Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price “under the table". In this way, the launderer can, for example, purchase a €2 million, while secretly passing the balance to the seller. After holding the property for a period of time, the launderer then sells it for its value of €2 million.

Loan Back: Using this method, a criminal provides an associate with a sum of illegitimate money and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of the necessary documentation. This creates an illusion that the criminal's funds are legitimate.

The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal and providing another means to transfer money.

1.7 Definition of Terrorism Financing

Terrorism is defined as the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

Terrorism financing is an offence by any means, directly or indirectly, unlawfully and willfully, which provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, in order to carry out an act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

a. Offence of ML

The Company is required to comply with both the provisions of the The Company is required to comply with both the provisions of the FCC Act 2023 and the FIAMLA in relation to obligation to prevent money laundering offences.

The FIAMLA and the regulations thereunder, on the other hand, has provided detailed obligations on financial institutions to prevent money laundering offences which include the Company to appoint an MLRO, a Deputy MLRO and a compliance officer and to meet prescribed due customer due diligence requirements.

The offence of Money Laundering is described under section 36 (1) of the FCC Act 2023 as follows:

"(1) Any person who –

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

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

where he suspects or has reasonable grounds to suspect that the property is derived or realised, in whole or in part or directly or indirectly, from any crime, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years.

(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 and shall, on conviction, be liable to a fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years.

…

(4) In this Act, reference to concealing or disguising property which, or in whole or in part or directly or indirectly, is or represents the proceeds of a crime, shall include concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

b. Offence of Bribery

In alignment with sections 19 and 20 of the FCC Act 2023, a person[2] engaging in an act of bribery by a public official or of a public official shall commit an offence and shall, on conviction, be liable to a fine not exceeding 20 million rupees and to penal servitude for a term not exceeding 10 years.

c. Financial Crime

The Company is a legal person for the purposes of the FCC Act 2023 and as such has the obligation to have adequate procedures in place to prevent it or any person acting on its behalf from committing an offence under Part III of the FCC Act 2023. This paragraph of this Manual constitute the framework under the FCC Act 2023 to prevent the Company and any of its staff members (a Covered Person) from the commission of any financial crime.

*Financial Crimes under the FCC Act 2023 consist of various offences related to financial misconduct under Part III of the FCC Act 2023, any crime committed under the law of any financial or competent authority which, in view of its financial implications, complexity, scope, nature or in the public interest, the Financial Crime Commission ("**FCC**") decides, after consultation with that authority, that it shall investigate into the matter and includes any ancillary offence relating to the foregoing.*

Part III of the FCC Act 2023 is divided into six sub-parts:

(a) Corruption Offences which address various forms of bribery and corruption, including bribery of public officials, offences related to influencing public officials, bribery in contract procurement, and corruption in private entities.

(b) Money Laundering Offences: This section focuses on activities involving the processing of criminal proceeds to disguise their illegal origins. It also includes provisions for the limitation of cash payments to prevent money laundering.

(c) Fraud Offences: It covers fraudulent activities such as fraud by false representation, fraud by failing to disclose information, and electronic fraud.

(d) Financing Drug Dealing Offences: This section criminalises the financing of drug trafficking activities.

(e) Other Offences: This includes offences such as conspiracy, aiding and abetting crimes, and breaches of guidelines.

(f) Obligations and Liability of Legal Persons: It imposes obligations on legal persons and sets out their liability for financial crimes.

The table below shows a summary of the offence classification:

Corruption Offences	*Bribery by public official* *Bribery of public official* *Taking gratification to screen offender from punishment* *Public official using his office for gratification* *Bribery of, or by, public official to influence the decision of public body* *Influencing public official* *Traffic d'influence* *Public official taking gratification* *Bribery for procuring contracts* *Bribery for procuring withdrawal of tenders* *Conflict of interests* *Treating of public official* *Receiving gift for corrupt purpose*

[2] In alignment with the FCC Act 2023, a 'Person' shall include a natural person or legal person.

	Corruption in private entities *Corruption to provoke serious offence* *Bribery by, or of, foreign public official* *Corruption in relation to sporting events*
Money Laundering Offences	*Money laundering* *Limitation of payment in cash* *Alleged proceeds of crime*
Fraud Offences	*Fraud by false representation* *Fraud by failing to disclose information* *Making or supplying articles for use in fraud offence* *Failing to pay for goods and services* *Fraud by abuse of position* *Electronic fraud*
Financing Drug Dealing Offences	*Financing of drug dealing*
Other Offences	*Making or supplying articles* *Possession of articles* *Conspiracy* *Aiding, abetting or counselling* *Attempt* *Penalty for breach of guidelines*
Ancillary offences	*Any crime committed under the law of any financial or competent authority which, in view of its financial implications, complexity, scope, nature or in the public interest, the Commission decides, after consultation with that authority, that it shall investigate into the matter; and includes any ancillary offence to the above listed crimes.*

The Board shall ensure that processes and procedures are implemented to ensure that the Company or its services are not misused to camouflage instrumentality, where instrumentality is defined by the FCC Act 2023 as follows: *"instrumentality – (a) means any property used or intended to be used in any manner in connection with a criminal offence or unlawful activity; and (b) includes a benefit…"*

d. Non-Compliance

Any non-compliance with the abovementioned laws, regulations, guidelines will entail regulatory and internal sanctions, where applicable.

Any breach of the provisions under this Manual shall trigger warnings and/or disciplinary actions and/or potential sanctions which shall be determined by the Board. Should a Board Member be involved in the breach reported/observed, then the latter will not be authorised to vote on the disciplinary actions and potential sanctions.

In line with section 18 (3) of the FIAMLA, where it appears or where it is represented to the FSC that any financial institution falling under its purview has refrained from complying, or has failed to comply, with any requirement imposed under the FIAMLA 2002, any regulations made under the FIAMLA 2002 or any guidelines issued or under the FSA, and that the failure has been caused by a ***negligent act, an omission or by a serious defect in the implementation*** *of any such requirement, the FSC may proceed against the Company under section 7 of the FSA.*

2. Roles and responsibilities

The Company's organisational structure is made up of the following:

a) Board Members consisting of executive and non-executive directors;

b) Dealing Team Members;

c) Money Laundering Reporting Officer ('MLRO') and Deputy MLRO;

d) Compliance Officer;

e) Company Administrator;

f) Back Office Support Team; and

g) Employees and Officers.

2.1. Lines of Defence

The Company's AMLCFTP Risk Management Strategy is inspired by the three Lines of Defence ('LoD') framework. The three LoD strategy is a risk management framework that is used to help organisations identify, assess and mitigate risks. The framework is based on the principle of segregation of duties, which means that different people or groups of people are responsible for different aspects of risk management.

By having different people or groups of people responsible for different aspects, the organisation can reduce the risk of errors and omissions. Additionally, the framework can help to ensure that risks are identified and managed in a timely and effective manner.

First line: Business Units/Operational Management

The First LoD is made up of the firm's operational and customer-facing teams. These teams deal with risk as part of their day-to-day activities and as such it is deemed most practical for them to be responsible for owning and managing those risks. The First LoD primarily consists of operational management teams, business units, directors, dealing team members, Client acceptance/onboarding teams, transaction processing teams, HR teams, marketing teams, among others. The key role of the First LoD is to understand the risks that arise in their area of the business and make sure there are suitable controls in place to mitigate them, in line with the Company's overall risk management framework. Examples of how to managem risks at this stage involve timely trainings, timely reporting of risks, updating checklists/process sheets when conducting a task among others.

Second line: Risk management & compliance

The second LoD is the risk management function of the Company. The risk management function is responsible for providing oversight, support and guidance to the first LoD in their risk management activities and challenge where necessary, and building and maintaining the frameworks that support the first LoD to manage their risks in line with the Company's overall approach and risk appetite set by the board, and in compliance with all regulatory requirements and guidelines. This includes tasks such as monitoring and reporting on risk and ensuring policies laid out are fit for purpose.

Third line: Internal/External audit

The third LoD is the audit function which can be implemented internally or externally. The audit function is responsible for providing independent assurance that the Company's risk management framework is effective. This includes testing the effectiveness of risk controls and issuing audit reports.

The intention behind implementing a 3 LoD infrastructure contributes to the following:
- improving the overall risk management maturity of the Company;
- reducing the risk of errors and omissions;
- ensuring that risks are identified and managed in a timely and effective manner; and
- improving the efficiency and effectiveness of the organisation's risk management function.

The key to making the most of the Three LoD is ensuring that roles don't start to blur into each other. The Company shall ensure that there is open communication across the three lines, but their areas of responsibility should remain distinct. In particular, it's important for the second line to maintain independence and distance from the first lin's activities. For example, a second line team member might assist in creating a tool to help first line build and run a risk assessment process however the second line is not responsible for actually building or running the assessment themselves.

2.2. Board

The Board of Directors and Senior Management have the responsibility to inter-alia:

a) design, implement and monitor an AMLCFTP framework for the Company;
b) undertake timely risk assessments of the business, of the customers, of third parties among others;
c) Allocate responsibilities to officers/departments/service providers to ensure that AMLCFTP policies, procedures, processes, systems are performed satisfactorily;
d) arrange for the a training programme on AMLCFTP and financial crime for the Company and its officers/employees;
e) Promote a healthy and efficient AMLCFTP compliance culture.

The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the Company, including those of money laundering, financing of terrorism, proliferation and financial crime. The Board must therefore take ownership of, and ultimate responsibility for, the enterprise-wide risk assessments which include the Business Risk Assessment, the Customer Risk Assessment and the Third-Party Risk Assessments) and ensure that they remain up to date and relevant. In so doing, the Board shall ensure that all relevant units of the Company perform their functions regarding risk identification and management effectively. On the basis of its risk assessment outcome, the Board shall establish a formal strategy for AMLCFTP and financial crime. If needed, following this exercise, this Manual shall also undergo changes are appropriate.

Where the Company forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business.

The Board has the obligation to document its systems and controls (including policies and procedures) and clearly apportion responsibilities regarding AMLCFTP and combatting of financial crime, and, in particular, responsibilities of the Compliance Officer ("CO") and Money Laundering Reporting Officer ("MLRO") (and in his/her absence the DMLRO).

In respect of the above, the Company's policy shall be to ensure:

(a) that its processes, policies, procedures, manuals are effective;
(b) that its processes, policies, procedures, manuals reviews are conducted on an adequate frequency as approved by the Board;
(c) that the extent of review of processes, policies, procedures, manuals are appropriate.

The Board shall take a risk-based approach when defining its review policy and ensure that those areas that are deemed to pose the greatest risk to the Company are reviewed more frequently.

