BEX Mauritius
Block Exchange

AML Manual

Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation Compliance Manual

Table of Content

Acronyms

BRA	Business Risk Assessment
Company	BEX Mauritius Block Exchange
CDD	Customer Due Diligence
CO	Compliance Officer
CRA	Client Risk Assessment
DMLRO	Deputy Money Laundering Reporting Officer
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIAMLA	Financial Intelligence and Anti Money Laundering Act
FIAMLR 2018	Financial Intelligence and Anti Money Laundering Regulations
FIAMLR 2019	Financial Intelligence and Anti-Money Laundering (Registration of Reporting Persons) Regulations 2019
FIU	Financial Intelligence Unit
FSC	Financial Services Commission
FSC Handbook 2020	The Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020 (last updated in March 2021)
Listed Party	Person or entity designated under the UNSA or listed by or under the authority of the United Nations Security Council
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
NRA	National Money Laundering and Terrorist Financing Risk Assessment of Mauritius
NSC	National Sanctions Committee
NSSec	National Sanctions Secretariat
PF	Proliferation Financing
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UN	United Nations
UNSA	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Act 2019
UNSCR	United Nations Security Council Resolution

1. Introduction

1.1 BEX Mauritius Block Exchange ("the Company") is incorporated in April 2022 as a Global Business Category licence (GBL) under the Laws of Mauritius and a Securities Trading Systems licence with the Financial Services Commission ("FSC") under the Securities Act 2005 (the "Securities Act"). the Company shall therefore be a reporting person for the purposes of the Financial Intelligence and Anti-Money Laundering Act ("FIAMLA") and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ("UNSA") and shall therefore be required to comply with the anti-money laundering and combatting the financing of terrorism and proliferation (AML/CFT) obligations under these enactments. The Company shall register the MLRO and DMLRO in the GO AML platform of the FIU as well as itself as an organization

Money Laundering

1.2 Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully "laundered", the criminal can enjoy these monies without revealing their original source. In Mauritius, the offence of money laundering is criminalised under the FIAMLA.

1.3 It should be noted that for money laundering purposes, proceeds of crime do not only refer to money but includes property[1] of any kind, nature or disposition, whether tangible or intangible and includes-

a) any currency, whether or not the currency is legal tender in Mauritius, and any bill, security, bond, negotiable instrument or any instrument capable of being negotiated which is payable to bearer or endorsed payable to bearer, whether expressed in Mauritius currency or otherwise;
b) any balance held in Mauritius currency or in any other currency in accounts with any bank which carries on business in Mauritius or elsewhere;
c) any balance held in any currency with any bank outside Mauritius;
d) motor vehicles, ships, aircraft, boats, works of art, jewellery, precious metals or any other item of value; and
e) any right or interest in property;

1.4 Section 2 of the FIAMLA describes the term "crime"

(a) as an offence punishable by –

(i) penal servitude;

(ii) imprisonment for a term exceeding 10 days;

(iii) a fine exceeding 5,000 rupees;

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

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

[1] See definition of the term "property" under section 2 of the FIAMLA

1.5 The offence of money laun dering is defined under section 36 of the Financial Crime Commission Act 2023 ("FCCA") as follows -

Section 36 FCCA:

(1) Any person who -
  (a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
  (b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime,

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

(2) A bank, financial institution, cash dealer or member of a relevant profession or occupation that fails to take such measures as are reasonably necessary to ensure that neither it nor any service offered by it, is capable of being used by a person to commit or to facilitate the commission of a money laundering offence or the financing of terrorism shall commit an offence.
(3) In this Act, reference to concealing or disguising property which is, or in whole or in part, directly or indirectly, represents, the proceeds of any crime, shall include concealing or disguising its true nature, source, location, disposition, movement or ownership of or rights with respect to it.

1.6 It is also important to note that:

- A person may be convicted of a money laundering offence notwithstanding the absence of any conviction of another person for any underlying predicate crime – the proceeds of which are allegedly laundered.
- The offences contain an important objective test of suspicion. The test means that it is possible for the offences to be committed in circumstances where a person had reasonable grounds to suspect that property had been derived from crime, even where they did not actually suspect that to be the case.
- The offences can be committed in relation to proposed as well as actual transactions. A separate offence of conspiracy to commit an offence is contained within section 48 of the FCCA.

Three stages of Money Laundering

1.7 Traditionally, the process of Money Laundering occurs in 3 stages which can be seen below. However, it is to be noted that it is not mandatory that the stages occur in the same order or that all of the stages happen.

1.8 The **placement stage**, which is the initial stage, is the introduction of criminally tainted money into the financial system.

1.9 The **layering stage** is the dissociation of the dirty money from their source through a series of transactions to obscure the origins of the proceeds. These transactions may involve different entities such as companies and trusts as well as different financial assets such as shares, securities, properties or insurance products.

1.10 The **integration stage** is the use of the funds in the legitimate economy through for instance, investment in real estate or luxury assets. However, with features like access, anonymity and speed which stem from modern technology, criminals are very creative in developing new techniques to disguise the nature of their illegal proceeds. To have an indication of the current money laundering situation, international organizations like the FATF, the Egmont Group and the IMF publish, in that respect, regular typologies studies describing the techniques, patterns and trends used by launderers.