The standard frequency for a compliance review shall be on an annual basis unless otherwise required by the Board. In this respect, earlier reviews shall be scheduled upon detection of relevant trigger event(s).

Trigger events are defined as tangible or intangible barrier(s) or occurrence(s) which, once breached or met, causes another event to occur. Trigger events include negative news/adverse media about the individual or entity, a legal status or domicile change, change in the business plan of the Company, change in the screening tool of the Company, substantive change in the client target market, substantial change in the marketing tools being used for the Company, discovery of positive sanction matches in the Company's database, too many client complaints, and so on. These trigger events will initiate a CDD process or a CDD review process or a risk assessment process, and compliance reporting among others. The action shall be circumstantial and determined on a case-to-case basis after analysis of the relevant matter at hand.

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 Company occur. Where, as a result of its review, changes to the compliance arrangements/processes/frameworks are required, the Board must ensure that the Company makes those changes in a timely manner.

The Company is responsible for appointing a CO. In addition to appointing a CO, the Company shall ensure that there is an independent audit function in accordance with Regulation 22 (d) of the FIAMLR 2018 to test the effectiveness of the money laundering and financing of terrorism policies, procedures and controls of the Company.

The Board must ensure that the compliance review policy takes into account the size, nature and complexity of the business of the Company, 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 Company's policies, procedures and controls.

According to the FSC Handbook, the Board or senior management of the Company 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 money laundering and financing of terrorism;
h) ensure adequate resources are given to the CO to enable the standards within the FSC Handbook to be adequately implemented and periodically monitored and tested; and
i) ensure procedures are established and maintained which allow the 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").

2.3. MLRO

In accordance with the FIAMLA 2002 and FIAMLR 2018, the Company must appoint an MLRO. Pursuant to Regulation 27 of FIAMLR 2018, the Company must establish, document, maintain and operate reporting procedures that shall –

(i) enable all its directors or, as the case may be, partners, all other persons involved in its management, and all appropriate employees to know to whom they should report any knowledge or suspicion of money laundering and terrorism financing activity;

(ii) ensure that there is a clear reporting chain under which that knowledge or suspicion will be passed to the Money Laundering Reporting Officer;

(iii) require reports of internal disclosures to be made to the Money Laundering Reporting Officer of any information or other matters that come to the attention of the person handling that business and which in that person's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity;

(iv) require the Money Laundering Reporting Officer to consider any report in the light of all other relevant information available to him for the purpose of determining whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing activity;

(v) ensure that the Money Laundering Reporting Officer has full access to any other information that may be of assistance and that is available to the reporting person; and

(vi) enable the information or other matters contained in a report to be provided as soon as is practicable to the FIU where the Money Laundering Reporting Officer knows or suspects that another person is engaged in money laundering or terrorism financing activities."

The primary duty of the MLRO will be receiving and evaluating internal STR and where appropriate, filing the STR with the FIU.

In the absence of the MLRO, appointment of Deputy MLRO must be duly notified to the FSC, and he/she is expected to fulfil similar duties as that of the MLRO.

2.4. Compliance Officer

As part of its compliance arrangements, the Company is responsible for designating a CO who shall be responsible for the implementation and ongoing compliance of the Company with internal programmes, controls and procedures in accordance with the requirements of the FIAMLA 2002 and FIAMLR 2018.

The CO shall have the following functions:

a) ensuring continued compliance with the requirements of the FIAMLA 2002 and FIAMLR 2018 subject to the ongoing oversight of the Board and senior management;

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

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

d) contributing to designing and implementing the AML/CFT framework for the Company.

2.5. Company Administrator

The Company has entered into an Administration Agreement with the appointed Company Administrator, which will act as the Administrator of the Company. The Company Administrator must be licensed with the FSC as a Management Company and supervised by the FSC in terms of its AML/CFT controls.

The Company Administrator will perform:

- certain administrative functions, including but not limited to customer identification and verification, performing enhanced due diligence, screening and risk profiling;

- accounting;

- registrar;
- transfer agency services for the Company (E.g. Customer / Shareholder register); and
- transactional record keeping.

Where the Company Administrator outsources certain of its functions to a Company Administrator Agent, the Company Administrator enters into an administration agreement with the Company Administrator Agent, however, the approval for the use of the Company Administrator Agent to conduct functions of the Company Administrator must be approved and vetted by the Board of the Company first.

2.6. Outsourcing of compliance-related functions

The Company may outsource some or all of its compliance functions related to AML/ CFT to a third party which shall ensure that the Company implements its program for combating money laundering and terrorism financing and managed all potential risks relating thereto in accordance with the third party's own policies and procedures.

Prior to outsourcing the compliance-related functions, the Company shall assess the policies and processes of the third party.

The Company will use the KYC Provider to conduct screening and verification of clients.

3. Customer acceptance requirements

To establish a business relationship with a prospective investor/client, the Company has to obtain the appropriate information from the person seeking to establish the business relationship or from the person acting on behalf of that prospective investor. The information obtained is required to be verified by comparing it with information and/or documentation obtained from source(s) as required by local legislation.

3.1 CDD Measures -

CDD is the key element of an internal AML/CFT system and it relates to measures taken to:

- identify and verify the identity of a customer using reliable, independent source documents, data or information;
- identify and verify all associated parties to the customer;
- screen potential and existing customers for adverse media and targeted sanctions;
- understand the nature and intended purpose of the business relationship or transaction;
- understand the ownership and control structure of the customer;
- identify and take reasonable measures to verify the identity of beneficial owners of the customer;
- determine the source of funds of the customer, and if applicable, the source of wealth;
- identify the jurisdictions associated with the customer;
- enable the Company to risk profile the customer;
- monitor customers' transactions and activities to ensure they are consistent with the Company's knowledge of the customers, their business and risk profile.

AML/CFT laws require that a risk-based approach be adopted when conducting CDD, as opposed to a tick-box approach, to ensure that the CDD measures in place correspond to the risks identified with the customer. This approach constitutes the foundation to an effective customer risk assessment which determines the extent of information and documentation to be requested from the customer, the extent to which the business relationship is scrutinized, and how often CDD documentation, data or information held is reviewed and updated.

In that respect, all customers are categorized in three distinctive risk categories, namely: **Low, Medium and High**, which is in line with FSC's Effective Customer Risk Assessment and the AML/CFT Handbook.

3.1.1 Low Risk Customer

If the level of ML/TF risk associated with the customer is assessed to be **Low**, it may be possible and appropriate to apply **Reduced or Simplified CDD**[3] measures in exceptional scenarios.

When will Simplified CDD apply?

The Company may apply simplified CDD measures where lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by the regulator.

The Company will be guided by Chapter 7 of the AML/CFT Handbook.

Where the Company determines that there is a low level of risk, it shall ensure that the low risk identified is consistent with the findings of the national risk assessment[4] or any risk assessment of the regulator, whichever is most recently issued. The latest National Risk Assessment Report was issued in August 2019.[5] An extract of the overall ML/TF vulnerability, threat and risk ratings are indicated below:

	Vulnerability Rating	Threat Rating	ML Risk Rating
Money Laundering	**Medium-High**	**Medium-High**	**Medium-High**
Terrorism Financing	**Medium High**	**Medium-Low**	**Medium**
ML Sector Ratings			
Gambling Sector	High	High	High
Trust and Company Service Providers	Medium-High	High	High
Securities Sector	Medium-High	Medium-High	Medium-High
Banking Sector	Medium	High	Medium-High
Other Financial Institutions – under BoM Supervision	Medium	High	Medium-High
Legal professions (Law Firms/Barristers/Notaries/Attorneys)	Medium-High	Medium	Medium-High
Real estate Sector	High	Medium	Medium-High
Jewellery Sector	High	Medium	Medium-High
Insurance Sector	Medium	Medium-Low	Medium
Accountancy Sector (Accountants/Auditors)	Medium	Medium	Medium
Other Financial Institutions – under FSC Supervision	Medium-High	Medium-Low	Medium
Other Financial Institutions – Credit Unions	Medium-Low	Medium-Low	Medium-Low

Simplified CDD shall not apply where the Company knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in ML/TF or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in ML/TF.

The Company 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;

[3] Please refer to Annexure H for the details of the Reduced CDD documents required

[4] The term "national risk assessment" means the report issued under section 19D(2) of the FIAMLA 2002, which provides that the Ministry of Financial Services and Good Governance shall conduct an assessment of the risks of money laundering and terrorist financing affecting the domestic market and relating to cross border activities and shall in particular, identify:

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

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

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

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

[5] Source: https://financialservices.govmu.org/Documents/NRA%20Report/Public%20Report%202019-compressed.pdf

(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 the Company 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.

Where simplified CDD measures are adopted, the Company 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.

3.1.2 Medium Risk Customer

If the level of ML/TF risk associated with the customer is assessed to be **Medium**, the **standard CDD measure**[6] is applicable.

3.1.3 High Risk Customer

If the level of ML/TF risk associated with the customer is assessed to be **High**, in addition to the standard CDD measures, an appropriate level of **Enhanced CDD**[7] should also be performed, documented and evaluated prior to the acceptance.

Enhanced CDD shall be performed:

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

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

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

(d) in relation to correspondent banking relationships, pursuant to regulation 16;

(e) subject to Regulation 15 of the FIAMLR 2018[8], where the customer or the applicant for business is a political exposed person;

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

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

---

[6] Please refer to Annexure H for the details of the standard CDD documents required

[7] Please refer to Annexure H for the details of the EDD documents required

[8] Regulation 15 of the FIAMLR 2018 relates to a foreign PEP, Domestic PEPs, International Organisation PEPs and close relatives and associates of PEPs.

.

Enhanced CDD measures that may be applied for higher risk business relationships include:

(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the customer and the beneficial owner;

(b) obtaining additional information on the intended nature of the business relationship;

(c) obtaining information on the source of funds or source of wealth of the customer;

(d) obtaining information on the reasons for intended or performed transactions;

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

(f) 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;

(g) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

The following types of Customers shall require application of the EDD:

- Politically Exposed Persons ('PEPs');
- Reputationally Exposed Persons ('REPs');
- Any Customer that their nature entails a higher risk of money laundering or terrorist financing;
- Any Customer determined by the risk profiling methodology as being High Risk and
- Any category of Customer as set out in tables 1 and 2 below.

The EDD conducted must be adequate to assess and, where necessary, identify mitigants to the identified risk(s) and/or inform the Board regarding a decision to establish, continue or terminate the business relationship or enter into a single transaction.