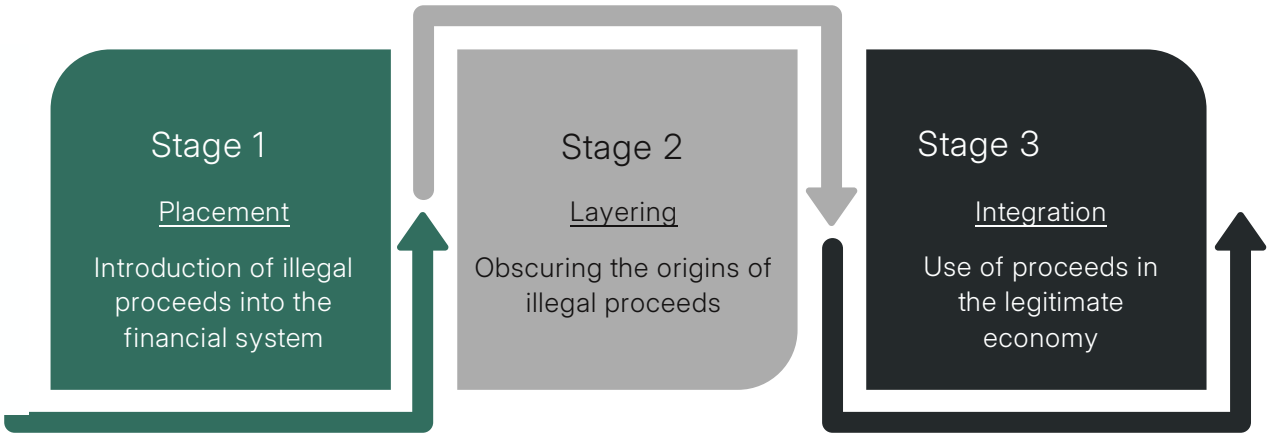


Figure 1. Three stages of money laundering

Terrorism financing

1.11 The financing of terrorism can be defined as the wilful provision or collection of funds, by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used in full or in part, to carry out terrorist acts; by a terrorist organization; or by an individual terrorist. In Mauritius, the offence of terrorist financing is criminalized under section 4 of the Convention for the Suppression of the Financing of Terrorism Act.

Financing of terrorism

(1) Any person who, by any means whatsoever, wilfully, and unlawfully, directly or indirectly, provides or collects funds with the intention or knowledge that it will be used, or having reasonable grounds to believe that they will be used, in full or in part, to commit in Mauritius or abroad –
(a) an offence in breach of an enactment specified in the Third Schedule; or
(b) an act of terrorism, shall commit an offence.

(1A) Any person who, by any means whatsoever, wilfully, and unlawfully, directly or indirectly, provides funds to any individual to travel to a State, other than that individual's State of residence, for the purpose of perpetration, planning, or preparation of, or participation in, terrorist acts or the provision or the receiving of terrorist training, shall commit an offence.

International initiatives to combat money laundering, terrorism financing and proliferation financing

1.12 The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society and the international financial services system.

1.13 The FATF has developed the FATF Recommendations, or FATF Standards, which ensure a coordinated global response to prevent organized crime, corruption, and terrorism. They help authorities go after the money of criminals dealing in illegal drugs, human trafficking, and other crimes.

1.14 The FATF also works to stop funding for weapons of mass destruction, which is commonly referred to proliferation financing (PF). There is no universal definition of term but for the purposes of the FATF, "Proliferation financing" refers to:

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

1.15 In Mauritius, the term "proliferation financing" is defined in relation to a person under Section 2 of the FIAMLA:

> "proliferation financing", in relation to a person, means the person who –
> (a) makes available an asset;
> (b) provides a financial service; or
> (c) conducts a financial transaction; and
> knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended to, in whole or in part, facilitate proliferation regardless of whether the specified activity occurs or is attempted.

1.16 In February 2012, the FATF issued the revised 40 Recommendations which have been endorsed by over 200 jurisdictions across the globe. Mauritius which is a founding member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF Style Regional Body, has also endorsed the FATF Recommendations and remains committed to implementing them.

1.17 In an endeavour to combat money laundering and terrorism financing, Mauritius adopted the FIAMLA in 2002, the Prevention of Terrorism Act 2002 and the Convention for the Suppression of the Financing of Terrorism Act 2003. Since then, several amendments have been brought to these enactments. In September 2018, the Financial Intelligence and Anti-Money Laundering Regulations 2018 (FIAMLR 2018) were issued and the FIAMLR 2003 were revoked. In May 2019, Mauritius adopted the UNSA to provide a legal framework for the implementation of targeted financial sanctions under the United Nations Security Council Resolutions 1373 (2001) and 2231(2015) as well as the United Nations sanctions regimes. As at date there are 14 on-going UN sanctions regimes. **Annex 1** contains a summary of the UN sanctions regimes.

1.18 The legislative and regulatory framework in Mauritius for combatting money laundering and terrorist financing includes-

- The FIAMLA as amended by the Finance (Miscellaneous Provisions) Act 2018, The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019, the Anti-Money Laundering and Combatting the Financing of Terrorism (Miscellaneous Provisions) Act 2020, the Finance (Miscellaneous Provisions) Act 2021 and as may be amended from time to time, (the FIAMLA)

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

- The Financial Intelligence and Anti-Money Laundering Regulations 2018 (FIAMLR 2018)

- The Financial Intelligence and Anti-Money Laundering (Registration of Reporting Persons) 2019 (FIAMLR 2019)

- The Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020 (last updated in March 2021) issued by the Financial Services Commission (FSC Handbook)

1.19 The Anti Money Laundering and Countering the Financing of Terrorism and Proliferation Compliance Manual ("the AML/CFT Compliance Manual") is designed to ensure that the Company adheres to all applicable laws, regulations, and regulatory requirements in relation to AML/CFT.

1.20 The Company shall ensure that the AML/CFT Compliance Manual and any changes thereto is communicated to every existing employee as well as new recruits.

1.21 The Compliance Officer shall monitor that the Company maintains a record in writing of-

- the policies, controls and procedures approved by the Board
- any changes to those policies, controls and procedures made as a result of regular review and updates as required under the FIAMLA and
- the steps taken to communicate those policies, controls and procedures or any changes to them to all existing employees and new recruits.