The following measures must be applied in cases of high-risk relationships:

1. Increased intensity of CDD measures, including verification of source of wealth;
2. Extensive ongoing monitoring must be conducted on all transactions (including but not limited to bank transactions) to verify source and destination of funds (special attention to PEPs) and ascertain whether such transactions are properly supported/evidenced (e.g. Board approval, relevant executed agreements, etc.);
3. Quarterly screening (via KYC Provider and Internet Check) must be performed;
4. Increased review periods of customer information.

It is most important for the Company that the procedures adopted to verify identity for non-face-to-face Customer relationships be at least as rigorous as those for face-to-face Customer relationships. A Customer's failure to be physically present in the identification procedure reduces the possibility for the Company to verify the identity of the person, thus increasing the risk of money laundering and terrorism financing (ML/TF). In the event that verification of identity is performed on a non-face-to-face basis, the Company will carry out these additional checks to manage risks arising from establishing such business relations with Clients:

a) verification of telephone number of the Client;
b) holding real-time video call with the Client;
c) confirmation of the Client's address through an exchange of correspondence or other appropriate method (via KYC Provider);

d) confirmation of the Client's SoF and SoW by requiring the presentation of additional documents (double verification);
e) performing screening in accordance with Section 2.6.
f) .

Where reliance is placed upon third parties for CDD measures, it is ensured that such persons/institutions are:

(i) regulated, supervised and monitored and subject to CDD in line with section 17C of the FIAMLA 2022; and
(ii) regulated, supervised and monitored and subject to record keeping requirements pursuant to section 17F of the FIAMLA 2002 and Regulation 21 of the FIAMLR 2018 which provides for third party reliance.

the group applies the measures as applicable to regulation 21(4) of the FIAMLR 2018 (when third party is part of the same financial group) Please refer to Section 2.5.6.

3.2 Business involving a material exposure to "Other higher risk customers and activities"

Business activities and services listed 9 in Table 1 below which, whilst not automatically requiring escalation to the Board, are nonetheless considered to present a higher level of risk and which therefore need to be subject to enhanced oversight.

Table 1

Category	Higher risk activities	Rationale
Cash intensive business	Casinos Betting shops	Money laundering potential
Charitable organisations	Provision of fiduciary services to charitable organisations	Increased AML/CFT risks Potential reputational risk
Consultancy	Entities solely existing for the receipt of consultancy fees or commission payments	Money laundering potential Potential tax risk
Dealers & traders in high value goods and services	Antiques Diamonds Fine Arts Precious metals and gems	Money laundering potential Provenance/title issues
Money Services Businesses	Exchange Bureaux Travel Bureaux	Increased AML/CFT risk
Natural Resources	Involvement, directly or indirectly, in mining, drilling or quarrying for natural resources	Increased Anti Bribery and Corruption risk Potential reputational risk
Public Enterprise Appointments	Provision of director/officer services to any entity whose securities are listed or traded on a public stock exchange (a "Public Enterprise") – this includes acting as a Director or Officer of subsidiaries of a publicly listed group.	Public interest dimension Potential legal liability Potential regulatory exposure Potential reputational risk
Reputationally Exposed Persons (REPs)	Any proposed new customers or prospects for whom other "relevant adverse information" (RAI) is identified during the course of the CDD/EDD process, for example:	Potential reputational risk

[9] The list is not exhaustive and may be added to or reclassified from time to time.

	• other (unresolved) due diligence information or evidence that otherwise calls into question the integrity or bona fides of the customer/prospect, such as positive World Check hits, EDD reports, etc.	

3.3 Category of Higher risk customers for Board approval

The list in Table 2 below specifies certain types of Higher risk customers, activities and services **which need to be escalated to Board for approval:**

Table 2

Category	Higher risk activities	Rationale
Government Contracts	Customers whose principal activity and/or purpose is the procurement and/or servicing of government contracts (Military, Defence, Technology, Outsourcing, Construction, etc.)	Increased potential for bribery Potential reputational risk
Initial Coin Offerings/Crypto-currencies	Provision of director/officer services to any structure engaged in initial coin offerings, cryptocurrencies or crypto exchanges.	Potential legal liability Potential reputational risk
Pharmaceuticals (including medicinal cannabis)	Manufacture, marketing or sale of pharmaceutical goods or devices which are not licensed or have not received marketing authorization in the jurisdiction where they are manufactured, marketed, sold or supplied.	Potential connection with criminal activity Potential reputational risk
Politically Exposed Persons (PEPs)	Customers/prospects that are identified as having prominent public functions or high political exposure, pose higher Money Laundering risk, particularly where connected to a region or country which is known to present a heightened risk of bribery & corruption and/or political instability.	Increased Anti Bribery and Corruption risk Potential reputational risk Regulatory requirement for enhanced oversight
Arms, armaments and ammunition	Manufacture, trading, transfer (importation/exportation) of Non Military / **Military grade** weapons, explosives, munitions or other controversial weapons	Potential connection with criminal activity Potential reputational risk
Exotic species	Dealing or trading in exotic species	Potential connection with criminal activity Potential reputational risk

Business involving a material relevant[10] connection to a country that is subject to FATF call to apply countermeasures with respect to money laundering and terrorist financing risks	The following countries are subject to a FATF call to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from these jurisdictions : **1. Iran** **2. Democratic People's Republic of Korea (North Korea)** **3. Myanmar** This list shall be amended from time to time to reflect the list of jurisdiction black listed by the FATF. It is the Company's policy **not to deal with clients or structures connected to the above countries**, other than on an approved exceptional basis.	Potential regulatory enforcement and/or reputational damage.
High Risk Countries or Territories	Business involving a **material relevant connection to a prescribed higher risk country or territory**	Potential AML/CFT risks Potential reputational risk

[10] A material relevant connection may arise by virtue of an individual's or entity's country of origin, country of residence or domicile, geographic sphere of activities, business or commercial associations, source of wealth, source of funds, etc.

3.4 Categories of Business that will NOT BE ACCEPTED

The categories of business relationships listed in Table 3 below are unlawful in Mauritius:

Table 3

Prohibited Business	Additional Guidance
1. Business that is conducted in anonymous or fictitious names	AML laws prohibit financial institutions from opening anonymous or fictitious accounts. In this context, the Company should not set up or maintain business relationship with an anonymous customer or with a customer which the Company has reasonable cause to suspect, is in a fictitious name.
2. Business relationship with a shell bank.	The Company shall not enter into or continue business relationship or occasional transaction with a shell bank (entity). A "shell bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.
3. Business relationship with clients from Prohibited jurisdictions	The Company shall not enter into or continue business relationship or occasional transaction with a client from Prohibited jurisdictions. It is the Company's policy **not to deal with** clients or structures connected to the Prohibited countries. This list shall be amended from time to time.

The categories of new businesses listed in Table 4 below are considered to be outside of the Company's risk appetite and are therefore prohibited:

Table 4

Prohibited Business	Additional Guidance
1. Business that violates the Company's **zero tolerance approach to non- compliance with applicable economic sanctions imposed by the European Union ("EU"), United Nations Security Council ("UNSC"), US Office of Foreign Assets Control ("OFAC"), United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ("UNSA")**	▪ The United Nations Security Council's website; ▪ U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") website; and ▪ European Commission's website.
2. Business that violates the Company's **zero tolerance approach to bribery[11] and corruption[12]**	Best Practices Paper: The Use of the FATF Recommendations to Combat Corruption (FATF Publication)
3. Business involving activities by serviced entities that would constitute **tax fraud or tax evasion** in	Best Practices: Managing the anti-money laundering and counter-terrorist financing policy

[11] Bribery typically involves offering, promising, giving or receiving a financial (or other) advantage with the intention to induce the recipient or any other person to act improperly in the performance of their functions, or to reward them for acting improperly.

[12] Corruption involves the abuse of entrusted power or position for personal or commercial gain and often includes bribery.

	the jurisdictions where those activities are taking place.	implications of voluntary tax compliance programmes (FATF Publication)
4.	Business involving activities by the Company's applicants for business that are illegal in the jurisdiction(s) in which the activities are carried out, and/or which would be illegal if carried out in the jurisdiction(s) from which the Company would be providing the services.	Reference to be made to FIAMLA 2002 and FIAMLR 2018

5. Business involving **"Unacceptable activities"**

*The following activities are illegal and/or considered to be reputationally unacceptable and are therefore **prohibited** by the Company:*

Category	Prohibited activities
Bearer Share entities	• Provision of formation, domiciliation and/or administration services to any entity that has issued, or has the ability to issue bearer shares
Environmental Social Governance (ESG)	• Mining and trade of rough diamonds unless Kimberly certified • Destruction of high conservation value areas • Ship breaking • Products or activities that impinge upon the lands owned or claimed under adjudication by indigenous and/or vulnerable people or groups without full documented free prior and informed consent (FPIC) of such people or groups
Modern Slavery	• Child labour • Forced labour
Red light business	• Paedophilia • Prostitution and distribution of adult entertainment • Pornography • Strip Clubs
Waste products	• Cross border trade of waste or waste product unless compliant with Basel Convention and underlying regulations • Shipment of oil or hazardous substances in single hull carriers or in tankers not compliant with International Maritime Organisation (IMO) requirements • Cross border trade of radioactive material or unbounded asbestos fibers

3.5 Inability to conduct CDD

If the Company is unable to:

- establish and verify the identity of a customer or other relevant person;
- obtain information to understand the nature and intended purpose of the business relationship and source of funds; or
- conduct on-going due diligence,

the Company:

- may not establish a business relationship or conclude a single transaction with a customer;
- may not conclude a transaction in the course of a business relationship, or perform any act to give effect to a single transaction; or
- must terminate an existing business relationship with a customer

and shall submit a STR if the circumstances which prevent the Company from conducting customer due diligence are suspicious or unusual.

For more details on the CDD documentation, please refer to the CDD checklist in Annexure 4.

3.6 Third Party Reliance

The Company 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 Company shall ensure that the identification information sought from the third party is adequate and accurate. The third party must be regulated, supervised, monitored for AML/CFT purposes and subject to CDD in line with section 17C of the FIAMLA 2002 and record keeping requirements pursuant to section 17F of the FIAMLA 2002 and Regulation 21 of the FIAMLR 2018 which provides for third party reliance.

Moreover, where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the Company.

When reliance is placed on a third party that is part of the same financial group of the Company, the latter must ensure that the group applies the measures as applicable to Regulation 21(4) of the FIAMLR 2018.

3.7 Screening

Screening covers Targeted Sanctions, PEP's and Adverse Media on the customers, Associated Parties, BO(s) and all parties identified in the organisational and control structure. The Company shall ensure that its customers, connected parties of customers and all natural persons appointed to act on behalf of customers are screened through KYC Provider Check and Internet Check for the purpose of determining if there are any money laundering and terrorism financing risks in relation to the customers.