1.22 Employees should familiarize themselves with the FSC Handbook where specified in the AML/CFT Compliance Manual.

1.23 The Company is firmly committed to participating in national and international efforts to combat money laundering and the financing of terrorism and proliferation and will not allow its operations to be used or abused for purposes of these or other financial crimes.

1.24 The Company will observe all relevant and applicable restrictive measures under UN sanctions regimes and United Nations Security Council Resolutions (UNSCR) that apply or may apply to its operations and in accordance with the UNSA shall not establish or maintain any business relationship or conclude any transaction with an individual or entity on a UN sanctions list or on the domestic list.

1.25 The Company shall not establish or maintain any business relationship or conclude any transaction with an individual or entity on a sanctions list including-

- The Office of Foreign Asset Control in the United States of America (OFAC lists)
- Her Majesty's Treasury in the United Kingdom (HMT lists) and
- The Council of the European Union (EU lists).

1.26 The Company aims to be compliant with all AML/CFT legal and regulatory requirements and therefore all the policies and procedures set out in this manual should be strictly adhered to. Failure to do so is a breach towards the Company and the regulatory authorities.

1.27 Staff members should be aware of the offences under sections 14(3), 18(3), 19, and 32A of the FIAMLA and Regulation 33 of the FIAMLR 2018. **Annex 2** sets out the relevant extracts of the FIAMLA and FIAMLR 2018 in this respect.

2. AML/CFT Policy statement and Risk Appetite

Policy Statement

2.1. The objective of this AML/CFT Compliance Manual is to outline to staff members the obligations, regulations, rules and best practices on the prevention and detection of money laundering, terrorist financing and proliferation financing contained within the relevant laws, regulations and guidelines issued by Mauritius authorities.

2.2. The AML/CFT Compliance Manual shall be approved by the Board of Directors.

Objectives of the AML/CFT Policies

2.3. The Company is committed to conducting its business ethically, responsibly and in compliance with all applicable legislation, regulation, adopted industry codes and -standards as well as adhering to all internal policies and sound corporate governance principles and is committed to effective management of all relevant risks, including the risk that the institution may be used by criminal and terrorist elements to further their objectives and gains.

2.4. The Company has no appetite for deliberate or purposeful violations of legislative or regulatory requirements, adopted industry codes and standards, internal policies or governance principles. The Company seeks to conduct its business with due skill, care and diligence in order to minimise violations arising from negligence. All identified breaches of requirements will be addressed as soon as practicable.

2.5. Accordingly, the Company has established adequate AML/CFT policies, practices, and procedures, for the management of its ML/TF risks to-

- promote business with clients in such a manner that will minimise the risk of the Company receiving the proceeds of unlawful activities or being used for money laundering or terrorist financing purposes.
- prevent the Company from being used as a channel for money laundering, terrorist financing and proliferation financing.
- establish a framework for adopting appropriate AML/CFT procedures and controls in the operations/business processes of the Company.
- ensure compliance with the AML/CFT laws and regulations in force.
- protect the Company's reputation.

- assist competent authorities in their effort to prevent and combat money laundering, terrorist financing and proliferation financing.
- lay down AML/CFT compliance norms for the employees of the Company.
- ensure that reasonable steps are taken to manage these risks.
- maintain high ethical and professional standards.

2.6. The Company has adopted the following AML/CFT policies which are subject to regular review to ensure they remain current with legal requirements and regulatory expectations.

Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT) And Sanctions Compliance Policies

Risk Based Approach

The Company shall maintain a risk-based approach towards the detection and prevention of ML and TF and consequently shall maintain a risk assessment framework to identify, mitigate and periodically review its ML and TF risks.

Governance

The Company shall maintain and promote a governance framework to effectively manage its ML, TF and sanctions compliance risks that includes-

a. Allocation of explicit accountabilities and responsibilities to manage ML, TF, and sanctions compliance risks.
b. Appointment of a qualified AML/CFT/Sanctions Compliance Officer to have the responsibility for the AML/CFT and sanctions compliance functions with the stature and the necessary authority.
c. Appointment of a Money Laundering Reporting Officer (MLRO) and a Deputy Money Laundering Reporting Officer (DMLRO) to have responsibility for receiving internal suspicious transaction reports and making external disclosures to the Financial Intelligence Unit.
d. A strategy from Senior Management that actively promotes a strong AML/CFT and sanctions compliance culture.
e. Governance that sets out appropriate mandates, authorities and oversight capabilities.
f. Adequate resources in respect of personnel, competency and technology.
g. The responsibilities that all employees have in the management of ML, TF and sanctions compliance risks.
h. The specific accountabilities held by the relevant bodies and functions within the governance structure, including the Board, Senior Management, compliance, MLRO, DMLRO and employees.

Three lines of defence model

The Company supports and shall apply the Three Lines of Defence concept in its institutional Risk Management approach. It believes that the Three Lines of Defence concept is a key element in ensuring effective governance and oversight of ML, TF and sanctions compliance risks.

Compliance function

The AML/CFT and sanctions compliance function in the Company shall be appropriately authorised, positioned, resourced, and provided with reasonable, on-going access to all relevant staff, information and documentation to discharge their responsibilities.

AML/CFT Procedures

The Company shall adopt and maintain risk-based AML/CFT procedures that shall be approved by the Board of Directors.

The Board shall be responsible for periodically reviewing and keeping the procedures up to date.

Any amendments to the procedures shall be documented and approved by the Board.

The Board shall ensure that the policies and procedures (including changes thereto) are communicated to all employees of the Company and shall monitor the implementation of the policies and procedures.

Targeted Financial Sanctions

The Company shall adopt and maintain procedures for ensuring compliance with Targeted Financial Sanctions requirements under the UNSA.

Suspicious transaction reporting

The Company shall report any activity that it detects which is suspicious and may involve a potential money laundering, terrorism financing or proliferation financing offence or proceeds of crime to the Financial Intelligence Unit.

The Company shall appoint a Money Laundering Reporting Officer (MLRO) and a Deputy Money Laundering Reporting Officer (DMLRO) to whom an internal suspicious transaction report shall be made.

The MLRO and the DMLRO shall be the contact point for all issues regarding the FIU and shall be registered with the FIU.

Tipping off and confidentiality

Directors, officers and employees of the Company shall not disclose to any unauthorized third party the fact that an STR or related information is being or has been filed with the FIU.

Foreign branches and subsidiaries

The Company shall comply with the AML/CFT and sanctions compliance laws, rules, regulations, and regulatory requirements of the countries in which it maintains its operations.

Resources

The Company shall maintain reasonable steps to ensure that sufficient funding and resources are available for the implementation and performance of activities required by its AML/CFT and sanctions compliance Program.

Employee Screening

The Company shall maintain adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.

Training

The Company shall maintain an ongoing AML/CFT Training Programme.
Directors, officers, and employees of the Company shall attend AML/CFT and sanctions compliance training to understand their obligations under the relevant legal and regulatory requirements.

Customer Acceptance

The Company shall maintain customer acceptance procedures commensurate with the level of risk associated with the customer.

Failure to satisfactorily complete CDD

Where the Company is not able to satisfactorily complete Customer Due Diligence or Enhanced Due Diligence measures it shall terminate the business relationship and file a report with the Financial Intelligence Unit.

Monitoring

The Company shall monitor its customers, their transactions, and its employees, consistent with the level of money laundering and terrorist financing risk they represent.

Politically Exposed Persons

The Company shall put in place and maintain appropriate risk management systems to determine whether a customer or beneficial owner is a PEP and maintain adequate procedures when dealing with PEPs.

Third Party Reliance

The Company may rely on third parties to perform CDD measures or to introduce business and shall maintain procedures and processes when relying on third parties.

High-Risk Countries

The Company shall with respect to business relationships or transactions involving a high-risk country apply enhanced due diligence measures.

Record keeping

The Company shall maintain record keeping procedures in line with statutory requirements.

New Technologies

The Company shall manage new and revised changes to its products, business processes and systems to ensure that ML and TF risks **are identified and managed.**

Anonymous and fictitious accounts

The Company shall not establish or maintain an anonymous account or an account in a fictitious name.

Shell Banks

The Company shall not enter or continue a business relationship or occasional transaction with a shell bank.

Independent Audit

The Company shall maintain an independent audit function pursuant to Regulation 22 (1) (d) of the FIAML Regulations 2018.

Compliance Reviews

The Company shall maintain appropriate procedures for monitoring and testing compliance with AML/CFT and sanctions compliance requirements.

Compliance Culture "Tone from the Top"

The Board shall be responsible for promoting AML/CFT and sanctions compliance as a core value of the Company.

ML/TF Risk Appetite

2.7. The Company is aware that it is exposed to compliance risks if an appropriate AML/CFT and sanctions compliance programme is not established. The Company defines 'compliance risk' as the risk of damage to its business model, reputation, and financial condition from failure to meet laws and regulations, internal standards and policies and expectations of key stakeholders such as shareholders, supervisory authorities and other competent authorities, customers, employees, and society as a whole.

2.8. The three main ML/TF compliance risks and the risk appetite associated with those risks, are:

ML/TF risk

2.9. The Company does not tolerate the crimes of money laundering, terrorist financing or proliferation financing. The Company will conduct its business to ensure that it minimizes the risk of its systems and processes being used for ML, TF, or PF purposes.

Sanctions Compliance Risk

2.10. The Company will not establish a business relationship with a person or entity listed by or under the authority of the United Nations Security Council or a person designated pursuant to the UNSA.

2.11. If one of its customers is listed or designated (listed party) in the course of the business relationship, the Company will not deal with the funds or other assets of the listed party under its control or make funds or other assets available to or for the benefit of the listed party.

2.12. In case of any breach, the Board shall convene an exceptional meeting to resolve the matter as soon as possible. In parallel, a board sub-committee shall be set up to identify the causes of such a breach for corrective future action. The Company aims to be compliant at all times.

Regulatory Compliance Risk

2.13. The Company is unwilling to accept any regulatory breach. The Company will ensure that it adopts all regulatory, legal and compliance requirements and in case of any breach, the Board shall convene an exceptional meeting to resolve the matter as soon as possible. In parallel, a board sub-committee shall be set up to identify the causes of such a breach for corrective future action. The Company aims to be compliant at all times.

2.14. In line with the above policy statement, the Company has in accordance with AML/CFT requirements adopted detailed procedures set out in this manual to, among other things-

- establish an AML/CFT governance structure
- identify assess and understand the money laundering and terrorism financing risks for customers, countries or geographic areas and products, services, transactions, or delivery channels.
- mitigate and manage effectively the risks of money laundering and terrorism financing identified.
- implement a risk-based programme against money laundering and terrorism financing which includes —

(a) designation of a compliance officer.
(b) screening procedures to ensure high standards when hiring employees.
(c) an ongoing training programme for its directors, officers, and employees to maintain awareness of the AML/CFT legal and regulatory requirements to assist them in identifying and reporting suspicious transactions.
(d) an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with AML/CFT legal and regulatory requirements.
(e) establish the function of an MLRO and a DMLRO
(f) establish and maintain record keeping procedures
(g) establish and apply Customer due diligence measures including enhanced due diligence measures and on-going monitoring.
(h) detect and report suspicious transactions
(i) implement Targeted Financial Sanctions

3. Governance

3.1 The Company believes that effective ML/FT risk management requires proper governance arrangements and in particular, the requirement for the board of directors to approve and oversee the implementation of policies and procedures for risk, risk management and compliance in the context of ML/TF risk. In addition, to discharge its responsibilities, the Board shall:

3.1.1 within the limits set by the Company's AML/CFT compliance strategy and compliance risk appetite, set an appropriate corporate culture within which effect is given to this strategy and appetite.