All new customers and their Associated Parties (including BO., Immediate, Intermediate and ultimate owners) must be screened up front through KYC Provider Check and Internet Check, prior to on boarding. Existing customers must also be screened regularly. It is the Company's responsibility to ensure that ongoing screening is carried out on its applicants for business.

Regularly under this paragraph is defined as follows:

Low Risk	Medium Risk	High Risk	PEP	Trigger event
Annually	Bi-Annually	Quarterly	Quarterly	Immediately (24 hours from date of identification of trigger event)

Any new employees of the Company shall also be screened against UN's list of designated persons under terrorist and proliferation financing, targeted sanctions prior to employment and annually thereafter.

3.8 Sanctions Screening

Targeted sanctions are restrictive measures imposed on individuals and/or legal entities in an effort to maintain or restore international peace and security as an alternative to the use of armed force. These restrictive measures include, but are not limited to, financial sanctions, trade sanctions and travel restrictions. They exist for a variety of political, military, social and economic reasons, and work by preventing individuals and/or legal entities engage in abusive activities (for example, terrorist financing or the purchasing of weapons of mass destruction).

Why does Mauritius need to implement Targeted Sanctions?

The United Nations (UN) imposes sanctions and requires member states to implement them through the resolutions passed by the UN Security Council which has the primary responsibility for the maintenance of international peace and security. Mauritius, as a member of the UN, is mandated to implement the United Nations sanctions regimes including those related to terrorism and the proliferation of weapons of mass destruction. In addition, Mauritius, being an International Financial Centre, and founder member of the Eastern and Southern Africa Anti Money Laundering Group is committed to comply with international standards, namely the Financial Action Task Force Standards ('FATF'), to protect the integrity of its financial system. The FATF requires countries to implement targeted financial sanctions related to terrorism and terrorist financing under Recommendation 6 and targeted financial sanctions in relation to proliferation financing under Recommendation 7. The above obligations of the UN and FATF are enshrined in the UNSA 2019.

Procedure actions:

A) Before the Company enters into a business relationship with a potential Client or enters into an agreement with a counterparty or service provider, it performs due diligence of that Client/counterparty/service provider, including a World-Check search via KYC Provider.

This way, the Company will detect any relevant finding for that the potential Client/counterparty/service provider.

B) The AMLRO will examine the findings, if necessary, liaise with external consultants and/or lawyers and inform accordingly the senior management of these findings.

C) If despite any such finding, the Company intends to proceed with any transaction or relationship that falls within the scope of the Sanctions and/or Restrictive Measures that may be adopted, the Company will, through the AMLRO, submit a request to the competent authority of Mauritius.

The AMLRO will maintain a file of all the actions followed in such cases. That file will include all written and electronic communication in respect to the act in question, including any communication with the relevant authorities, decisions taken, and any other important information on the matter.

If a member of staff is suspicious that financial sanctions are being contravened, or that a Client, counterparty or any other third party is a designated person or entity on an official sanctions list, this must be escalated to the AMLRO immediately. Following escalation, after assessing all available information, if AMLRO is unable to determine whether a customer or third party is indeed one and the same as a listed person/entity they should seek guidance from the supervisory authority.

Sanction Match

Any potential match identified through our screening process must be properly investigated before the Company can take any further steps.

Any employee is responsible for reporting any potential matches immediately to the AMLRO. The AMLRO will investigate whether there is an actual match.

The opening or the maintenance of accounts or the execution of transactions related to close family members or close associates or related entities (irrespective of % age of ownership (directly or indirectly) of parties subject to specific EU, U.S., UK and U.N sanctions, **is strictly prohibited**.

The execution of transactions with any of parties subject to specific EU, U.S., UK and U.N sanctions and related entities with ownership (directly or indirectly) equal or over 50%, **is strictly prohibited**.

Enhanced due diligence must be applied on all customers who are connected with countries that have sanctions imposed on them. Their activities must be comprehended fully to enable the correct assessment and treatment of their transactions.

For entities that are subject to sectorial sanctions, the following should apply: No transactions involving these affected entities in the specific sectors are allowed. In case of acceptance such a client, the approval from AMLCO and Director is required, the close monitoring should be in place, the client should be categorized as High Risk. Under OFAC's '50 percent rule', any entity that is owned 50 percent or more by one or more parties under Sectoral Sanctions, must be treated as though it itself is under Sectoral Sanctions.

3.9 PEP

A. INTRODUCTION

PEPs are individuals who are or have been entrusted with prominent public functions, for example Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories (FATF definition of PEPs). PEP status itself does not, of course, incriminate individuals or entities. It may, however, put a customer into a higher risk category.

In relation to a foreign PEP, whether as customer or beneficial owner, in addition to performing the standard CDD measures, the business unit shall:

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

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

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

(d) conduct enhanced ongoing monitoring on that relationship.

In relation to domestic PEPs or an international organization PEP, in addition to performing the CDD measures required under these regulations —

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

(b) in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP, adopt the measures in paragraphs (l)(b) to (d).

The relevant requirements of the above paragraphs shall apply to family members or close associates of all types of PEP.

Regulation 15(5) of the FIAMLR 2018 defines the terms “close associates” and “family members” as follows:

“close associates”

a. means an individual who is closely connected to a PEP, either socially or professionally; and

b. includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee

“family members”

a. means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and

b. includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee

B. Implementation of normal CDD measures[13]

For foreign and domestic/international organisation PEPs, the Company shall implement effective CDD measures in line with FIAMLR 2018. Reg 15 imposes additional requirements for PEPs which are summarised below.

C. Enhanced measures

For foreign PEPs: Reg 15(1)(a) of FIAMLR 2018 requires appropriate risk management systems to determine whether the customer or beneficial owner is a foreign PEP. This means that proactive steps must be taken, such as assessing customers on the basis of the risk criteria, risk profiles, the business model, verification of CDD information and the business unit’s own research, to determine whether a customer or a beneficial owner is a foreign PEP.

For domestic/international organization PEPs: Reg 15(2) of FIAMLR 2018 requires taking reasonable measures, based on the assessment of the level of risk, to determine whether the customer or beneficial owner is a domestic PEP/international organization PEP. This means reviewing according to relevant risk factors, CDD data collected in order to determine whether a customer or beneficial owner is a domestic/international organization PEP. The Company will determine the risk of the business relationship and in low risk cases, no further steps will be required.

D. Risk Mitigation Measures

For Foreign PEPs: Apply the enhanced risk mitigation measures of Reg 15 (1)(b) to (d) in all cases

For domestic/international organization PEP: In cases of a higher risk business relationship with the PEP apply the enhanced risk mitigation measures of Reg 15 (1)(b) to (d).

The Company’s PEP identification process will be supported by a KYC Provider Screening and Media Check.

Once the client onboarding team identifies a PEP, the relevant officer will notify CO and will update the Customer Risk Assessment accordingly supported by relevant enhanced due diligence. The officer shall mandatorily gather information about the individual PEP’s business or status and their source of funds and wealth.

Prior to proceeding with onboarding, the officer shall seek for approval of senior management in writing (Including email approval).

[13] Reg 3-10 of FIAMLR 2018

In the event that the Company is unable to perform the required EDD, the latter shall terminate the business relationship and file a STR under section 14 of the FIAMLA.

Records of any risk mitigation control and measures will be documented and maintained.

E. Ongoing Monitoring of PEP

Once a business relationship has been established with a PEP, on-going monitoring must be conducted on all related transactions to ensure that they are in line with the customer's source of funds and wealth and original account mandate. This can be achieved by requesting for additional information to understand the purpose of a transaction and verifying the provenance of the source of funds and where required, to request for evidentiary documents such as agreements, invoices, bank statements, etc.

Furthermore, quarterly KYC Provider Check and Internet Check must be conducted on the PEP and evidences of such screening kept on records.

Annual CDD reviews must be conducted on all customers identified as PEPs and approved by Board / Senior Management.

The following information and documentation must be reviewed/reconfirmed/updated when conducting an annual review of a PEP investor:

- all KYC information;
- the relevance of the EDD conducted initially including reconfirmation of the customer's source of funds and source of wealth; and
- where adverse information such as ongoing litigation or regulatory proceedings were noted as part of the on-boarding information, further checks must be undertaken to ascertain any outcomes or obtain updated information.

Information obtained from the customer may be compared against additional independent sources in order to verify the accuracy of the information. The formal decision and reasons to either maintain or terminate the PEP relationship must be documented.

F. Factors to consider in establishing/maintaining/terminating a customer relationship with a PEP

The following are factors, which should be considered in deciding whether to establish/ maintain/terminate a customer relationship with a PEP:

- funding of the account: are the funds/proceeds in the Company's account in line with the customer's source of funds and wealth and original account mandate;
- is there a history of suspicious or unexplained transactions;
- is the customer responsive to requests for up to date information.

There should be a detailed consideration of the rationale for establishing, maintaining, or terminating the business relationship with the PEP.

[Note – where a customer has been accepted and the said customer or its beneficial owner or its associate or its family member is subsequently found to be, or subsequently becomes a PEP, appropriate EDD and Company Board's approval should be obtained as per above in order to continue such business relationships.]

G. Connected persons that are PEPs

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

The Company 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.

The Company 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.

3.10 Adverse Media - Determining the level of significance of information

The following should be considered when determining the level of significance of any information identified as a result of adverse media searches:

- Date of occurrence: The date of occurrence should be considered as the most recent date associated with the event/activity, as opposed to the first time it was reported. E.g., where the adverse media relates to alleged events, the date of the latest investigation or allegation should be used; where an offence has been confirmed, the date of conviction should be used. Although the length of time since an event occurred may not ultimately alter its significance, more recent events should be treated with additional caution, particularly in the case of alleged events as there may be less information available to validate the legitimacy of the event.

- Note: 'recent' means between 12 months to 5 years depending on the nature, severity and penalty of the alleged/confirmed offence.

- The nature of the allegation/fact: The full nature of the allegation, including any criminal or civil indictments should be recorded. It should be noted whether the allegation relates to money laundering or terrorist financing or potentially could result in money laundering or terrorist financing.

- Whether the information is allegation or fact: Consider whether the information identified is alleged, e.g. rumours, arrests but no charges brought, or whether actual involvement has been confirmed, e.g. through convictions or fines.

- Reliability of the source of the information: Identify and record each source consulted for information obtained.

3.11 Documentation of adverse media

In respect of the above, the Company shall 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.

3.12 Verification of source of funds and source of wealth

The source of funds and source of wealth are required to be verified to demonstrate a thorough understanding of the source of the initial and ongoing funds and wealth that will pass through the customer's account/product held at the Company. Where initial funding is provided by third parties, the Company should ensure that the relationship between the parties is fully documented and a rationale for such a relationship is recorded and analysed. If there is no proven rationale for the existence of such a relationship, further due diligence must be conducted and if required, escalated to Compliance for further investigation.

The source of funds and source of wealth of the PEP must be verified in accordance with the source of funds and source of wealth requirements applicable to that PEP.

3.13 Customer Risk Profiling

The Company must identify and assess its potential exposure to inherent ML, TF and sanctions risks introduced as a result of entering into a business relationship with a customer. The Company assesses business relationship risks through a Customer Risk Profiling Toolkit.

The Company will take a number of factors into consideration including but not limited to the following:

- Nature and type of Customer;

- Geographical location of the customer;

- Customer's source and destination of funds;

- Customer's Activity and Transaction Frequency;

- Product type

- Automatic risk adjustment to 'High' based on High Risk Indicators such as: a) Incomplete CDD, b) Dealing with PEP, c) Dealing with Sanctioned countries, d) Unsupported bank transactions, e) World Check Hit or any adverse info from media or internet, f) Reliance on Third Parties (not meeting requirements of FIAMLR 2018).

Risk profiling is applicable to:

- New Customers (at on-boarding stage); and

- Existing Customers.

The following Risk Profiling Classification & Review Date:

• High risk	• every year (12 months)
• Medium risk	• Every 2 years (24 months)
• Low risk	• every 3 years (36 months)

The Company is required to review its customer risk profiling methodology to ensure the customer risk categories remain relevant and reflective of the real risk that the Company is exposed to as a result of its

customer relationships. Frequency to review the methodology shall be annual.

3.14 Ongoing customer maintenance

On-going monitoring is essential to ensure that the ML, TF and sanctions risk profile of customers remain current.

Periodic reviews of customers shall be conducted to monitor business relationships on an on-going basis so that risk of money laundering and / or terrorist financing can be identified and mitigated.

This will include review of CDD documents on a risk-based approach to ensure that up-to-date information is held in relation to business relationships. Any deficiencies noted will be reported to the Board of the Company with appropriate recommendations in compliance with the laws of Mauritius.

As a general guideline, the ongoing review of the customer relationship shall be conducted within the specified time frames according to the customer's risk profile which is as follows:

• High risk	• every year (12 months)
• Medium risk	• Every 2 years (24 months)
• Low risk	• every 3 years (36 months)

3.15 Transaction Monitoring

The Company shall monitor its business relations with customers on an ongoing basis and observe the conduct of customers' activities and transactions to ensure that same are consistent with its knowledge of the customer, its business and risk profile and where appropriate, the source of funds.

The ongoing monitoring of customers' activities and transactions is a fundamental aspect of effective ongoing CDD measures in the identification and mitigation of money laundering and terrorist financing risks.

Transaction Monitoring is a process put in place to monitor all transactions and activity of the Company on an ongoing basis, which involves a combination of real-time and post-event monitoring. In the case of real time monitoring, the focus is on transactions/activity where information/instructions are received before a payment instruction is processed. Post-event monitoring consists of reviewing transactions/activity on a periodic basis (e.g. monthly).

The over-riding principle is to ensure that unusual transactions and activity are identified and subject to a heightened level of scrutiny or examination within the shortest delay and properly documented.

Where the risks of money laundering or terrorism financing are higher, enhanced CDD measures must be conducted which are consistent with the risks identified. Of note, Transaction Monitoring can trigger an Internal Investigation and warrant a STR report, in case a suspicious transaction is identified.

The CO will conduct sample checks on the transaction monitoring process.

3.16 Enterprise Level AML/CFT Risk Assessment

An enterprise level AML/CFT risk assessment is an analysis of potential threats and vulnerabilities to money laundering and terrorist financing to which the Company's business is exposed to.

Risk management requires a systematic approach; it is a cyclical process. The Company is expected to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at regular intervals, because risks are not static. Risks to the Company may change as a result of both internal and external factors.

Since the risks of AML/CFT vary from business to business and are not static, it is the responsibility of the Company 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. While the responsibility for the quality and execution of the risk analyses lies with the first line of defence, **t**he ultimate responsibility for the Enterprise Level AML/CFT Risk Assessment lies with the Board of directors. The role of Compliance is process monitoring, facilitating and testing.

The Company shall conduct the risk assessment in line with Section 17 (2) of the FIAMLA 2002 which mandates that it takes into account:

(a) all relevant risk factors including –

(i) the nature, scale and complexity of the reporting person's activities;
(ii) the products and services provided by the reporting person;
(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.

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

The risk factors under Section 3.18 (a) above are non-exhaustive list and it is for the Company 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 Company has to demonstrate how effective and robust its business risk assessment is in line with its inherent risks and vulnerabilities and the FSC will assess to what extent the business risk assessment conducted reflect residual risks faced by the Company.

The assessment must be undertaken as soon as reasonably practicable after a 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.

AML and TF Risk Assessment Framework has been designed pursuant to FIAMLA 2002 and in line with the FSC Handbook which provides the methodology to conduct the risk assessment exercise and will help in:

(i) identifying the inherent risks;
(ii) evaluating the risk control programs; and
(iii) assessing the residual risks.

The Company shall document the risk assessments in writing, keep it up to date and, on request, make it available to relevant competent authorities without delay.

4. Suspicious Transaction Reporting

4.1 Recognition of Suspicious Transactions

Section 2 of the FIAMLA 2002 defines a suspicious transaction 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, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of 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."

The word "transaction" is also defined in section 2 of FIAMLA 2002, as follows –

""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 attempted transaction."

This definition is not exhaustive.

The assessment of suspicion should be based on a reasonable evaluation of different factors, including the knowledge of the Customer's business, financial history, unusual pattern of activity, risk profile, background and behaviour. All circumstances surrounding a transaction should be reviewed. It follows that an important precondition for recognition of a suspicious transaction or activity is that the employees of the Company must know enough about the business relationship to recognise that a transaction or activity is unusual.

In case of suspicion, an employee is not expected to know the exact nature of the underlying criminal offence (called the predicate offence), or that the particular funds were those arising out of the crime or being used to finance international terrorism. The simple rule is, where a transaction raises any suspicion, the employee should as a first step request more information from the customer about the circumstances surrounding the transaction. He must decide if the explanation received is reasonable and legitimate and if not, report the transaction to the MLRO.

4.2 Internal Reporting of Suspicious Transactions

It is a statutory obligation on all employees to report suspicious transactions promptly and directly to the MLRO or to his deputy in his absence. This should normally be done via an Internal STR Form ("ISF") as per ***Annexure 7***.

In urgent circumstances, an internal STR may be reported to the MLRO verbally and followed by the ISF. Failure to report suspicious transactions will constitute a breach of the FIAMLA 2002 and may entail criminal sanctions and interference with the preparation or submission of an internal STR may lead to disciplinary sanctions.

The MLRO shall be of sufficiently senior status and shall have relevant and necessary competence, authority and independence.

The contact details of the MLRO and those of the Deputy MLRO are provided below:

	MLRO	**Deputy MLRO**
Name	Uttra D. Boodan	Meetish Ramdeehul
Email	uttra.boodan@allserv.mu	meetish.ramdeehul@allserv.mu
Telephone	+230 5771 4060	+230 57327095

All suspicions reported to the MLRO will be recorded in writing, even if the suspicion is reported verbally. The internal STR should include full details of the Customer and a full statement as to the information giving rise to the suspicion. The MLRO will acknowledge receipt of the internal STR and, at the same time, provide a reminder of the obligation to do nothing that might prejudice enquiries – that is, ***'tipping off'*** the customer or any other person which is a criminal offence under Section 16 of the FIAMLA 2002 and upon conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment not exceeding 10 years.

Section 3(3) of FIAMLR 2018 stipulates that "Where a person suspects money laundering, terrorism financing or proliferation financing, and he reasonably believes that performing the CDD process, may tip-off the customer, he shall not pursue the CDD process and shall file a suspicious transaction report under section 14 of the Act".

Where an internal STR has been made, the MLRO shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing. The MLRO will validate all internal STRs before submissions to the FIU and make sure that reports are not made in bad faith, maliciously and without reasonable grounds.

4.3 Reporting of Suspicious Transactions to the FIU

Once the MLRO receives an ISF from the relevant staff member, he/she will determine whether the information contained in the internal STR gives rise to a suspicion that a Customer is engaged in ML, TF, or proliferation financing. In this respect, the MLRO shall have unfettered access to any or all information which he may need in considering his report. In making his/her judgment, the MLRO will consider all relevant information that has been made available to him. Regulation 29. (1) of the FIAMLR 2018 provides that, *'subject to regulation 26(3), where an internal disclosure has been made, the MLRO shall assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.'*

If, after completing the review he/she believes that there is (are) no fact(s) which can negate the suspicion, he/she has the obligation to report the transaction to the FIU through the latter's online platform, GoAML. If, on the other hand, the MLRO does not find it appropriate to report a transaction to the FIU, he/she will document the reasons for not doing so. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future dates, there is an investigation, and the suspicions are confirmed. On-going communication between the MLRO and the reporting staff is important.

The MLRO is expected to act autonomously, promptly, honestly and reasonably, and to make any determination in good faith.

4.4 Reporting Obligations and Offences

Section 14(1) of the FIAMLA provides that "Notwithstanding section 300 of the Criminal Code and any other enactment, every reporting person or auditor shall, as soon as he becomes aware of a suspicious transaction, make a report to FIU of such transaction not later than 5 working days after the suspicion arose."

Pursuant to section 14(3) of the FIAMLA -

"Where a reporting person or an auditor –

(a) becomes aware of a suspicious transaction; or

(b) ought reasonably to have become aware of a suspicious transaction,

and he fails to make a report to FIU of such transaction not later than 5 working days after the suspicion arose he 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."

For further information, please refer to the summary of offences annexed to this document.

4.5 Registers of Internal and External Disclosures

The Company must establish and maintain separate registers of –

(a) all internal disclosures; and

(b) all external disclosures.

The registers of internal disclosures and external disclosures may be contained in a single document if the details required to be included in those registers can be presented separately for internal disclosures and external disclosures upon request by a competent authority.

The registers must include details of:

(a) the date on which the report is made;

(b) the person who makes the report;

(c) for internal disclosures, whether it is made to the Money Laundering Reporting Officer or Deputy Money Laundering Reporting Officer; and

(d) information sufficient to identify the relevant papers.