3.1.2 ensure that the AML/CFT compliance strategy and compliance risk appetite are adhered to.

3.1.3 ensure that the Company's systems and controls are appropriately designed and implemented, and are effectively operated to reduce the risk of the business being used in connection with ML/TF/PF.

3.1.4 adopt and monitor the implementation of documented systems and controls which, inter alia, undertake risk assessments of the Company's business and its customers, determine the identity of customers and any beneficial owners and controllers, apply increased vigilance to transaction and relationships posing higher risks of ML and TF.

3.1.5 approve the outcome of the business risk assessment undertaken pursuant to section 17 of the FIAMLA and ensure that it is documented and reviewed periodically so that it remains up to date and relevant.

3.1.6 ensure that a MLRO, DMLRO and compliance officer are appointed.

3.1.7 monitor the effectiveness of the independent audit in assessing and evaluating the controls to prevent money laundering and the financing of terrorism and proliferation.

3.1.8 maintain adequate oversight of the overall AML /CFT measures undertaken.

3.1.9 set minimum standards and approve the policies regarding AML/CFT measures, including those required for customer acceptance, customer due diligence, record keeping, ongoing monitoring, reporting of suspicious transactions, targeted financial sanctions and combating the financing of terrorism.

3.1.10 assess the implementation of the approved AML/CFT policies.

3.1.11 define the lines of authority and responsibilities for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls.

3.1.12 review and assess the AML/CFT policies and procedures in line with changes and developments in products and services, technology, and trends in ML, TF and PF.

3.1.13 review, at least once a year, the report of the AML/CFT Compliance Officer and obtaining interim updates more frequently for activities that expose the Company to higher ML/TF risks.

3.1.14 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, in particular the adequacy of the human and technical resources allocated to the AML/CFT Compliance Officer.

3.1.15 implement the organizational and operational structure necessary to discharge the AML/CFT strategy paying particular attention to the adequacy of the human and technical resources allocated to the AML/CFT compliance function.

3.1.16 ensure adequate, timely and sufficiently detailed AML/CFT reporting to the FSC, FIU, NSSec and any other competent authority when required.

Risk Management

3.2 Within its broader governance framework, the Company has adopted the three lines of defence model to support its AML/CFT risk management programme. The responsibilities of each of the lines are:

3.2.1 The first line of defence, the business units (front line operating management) shall own and manage ML/TF risk and AML/CFT control. The first line of defence shall be responsible for identifying, assessing, and controlling the ML/TF risks of their business. They shall know and carry out the policies and procedures.

3.2.2 Senior management shall ensure that the first line of defence is allotted sufficient resources to carry out its functions effectively.

3.2.3 the second line of defence shall monitor ML/TF risk and AML/CFT control in support of management principally through the AML/CFT compliance officer, the MLRO and DMLRO

3.2.4 the third line of defence (independent audit) shall provide independent assurance to the board and senior management concerning the effectiveness of management of ML/TF risk and AML/CFT control. The independent audit may, subject to the FSC Handbook requirements, be carried out internally or may be outsourced to an independent third party.

3.3 The Board has delegated the effective execution of compliance management to the Senior Management of the Company. Senior Management shall be accountable to Board for the effective discharge of the delegated responsibilities.

3.4 The Board shall ensure that a robust independent compliance function is established for the Company.

3.5 The board of directors has appointed an AML/CFT/Sanctions compliance officer (Compliance Officer) to have overall responsibility for the AML/CFT function. In the performance of his function, the compliance officer shall have unrestricted access upon request to all books, records, and employees of the Company as necessary.

3.6 The compliance function will be responsible for the promotion and monitoring of the Group's culture of compliance and report on this regularly to the Board and management.

3.7 Ultimate accountability and responsibility for ensuring and overseeing the management of compliance in the Company resides with the Board.

3.8 In the absence of the compliance officer, senior management will be responsible for ensuring the continuity of the function of the compliance officer by making appropriate arrangements.

Remediation

3.9 In case of a breach of AML/CFT requirements, the Board will convene an exceptional meeting to resolve the matter as soon as possible. In parallel, the Board will set up a Board sub-committee to identify the causes of such a breach for corrective action.

3.10 After identifying the causes for such a breach, the Board Sub Committee will develop and recommend a remediation plan to the Board. Upon approval by the Board of the remediation plan the Board sub-committee will ensure that the remediation plan is implemented within such time as may be approved by the Board.

Duty of Vigilance of Employees

3.11 Staff members are at risk of being or becoming involved in criminal activity if they are negligent in their duty of vigilance and they should be aware that they face criminal prosecution if they commit any of the offences outlined under the relevant Laws.

3.12 Employees are therefore strongly advised and recommended to pay close attention to transactional pattern, suspicious behaviours of customers and whether all required mandatory documents, supporting documents and other relevant information are being held on file.

3.13 Employees shall ensure that they adhere strictly to the provisions of this Manual. In case of any non-adherence, the Company shall take necessary actions which may include disciplinary measures.

4. Money Laundering and Terrorist Financing Risk Assessment

4.1 Section 17 of the FIAMLA set out the framework for the adoption of a risk-based approach to combatting money laundering and terrorism financing. Adopting a risk-based approach implies the adoption of risk identification, assessment and management process for mitigating the ML /TF risks. This process encompasses recognising the existence of risk, undertaking an assessment of risk, understanding it and developing strategies to manage and mitigate the identified risks.

4.2 In addition, Chapter 4 of the FSC Handbook provides extensive guidance on the implementation of the risk-based approach (RBA). The RBA prescribes the following procedural steps to manage the ML and TF risks faced by the reporting person:

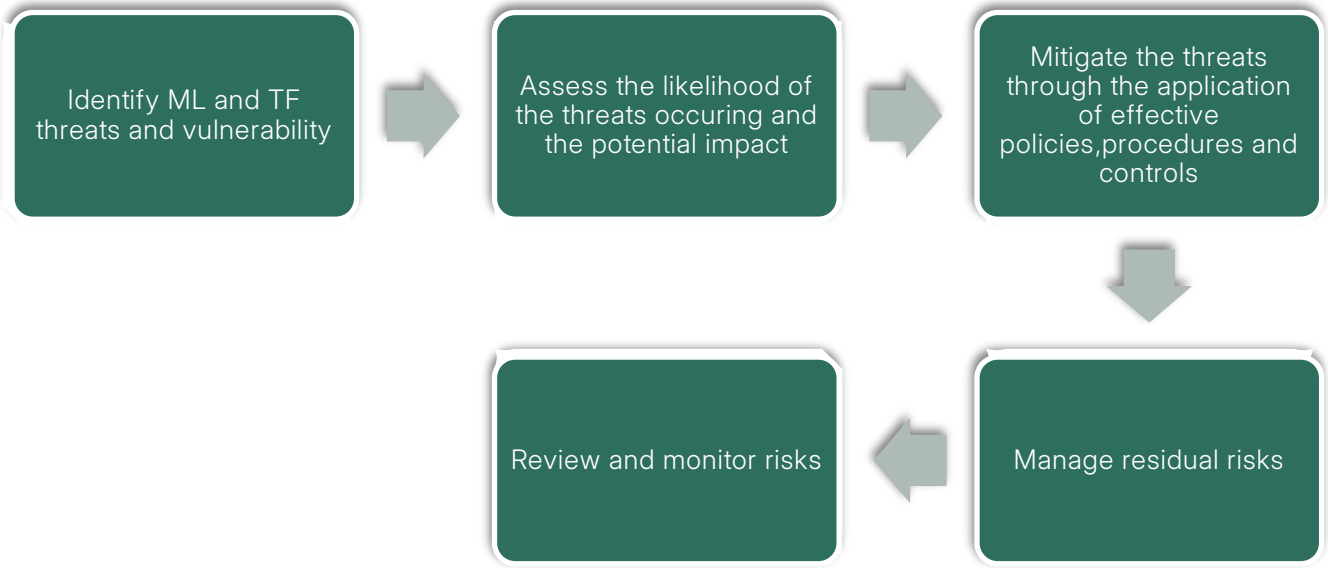


Figure 2 Risk Based Approach Process

4.3 In line with the above, the Company has developed policies and procedures to implement a risk-based AML/CFT framework which, as a first step requires the identification of ML and TF risks. In accordance with the outcome of the risk assessment, higher risk areas will be subject to enhanced procedures and other measures as set out in this Manual. These include enhanced CDD checks and enhanced transaction monitoring for higher risk situations. In situations where risks are lower, simplified or reduced controls may be applied. The implementation of the policies, procedures and controls will be monitored and enhanced as necessary. Senior management shall ensure that the allocation of resources shall be commensurate with the levels of ML and TF risks in the activities. More risk management resources shall be allocated to areas of greater risks.

Business Risk Assessment (BRA)

4.4 Under section 17 of the FIAMLA, a reporting person must take appropriate steps to identify, assess and understand the ML and TF risks for

- customers
- countries or geographic areas
- products and services
- transactions or
- delivery channels.

4.5 The nature and extent of any assessment of ML and TF risks must, in line with section 17(2) of the FIAMLA, have regard to the nature and size of the business of the reporting person and shall take into account-

(a) all relevant 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;
  (vi) technological developments and
(b) the outcome of any risk assessment carried out at a national level and any guidance issued.

4.6 The Company shall in accordance with section 17 of the FIAMLA and considering the guidelines provided in the FSC Handbook adopt a methodology to identify, assess and understand the money laundering and terrorist financing risks.

4.7 Management, compliance and risk management shall all work together on performing the BRA. Primarily, responsibility for the quality and execution of risk analysis shall lie with the first line of defence, as risks manifest themselves first there. The role of the Compliance officer is process monitoring, facilitating and testing. Other functions or departments such as audit shall also provide the necessary input. The ultimate responsibility for the BRA lies with the board of directors.

4.8 Prior to the launch of a new product or business practice or the use of a new or developing technology, the Company shall identify and assess the money laundering or terrorism financing risks that may arise in relation to such new products or business practices or new or developing technologies for both new and pre-existing products and take appropriate measures to manage and mitigate these risks.

Customer Risk Assessment (CRA)

4.9 To consider the extent of its potential exposure to the risk of ML and TF, the Company shall assess the risk of any proposed business relationship. In accordance with the FSC Handbook, the following risk assessment process shall be adopted-