4.6 Reporting under the FCC Act 2023

In alignment with section 56 of the FCC Act 2023, notwithstanding any other enactment, where in the discharge of his/her functions, any person[14] has reasonable grounds to suspect that an offence under the FCC Act has been, is being or is likely to be committed, he/she shall refer the matter to the Commission for investigation.

Further to provisions of section 113 of the FCC Act, notwithstanding any other enactment, where in the discharge of his/her functions, any person[15] has reasonable grounds to suspect that a person[16] has acquired unexplained wealth, he/she shall make a written report of the matter to the Commission.

[14] Person is defined as a natural or legal person under the FCC Act 2023.

[15] Person is defined as a natural or legal person under the FCC Act 2023.

[16] Person is defined as a natural or legal person under the FCC Act 2023.

5. Training

The Board and all relevant employees of the Company shall receive regular mandatory training to enable them to comply with the:

- provisions of the relevant legislations;
- any internal rules applicable to them, and
- AML/CFT Risk Framework.

Company employees are required to be appropriately trained for purposes of AML, CFT and sanctions in accordance with the degree of their engagement in relation to ML, TF and Sanctions risk.

The training shall cover the following:

(i) Money laundering & Terrorist Financing

(ii) Risk Based Approach to AML/CFT

(iii) Mauritius AML/CFT Legislative Framework

(iv) Regulatory Stance in the event of non-compliance to AML/CFT Laws

(v) Sanctions

(vi) Responsibilities of Board of Directors

(vii) AML/CFT Business Risk Assessment

(viii) Suspicious Transactions Reporting Obligations.

New employees would receive an introductory training on AML/CFT prior to them becoming actively involved in day-to-day operations and in any event before they engage into the provisions of financial services to Customers.

Refresher training for all relevant staff shall be provided at least on an annual basis. An effective training will develop an adequate internal compliance culture which is aimed at bringing down any cultural differences in the attitudes of its staff towards the ML and TF problem.

The Company must maintain records of all AML/CFT training delivered to employees.

A training log will be maintained by the Company.

6. Record Keeping

Record keeping obligations are applicable to CDD, transactional and other information required to manage ML, TF, proliferation and sanctions related risks in relation to the customers/officers/service providers.

Such records shall include details about the flow of customer's funds, customer statements and customers' identification and verification data and or documents.

The company stores all client documents (passports, utility cards, etc.) obtained during onboarding and subsequent work with clients.

Furthermore, the Company must keep records of:

- All reports made to and by the MLRO/Deputy MLRO/CO;
- All training provided in relation to AML and CFT.

Records should be sufficient to provide adequate evidence to the relevant local authorities to conduct their investigations.

Period for which records must be kept

The Company must keep all the records which relate to:

- the establishment of a business relationship, for at least seven years from the date on which the

  business relationship is terminated;

- a transaction which is concluded, for at least 7 years from the date on which that transaction is concluded; and

- reports made by and to the MLRO/CO, for at least 7 years from the date on which the report is made.

Transactional records and or documents are kept at either the Company's and or Company Administrator's registered office.

In line with regulation 14 (3) of the FIAMLR 2018, the Company shall ensure that all CDD information and transaction records are kept in such a manner that they are swiftly made available to the FIU or any relevant regulatory body or supervisory authority upon request. The Company's records shall be maintained in soft copy version which will automatically be recorded on the Company Administrator's Server. Relevant original documentation will be kept in hard copy on the physical Company files which will be archived as per data protection laws and retrieved as and when required.

7. Independent Audit

Regulation 22(1) (d) of the FIAMLR 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 2002 and FIAMLR 2018.

An AML/CFT independent audit is a vital element of any effective compliance programme for financial institutions. By virtue of the FIAMLA 2002 and FIAMLR 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.

Scope of independent audit

In line with international best practices, the independent audit exercise should be risk-based. Independent audit is the Company's final line of defence, therefore, it is vital to ensure that the AML/CFT independent audit is tailored to the Company'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);
- CO 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 Sanctions; and
- Suspicious Transaction Monitoring and Reporting.

If the Company 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.

Frequency of the Independent Audit

The frequency and extent of the review should be commensurate with the Company'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 Company can determine for itself the frequency to have its audits conducted. The greater the AML risk of the Company, and of the rate of change of the Company's business, the greater should be the frequency of audit.

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

For a Company that is in process of being wound up, it is recommended that at least one final independent audit is carried out until the Company is no more considered as a reporting entity under the FIAMLA 2002.

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

8. DUTIES AND OBLIGATIONS SUMMARY

A. Director Duties

Key responsibilities of the Directors of the Company shall be to:

- Develop a strategic plan to advance the Company's mission and objectives and to promote revenue, profitability, and growth as an organization.
- Review activity reports and financial statements to determine progress and status in attaining objectives and revise objectives and plans in accordance with current conditions.
- Oversee foreign operations to include evaluating operating and financial performance.
- Promote the Company to local, regional, national, and international constituencies.
- Evaluate performance of executives for compliance with established policies and objectives of the company and contributions in attaining objectives.
- Oversee Company operations to insure production efficiency, quality, service, and cost-effective management of resources.
- Troubleshooting trading related issues.
- Assert appropriate trade execution at Liquidity Provider.

General Director duties under Mauritian Law

Any director of the Company must as from the date of his appointment:

- Comply with certain duties and obligations as set out under the Companies Act 2001 of Mauritius (the "**Act**").
- These duties and obligations will apply in the same way to 'alternate directors'.

B. Duties and Responsibilities of the 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.

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

- Ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board and Senior Management;
- Undertaking day-to-day oversight of the programme for combatting money laundering and terrorism financing;
- Regular reporting, including reporting of non-compliance, to the Board and Senior Management on an annual basis or at shorter intervals whenever required.
- Contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

The Compliance Officer also ensures that:

- The Investment Dealer has an adequate system to comply with relevant laws, Guidelines, etc.;
- An appropriate system exists to monitor operational performances and make recommendations to rectify any deficiencies;
- He / she acts as the principal point of contact with the regulators.

The Compliance Officer is responsible for developing, maintaining and implementing plans in relation to compliance, which shall comprise of the following:

- Identifying key controls and inclusion in the Manual
- Designing checklists for monitoring compliance
- Conducting compliance checks
- Making appropriate recommendations where improvements are necessary
- Reporting findings to the Board, as may be required
- Organizing training sessions on compliance
- Updating the Board on new laws and regulations
- Monitoring the risk rating of each client
- Updating the manual for consideration and approval by the Board of Directors

The Compliance Officer must carry out compliance reviews to ensure that procedures and controls set out in the Manual are completed at all times. This should help ensure that the Investment Dealer operates within the parameters of the guidelines, codes and other regulations set out by the regulators.

While it is not anticipated that the Compliance Officer will personally conduct all monitoring and testing, the expectation is that he / she will have oversight of any monitoring and testing being conducted by the Company.
The circumstances of the Company may be such that, due to the small number of employees, the CO holds additional functions or is responsible for other aspects of the Company's operations. Where this is the case, the Company 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 Company 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.

The Compliance Officer must report to the Board of Directors of his / her findings arising from the compliance reviews.

When a breach or potential breach is identified, the Compliance Officer shall forthwith notify the Board for needful action.

C. Duties and Responsibilities of the MLRO and DMLRO

Adequate procedures should be implemented by Licensees to ensure that their MLRO has timely access to customer identification data and other CDD information, transaction records, and other relevant information in order to properly evaluate internal suspicious transaction reports.

MLROs must be autonomous in their decisions as to whether a suspicious transaction report should be made to the FIU.

MLROs may consult with colleagues as part of the evaluation process. However, the MLRO must be free to make his or her decision and without undue influence, pressure or fear of repercussions in the event that senior colleagues disagree with his/her decision. Where a MLRO validates an internal report about a transaction that has aroused suspicion, he/she has a legal obligation to make a report to the FIU.

The MLRO and Deputy MLRO in the absence of the MLRO:

- is the main point of contact with the Financial Intelligence Unit ("FIU") in the handling of disclosures;
- has unrestricted access to the CDD information of the Company's customers, including the beneficial owners thereof;
- has sufficient resources to perform his or her duties;
- is available on a day-to-day basis;
- reports directly to, and may have regular contact with the Board; and
- is fully aware of both his personal obligations and those of the Investment Dealer under FIAMLA and FIAML Regulations 2018, the FSC Handbook and this Compliance Procedures Manual.

Additionally, the MLRO is responsible for developing, maintaining and implementing plans in relation to money laundering and terrorist financing deterrence procedures, which shall comprise of the following:

- Designing appropriate system for the management of money laundering and terrorist financing risks;
- Providing advice and organizing training sessions on anti-money laundering and prevention of terrorist financing;
- Acting as the central point of contact for receipt of Money Laundering Suspicious Reports made by staff and subsequent validation, reporting and liaison with the FIU;
- Keeping records on money laundering and terrorist financing suspicion and advise the Company on necessary course of action concerning client relationship when filing a suspicious transaction report;
- Monitoring the risk rating of each client;
- Where necessary, updating the Manual with regards to money laundering and terrorist financing matters for consideration by the Board of Directors;

- Reporting of all money-laundering and terrorist financing issues to the Board on a annual basis, or at shorter interval, if required;
- 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;
- Maintaining all related records;
- Providing guidance on how to avoid tipping off the customer if any disclosure is made; and

- Liaising with the FIU, and if required with the FSC, and participating in any other third-party enquiries in relation to money laundering or terrorist financing prevention, detection, investigation or compliance.