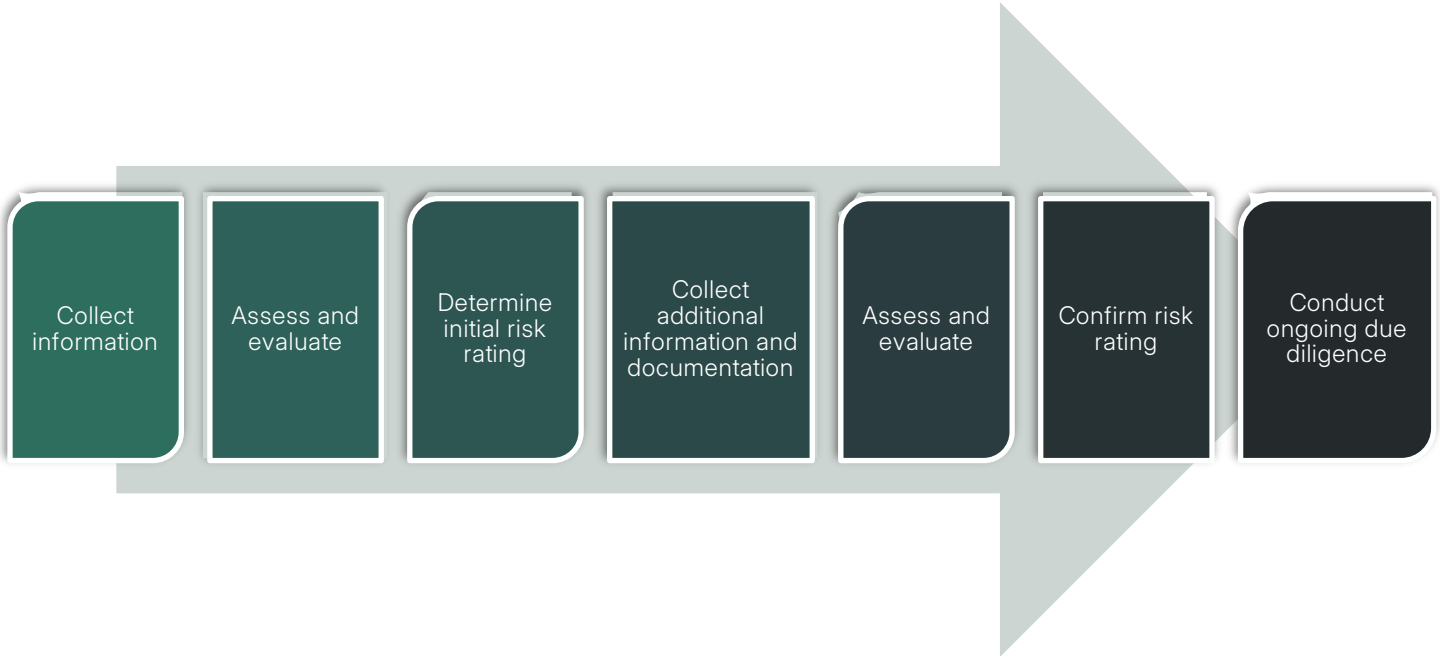


Figure 3 Customer Risk Assessment Process

Risk assessments reviews

4.10 The Compliance Officer will ensure that the BRA and CRA are kept up to date by initiating regular reviews. All employees and officers of the Company must when called upon by Senior Management participate and collaborate with the Compliance Officer to conduct the BRA and CRA or update or review any BRA or CRA.

4.11 The Compliance officer will ensure that business risk assessments are reviewed at least annually.

4.12 Regarding the frequency of the reviews, the Compliance Officer will be guided by the FSC Handbook 2020 which recommends that the CRAs should be reviewed at least annually for higher-risk customers or whenever a transaction with a high-risk country or high-risk customer occurs; at least every 3 years for standard risk customers subject to sector-specific guidance; and at the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business. The CRA shall be reviewed at least every four years for low-risk customers.

Risk assessments records

4.13 The Compliance Officer shall ensure that all risk assessments are recorded and documented in order to be able to demonstrate their basis. Any review of the risk assessment should be documented to evidence that an appropriate review has taken place.

4.14 The Company shall document the rationale when determining the applicability, impact and probability for all risk factors in the risk assessment working papers. It shall be the responsibility of the Compliance officer to ensure that such records are kept and maintained.

4.15 The Compliance Officer will with the approval of senior management make the risk assessments available to the FSC or other relevant competent authorities[2] on request and without delay.

Reports to the Board

4.16 The Compliance Officer will report the outcome of all BRAs and CRAs, including any reviews or updates, conducted to the Board. The reports to the Board will contain recommendations for approval on the measures that are required to manage and mitigate the risks identified through the establishment of appropriate and effective policies, procedures and controls.

[2] The term "competent authorities" is defined in the FIAMLR 2018 -

(a) means a public authority to which responsibility to combat money laundering or terrorist financing is designated; and

(b) includes a supervisory authority, regulatory body and an investigatory authority;

5. Customer Due Diligence Procedures

5.1 Customer Due Diligence (CDD) procedures are designed to ensure that the Company is aware of the identity of each customer, beneficial owner, and related third parties, understands, and obtains relevant information on the types of transactions that the customer conducts, evaluates the intended nature of the business relationship, and that the business relationship and transactions are monitored on an ongoing basis. This will allow the Company to assess the overall risk of their business relationships with these parties by assigning a dynamic risk rating (i.e., one that changes with the nature and severity of the risks identified) to each overall relationship, which will help determine the level of due diligence to be applied to each of the customers.

5.2 Consistent with the requirements of the FIAMLA and the FIAMLR 2018, the Company has adopted CDD procedures that respond to the ML/TF risk posed to the business relationship.

5.3 In accordance with section 17C(3) of the FIAMLA, where risks are higher enhanced due diligence measures consistent with the risks identified shall be conducted.

5.4 Where the risks identified are lower, simplified CDD measures may be conducted in accordance with such guidelines issued by the FSC.

5.5 Simplified CDD measures shall not be conducted where there is a suspicion of ML or TF, in which case enhanced CDD measures shall be applied.

5.6 The business units shall be primarily responsible for conducting customer due diligence measures and ensuring that all relevant records are kept and maintained.