9. Risk Classification Guide

μ: High-Risk Jurisdiction

To assess whether a jurisdiction is a High-Risk jurisdiction, due consideration shall be given to:

- FATF High-risk and other monitored jurisdictions
- European Commission AML/CFT List of High Risk Third Countries
- European Commission's list of non-cooperative jurisdictions for tax purposes
- Transparency International's Annual Corruption Perceptions Index
- OECD Global Forum on Tax Transparency and Exchange of Information for Tax Purposes Ratings
- Office of Foreign Affairs Control (OFAC) Countries List
- Basel AML Index
- Corruption Perception Index
- Global Peace Index
- Global Terrorism Index
- Financial Secrecy Index
- Run through "Know Your Country" FATF AML Deficiency List & Use "Google Boolean"

Business Activity Classification:

a) List of activities classified as High Risk:

1. Extractive Industries: Entities that deal in the extraction of natural resources, such as oil, minerals, gas and timber.
2. Government/Public Procurement Activities
3. Defence Industry: Contracting Work of highly specialised goods, systems and services.
4. Human Health Activities: Provision of health services, pharmaceutical products, and medical devices, including research, development, dispensing and promotion of same.
5. Large Infrastructure Projects: Contracting work for construction, continuing maintenance and upkeep.
6. Privatisation: Buying or obtaining from government something of large economic value through the process of privatisation.
7. Activities related to so-called "windfall revenue" including significant amounts of foreign aid.
8. FX Trading
9. Jewels, gems and precious metal dealers
10. Real estate agents
11. Cash Pooling Structures
12. Virtual currency trading (e.g. bitcoins)
13. Dealing in cultural objects like in sculpture, statues, antiques, collector items, archaeological pieces
14. NGO's and NPO (Non-profit organization)
15. Online trading/online marketing and E-commerce
16. Activities in gambling sector and casinos

17. Money Service provider
18. Trust and Company service Provider

b) List of activities classified as Medium Risk:

1. Legal Professions (including Law firms/ Barristers, Notaries, attorneys)
2. Accountancy sector (including Accounting firm and Auditors)
3. Trust and Company service Provider
4. Consultancy
5. Trading (e.g. Import and Export)
6. Life Insurance Sector
7. Banking Sector
8. Financial Institutions regulated by the FSC
9. Non-financial Entities regulated by the FSC
10. Financial Institutions regulated by BOM
11. Credit Union
12. Securities sector

c) List of activities classified as Low Risk:

1. Public Listed Companies on stock exchange
2. International Organisation (e.g. United Nation)
3. Government administrations or enterprises and statutory bodies

NRA Report 2019 : http://financialservices.govmu.org/English/Documents/2019/NRA%20Report/Public%20Report%202019-compressed.pdf

10. Due Diligence Documents Guide

List A - Individual

Information to be verified[17]:

(1) For a customer who is a natural person, the Company being a reporting person[18] shall obtain and verify –
(a) the full name, including, marital name, former legal name or alias;
(b) the date and place of birth;
(c) the nationality;
(d) the current and permanent address; and
(e) such other information as may be specified by a relevant supervisory authority or regulatory body.

(2) For the purposes of paragraph (1), documentary evidence as may be specified by a relevant regulatory body or supervisory authority shall be used for the purposes of verification of identity requirement.

	Documents required	
1)	**Verification of identity[19]:**	Certified true copy[20] of **either of the following:** ✓ a national identity card (make sure to seek recto verso where applicable); ✓ a current valid passport (make sure to see the MRZ, the clear picture, assess duration if aligned with country of issuance); or ✓ a current valid driving licence[21]. *From a risk based approach, the Company may opt to seek for multiple identification documents, on a case to case basis.
2)	**Verification of current and permanent residential address[22]:**	Original or certified true copy of either a: ✓ recent[23] utility bill (gas, water, electricity or landline telephone) – not more than 3 months old; or ✓ recent bank or credit card statement - not more than 3 months old; or (i) recent reference or letter of introduction from a financial institution that is regulated in Mauritius - not more than 3 months old; (ii) a regulated financial services business which is operating in a jurisdiction that complies with the FATF standards- not more than 3 months old; 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 - not more than 3 months old.

[17] Regulation 4 of the FIAML Regulations 2018 and Section 5.3 of the FSC's AML and CFT Handbook.

[18] As per Section 2 of FIAMLA, a reporting person means a bank, financial institution, cash dealer or member of a relevant profession or occupation which also includes the Company.

[19] **Where the legal person with which the natural person is associated 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.**

[20] The term 'certified true copy" implies that the document must be appropriately certified as a true copy of the original document either by a lawyer, notary, actuary, accountant or any other person holding a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius, a member of the judiciary or a senior civil servant.
The certifier should clearly state his/her name, date of certification, address and position/capacity on it together with contact details to aid tracing of the certifier.

[21] Where the Company is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence.

[22] If the current and permanent address differ, the client needs to provide a separate utility bill for each address. PO Box addresses are not acceptable.

[23] 'Recent' means issued within the last 3 months.

3)	**Fit and proper requirement (for Individuals, Principals of companies, BOs, UBOs, Shareholders, Directors)**	✓ Curriculum Vitae
4)	**Source of funds**	✓ Part of the Client (Account Opening) Questionnaire
5)	**Evidence of source of funds**	Original or certified true copy of: Example: Bank Statement, Salary Slip, Dividend Notice, etc…
6)	**For EDD purposes or other purposes:**	Original or certified true copy of either a: ✓ Bank Reference (not more than 6 months old) Should include: The date of account opening, satisfactory operations, address, full name, name of signatory and position, letterhead of bank, date of document. ✓ Professional Reference (not more than 6 months old) Should include: the date of start of professional relationship, nature of professional relationship, address, full name, name of professional, title and registration number of the professional, date of document, letterhead. ✓ Certificate of Character/ Police Clearance Certificate
7)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Director/Shareholder/BO/UBO): To be disclosed in Declaration Form (Appendix 13)
8)	**For 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
10)	**World Check screening reports (via KYC Provider)**	✓ Internal
11)	**Internet Check reports**	✓ Internal

Where a particular aspect of an individual's identity changes (such as change of name, nationality, or any other forms as approved), the Company shall 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. [For example, by using a newly issued replacement for the expired document.]

List B - Company

Information to be verified[24]:
Where the customer is a legal person or legal arrangement, a reporting person shall –
(a) with respect to the customer, understand and document –
(i) the nature of his business; and
(ii) his ownership and control structure;

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

[24] Regulation 5 and 6 of the FIAML Regulations 2018 and Section 5.4 and 5.5 of the FSC's AML and CFT Handbook

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

	Documents required	
1)	**Verification of existence:**	✓ Original or certified true copy of the Certificate of Incorporation or Certificate of Registration as applicable; and ✓ Extract of Companies Register (or equivalent); ✓ Details of the registered office address and principal place of business; ✓ Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; ✓ Personal visit to principal place of business.
2)	**Identification and verification of identity of underlying Principals[25]:**	✓ Original or certified true copy of the register of directors; ✓ Original or certified true copy of the register of shareholders/members; ✓ Certified true copy of identity and address verification documents as listed in List A above for the directors and authorized signatories; and ✓ Original or certified true copy of CDD documents[26] on the natural persons who ultimately have a controlling ownership interest in the company as per Lists A, B, C, D, E or F (as applicable)
3)	**Identification and verification of senior managing official[27] of the Company:**	✓ Original or certified true copy of CDD documents on the senior managing official.
4)	**Verification with the relevant companies registry that the Company continues to exist:**	✓ Recent Certificate of Good Standing[28;] or ✓ Extract of Companies Register (or equivalent); ✓ Verification on the website of the Registrar of Companies in the jurisdiction where the Company is incorporated; ✓ Any other source of information to verify that the document submitted is genuine.
5)	**Verification of the powers that regulate and bind the Company:**	✓ Certified true copy of the Constitution of the Company; or ✓ Certified true copy of the Memorandum and Article of Association (M&A) of the Company; and ✓ Certified true copy of the licence of the Company, where the latter is a regulated entity.
6)	**Verification of person(s) who purport to act on behalf of the Company is/are so authorized, and identifying the person(s):**	✓ Original Certificate of Authority signed by the director(s) or an extract of the minutes of the board meeting/ resolutions or Power of Attorney (PoA); ✓ Certified true copy of either valid passport, national identity card or driving licence of the authorized person(s); and ✓ Original or certified true copy of recent utility bill of the authorized person(s).

[25] Where the legal person with which the underlying natural person is associated 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.

[26]

Scenario A - The identity of all the natural persons who ultimately have a controlling ownership interest in the legal person.
Scenario B - Where there is doubt as to whether the person with the controlling ownership interest is the beneficial owner.
Scenario C - Where no natural person exerts control through ownership interests, the identity of the natural person exercising effective control of the legal person.
Senior Managing Official: Where no natural person is identified in the following scenarios, the identity of the natural person who holds the position of Senior Managing Official:

[28] Mandatory when there is a change in shareholding for an existing client or a transfer-in from another Management Company

7)	**Financial Statements**	✓ Audited annual financial report (if applicable) for two years; or ✓ Management accounts for two years
8)	**Source of funds**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Shareholder/ UBO): To be disclosed in Declaration Form (Appendix 13)
9)	**Evidence of source of funds**	✓ Copies of:Bank Statement, Dividend Notice, Audited Accounts etc…
10)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Clients: Information disclosed as part of the Client (Account Opening) Questionnaire ✓ Others (Director/Shareholder/UBO)
11)	**World Check screening reports via KYC Provider**	✓ Internal
12)	**Internet Check reports**	✓ Internal

List C – Legal Arrangement / Trust

Information to be verified[29]:
Where the customer is a legal person or legal arrangement, a reporting person shall –
(a) with respect to the customer, understand and document –
(i) the nature of his business; and
(ii) his ownership and control structure;
(b) identify the customer and verify his identity by obtaining the following information –
(i) legal name, legal form and proof of existence;
(ii) powers that regulate and bind the customer;
(iii) names of the relevant persons having a senior management position in the legal person or arrangement;

(iv) names and other information of the all parties of a Trust, including real UBOs;
(v) the address of the registered office and, if different, a principal place of business.

	Documents required	
1)	**Verification that the trust exists and identification of its Principals[30]**	✓ Original or certified true copy of the trust deed; or ✓ Original or certified true copy of the pertinent extracts thereof, containing the name of the trust, name of the settlor, name of the trustees, names of the protectors and enforcers (if any), beneficiaries[31] (if identified) and powers that regulate and bind the trust.
2)	**Identifying and verifying the identity of the Principals**	✓ Certified true copy of CDD documents as listed in List A or List B (as applicable) on the settlor, trustees, protectors, enforcers and the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust including through a chain on control or ownership- refer to Regulation 7 of the FIAMLR 2018
3)	**Identification and verification of senior management official[32]**	✓ Original or certified true copy of CDD documents on the senior managing official

[29] Regulation 5 and 7 of the FIAML Regulations 2018 and and Section 5.6 and 5.7 of the FSC's AML and CFT Handbook

[30] **Where the legal person with which the natural person is associated 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.**

[31] In case of discretionary trusts and/or beneficiaries who are minors, verification of identity of the beneficiaries may be delayed until prior to the making of any distribution to them. An original signed undertaking from the trustees will have to be obtained to this effect.

[32] Senior Managing Official: Where no natural person is identified in the following scenarios, the identity of the natural person who holds the position of Senior Managing Official:

4)	**Verification that the trust is registered (where applicable)**	✓ Certified true copy of Certificate of Registration ✓ Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in the circumstances.
5)	**Details of the registered office and place of business of the trustee**	✓ Letter/Extract of File form Registry
6)	**Source of funds**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Shareholder/BO/UBO): To be disclosed in SoF form
7)	**Evidence of source of funds**	✓ Copies of: Bank Statement, Dividend Notice, Audited Accounts etc…
8)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Director/ UBOs): To be disclosed in Declaration Form (Appendix 13)
9)	**World Check screening reports**	✓ Internal
10)	**Internet Check reports**	✓ Internal

The Company shall seek and obtain assurances from the trustee/s (or controlling individual/s) that all of the data requested under the above process has been provided, and that the individual(s) will notify The Company in the event of any subsequent changes.

List D – Partnership

Information to be verified[33]:
Where the customer is a legal person or legal arrangement, a reporting person shall –
(a) with respect to the customer, understand and document –
(i) the nature of his business; and
(ii) his ownership and control structure;
(b) identify the customer and verify his identity by obtaining the following information –
(i) name, legal form and proof of existence;
(ii) powers that regulate and bind the customer;
(iii) names of the relevant persons having a senior management position in the legal person or arrangement; and
(iv) the address of the registered office and, if different, a principal place of business.

	Documents required	
1)	**Verification of existence, nature of business and powers that regulate and bind the business**	✓ A copy of the partnership deed or Partnership Agreement; and ✓ A certified true copy of the Certificate of Registration (if registered); ✓ Personal visit to principal place of business; ✓ Reputable and satisfactory third party data, such as a business information service; ✓ Any other source of information to verify that the document submitted is genuine.

Scenario A - The identity of all the natural persons who ultimately have a controlling ownership interest in the legal person.
Scenario B - Where there is doubt as to whether the person with the controlling ownership interest is the beneficial owner.
Scenario C - Where no natural person exerts control through ownership interests, the identity of the natural person exercising effective control of the legal person.

[33] Regulation 5 and 6 of the FIAML Regulations 2018 and Section 5.4 and 5.5 of the FSC's AML and CFT Handbook

2)	**Identification and verification of the identity of the Principals**[34]	✓ Certified true copy of CDD documents as listed in Lists A, B, C, D, E or F (as applicable) on the General Partner and the Limited Partners.
3)	**Verification of person(s) who purports to act on behalf of the partnership is/are so authorized and identification of the person(s)**	✓ Original Certificate of Authority signed by the General Partner(s) and proof of identity of the authorized persons as outlined in List A or List B above.
4)	**Identification and verification of senior management official**[35] **of the Partnership**	✓ Original or certified true copy of CDD documents on the senior managing official
5)	**Source of funds**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Shareholder/BO/UBO): To be disclosed in SoF form
6)	**Evidence of source of funds**	✓ Original or certified true copy of: ✓ Example: Bank Statement, Dividend Notice, Audited Accounts etc…
7)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Director/Shareholder/BO/UBO): To be disclosed in Declaration Form (Appendix 13)
8)	**World Check screening reports**	✓ Internal
9)	**Internet Check reports**	✓ Internal

List D – Société

Information to be verified[36]**:**
Where the customer is a legal person or legal arrangement, a reporting person shall –
(a) with respect to the customer, understand and document –
(i) the nature of his business; and
(ii) his ownership and control structure;

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

	Documents required	
1)	**Verification of existence**	✓ Original or certified true copy of an acte de société, including profile of the société; ✓ In the case of Mauritian sociétés, verify with the Registrar of Companies if the société is registered and continues to exist; ✓ In the case of foreign sociétés, obtain a Certificate of Good Standing; ✓ Personal visit to principal place of business; ✓ Reputable and satisfactory third party data, such as a business information service; ✓ Any other source of information to verify that the document submitted is genuine.
2)	**Verification of the identity of the**	✓ Certified true copy of CDD documents as listed in List A, B, C, D, E or F (as applicable).

[34] **Where the legal person with which the natural person is associated 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.**

[35] The senior managing official need to be identified when the natural person who ultimately has controlling ownership interest in the company cannot be identified

[36] Regulation 5 and 6 of the FIAML Regulations 2018 and Section 5.4 and 5.5 of the FSC's AML and CFT Handbook

	Principals[37], administrators or gérants	
3)	**Verification of person(s) who purports to act on behalf of the société is/are so authorized and identification of the person(s)**	✓ Original Certificate of Authority signed by the Administrator(s) or Gérant(s) and proof of identity of the authorized persons as outlined in List A or List B above.
4)	**Identification and verification of senior management officials[38]:**	✓ Original or certified true copy of CDD documents on the senior managing official
5)	**Source of funds**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Shareholder/BO/UBO): To be disclosed in SoF form
6)	**Evidence of source of funds**	✓ Original or certified true copy of: ✓ Example: Bank Statement, Dividend Notice, Audited Accounts etc…
7)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Director/Shareholder/BO/UBO): To be disclosed in Declaration Form (Appendix 13)
8)	**World Check screening reports**	✓ Internal
9)	**Internet Check reports**	✓ Internal

List F – Foundations

Information to be verified[39]:
Where the customer is a legal person or legal arrangement, a reporting person shall –
(a) with respect to the customer, understand and document –
(i) the nature of his business; and
(ii) his ownership and control structure;

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

	Documents required	
(1)	**Verification of existence:**	✓ Certified true copy of legal document establishing the Foundation/Foundation Charter; ✓ Certified true copy of the Certificate of Registration or its extract from the public register (if registered); ✓ Personal visit to principal place of business; ✓ Reputable and satisfactory third-party data, such as a business information service; ✓ Any other source of information to verify that the document submitted is genuine.

[37] **Where the legal person with which the natural person is associated 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.**

[38] The senior managing official need to be identified when the natural person who ultimately has controlling ownership interest in the company cannot be identified

[39] Regulation 5 and 6 of the FIAML Regulations 2018 and Section 5.4 and 5.5 of the FSC's AML and CFT Handbook

(2)	**Identification and verification of identity of the Principals**[40]	✓ Certified true copy of CDD documents as per Lists A, B, C, D, E or F as applicable on the Founder(s), members of the Council and beneficiaries.
(3)	**Identification and verification of senior management official**[41]	✓ Original or certified true copy of CDD documents on the senior managing official
(5)	**Profile**	✓ Copy of the latest report and accounts of the Foundation
(6)	**Source of funds**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Shareholder/BO/UBO): To be disclosed in SoF form
(7)	**Evidence of source of funds**	✓ Original or certified true copy of: ✓ Example: Bank Statement, Dividend Notice, Audited Accounts etc…
(8)	**FATCA and CRS Due Diligence documents including the self-certification forms**	✓ Client: Part of the Client (Account Opening) Questionnaire ✓ Others (Director/Shareholder/BO/UBO): To be disclosed in Declaration Form (Appendix 13)
(9)	**World Check screening reports**	Internal
(10)	**Internet Check reports**	Internal

List G – Reduced or Simplified CDD[42]

Regulated financial services business based in Mauritius or in an equivalent jurisdiction

	Documents required
(1)	Proof of existence of the financial services business
(2)	Proof of regulated status of the financial services business
(3)	FATCA and CRS Due Diligence documents including self-certification forms

The Company needs to be satisfied that the applicant is not acting on behalf of underlying principals.

Public companies listed on Recognised Stock / Investment Exchanges

	Documents required
(1)	Proof of existence
(2)	Proof of listed status
(3)	Latest annual reports and accounts for 2 years
(4)	**Verifying that the person(s) who purport(s) to act on behalf of the public listed company is/are so authorized and identify the person(s):** ▪ Original Certificate of Authority signed by the directors or an extract of the minutes of the board meeting/ resolutions and proof of identity of the authorized persons as outlined in List A
(5)	FATCA and CRS Due Diligence documents including self-certification forms

[40] **Where the legal person with which the natural person is associated 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.**

[41] The senior managing official need to be identified when the natural person who ultimately has controlling ownership interest in the company cannot be identified

[42] Chapter 7 of the FSC's AML and CFT Handbook. The Company's Risk and Compliance Team may be consulted for advice on conducting Reduced or Simplified CDD.

List H – Enhanced Due Diligence (EDD)

The EDD measures applicable are as defined hereunder. The Company reserves the right to request additional information and documentation, including source of wealth, as part of its on-boarding process and prior to accepting the Client.

Individual	1. Bank reference
Individual	2. Verify source of funds and source of wealth
Individual	3. Bank statements for last 6 months
Individual	4. Close monitoring of transactions
Individual	5. Ensure supporting documents for transactions, such as invoices and agreements are obtained
Individual	6. Criminal records checks and internet checks at time of client acceptance process (CAP) and thereafter quarterly
Individual	7. Consider more than one form of verification of ID
Corporate	8. Certificate of Good Standing
Corporate	9. Copy of latest audited financial statements
Corporate	10. Verify source of funds and source of wealth of UBO
Corporate	11. Bank reference on UBO
Corporate	12. Close monitoring of transactions
Corporate	13. Obtain supporting documents for transactions, such as invoices and agreements
Corporate	14. Criminal records checks and internet checks at time of CAP and thereafter quarterly
Trust	15. Bank reference on settlor
Trust	16. CV of settlor
Trust	17. Verify source of funds and source of wealth of settlor
Trust	18. Check regulated status, where applicable
Trust	19. Close monitoring of transactions
Trust	20. Criminal records checks and internet checks on CAP and thereafter quarterly
Partnership	21. CV of general partner/controlling partner
Partnership	22. Bank reference on general partner/controlling partner
Partnership	23. Verify source of funds and source of wealth
Partnership	24. Latest audited accounts
Partnership	25. Close monitoring of transactions
Partnership	26. Criminal records checks and internet checks on CAP and thereafter quarterly
Société	27. Certificate of good standing (for foreign Société)
Société	28. Latest audited accounts
Société	29. CV on Gérants /UBO
Société	30. Close monitoring of transactions
Société	31. Criminal records checks and internet checks on CAP and thereafter quarterly
Société	32. Latest audited accounts
Société	33. Check regulated status
Foundation	34. CV on the founder
Foundation	35. Bank reference on the founder
Foundation	36. Close monitoring of transactions
Foundation	37. Check regulated status
Foundation	38. Criminal records checks and internet checks on CAP and thereafter quarterly

List I – Updated Due Diligence

As part of the ongoing monitoring of clients, the Company shall:

- Monitor the expiry of passports of clients and request for renewed passports as and when necessary, thus ensuring that copies of valid passports, incorporating photographic evidence of identity, are held by the Company at all times.

- Where it becomes aware of a particular aspect of the client's identity has changed (e.g., change of name, nationality, or any other forms as approved), gather relevant updated CDD documents.

- Request clients for updated proof of address under the following risk-based approach, i.e., request frequency shall be based on the risk classification of clients.

Risk level	**Frequency to seek updated Proof of Address**
Low risk	Every Three Years
Medium risk	Every Two Years
High risk	Annually

- The confirmation of the validity of the Address shall be in the form of email.