5.7 Figure 4 below sets out the customer onboarding CDD process flow of the Company.

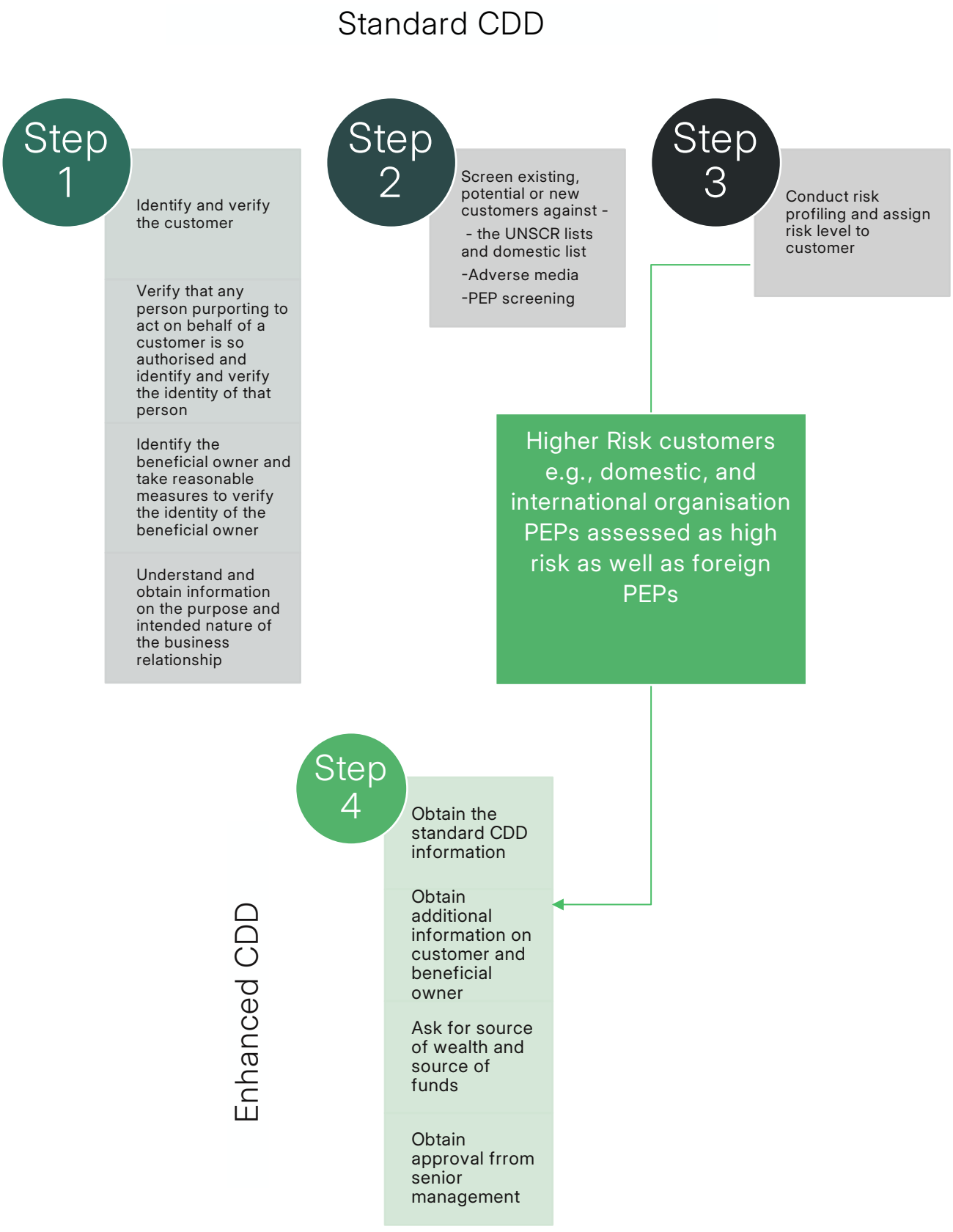


Figure 4 Customer onboarding CDD process flow

When is CDD required?

5.8 CDD measures shall be undertaken in accordance with section 17C of the FIAMLA and in the following circumstances:

- ✓ When opening an account for or otherwise establishing a business relationship with a customer
- ✓ carrying out occasional transactions 500,000 rupees, including situations where the transaction is carried out in a single operation or in several operations that appear to be linked.
- ✓ carrying out occasional transactions that are domestic or cross border wire transfers.
- ✓ there is a suspicion of ML/TF, involving the customer or customer's account or
- ✓ whenever the Company has doubts about the veracity or adequacy of previously obtained customer identification information.

5.9 Where the business unit forms a suspicion of ML/TF/PF, and it reasonably believes that performing the CDD process, may tip-off the customer, it must not pursue the CDD process, and it must make an internal disclosure to the MLRO.

5.10 In accordance with Regulation 3(3) of the FIAMLR 2018, the MLRO will be responsible for filing an STR with the FIU under section 14 of the Act and the STR will specify the reasons for not pursuing the CDD process.

CDD measures for all customers

5.11 When applying CDD measures for all customers, the Company shall, in accordance with Regulation 3 of the FIAMLR 2018, identify the customer whether permanent or occasional and verify the identity of the customer using reliable, independent source documents, and data.

5.12 The business unit shall ensure that all natural persons are identified and verified in line with the requirements of Regulation 4 of the FIAMLR 2018.

5.13 The business unit must identify and verify the identity of a natural person and collect information on natural persons in accordance with the procedures set out in the table below.

Data to be Identified	Methods of verification
1. Legal name (including any former names, aliases and any other names used) 2. Sex 3. Date of birth 4. Place of birth 5. Nationality	✓ Current valid passport ✓ Current valid national identity card ✓ Current valid driving licence
6. Current residential address 7. Permanent residential address	✓ Recent[3] utility bill issued to the individual by name ✓ Recent bank or credit card statement A recent reference letter of introduction from: ✓ A financial institution that is regulated in Mauritius ✓ A regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standard; or ✓ A branch or subsidiary of a group head quartered in a well- regulated overseas country or territory which applies group standard to subsidiaries and branches worldwide. And tests application of, and compliance with, such standard
8. Any public position held and, where appropriate, nature of employment (including self-employment) and name of employer	✓ A letter or written confirmation of the individual's status from the public body in question and or any EDD; a letter or other written confirmation of employment
9. Government issued personal identification number or other government issued unique identifier	✓ The relevant government documents.

[3] 'recent' means within the last three months.

5.14 The business unit must ensure that original documents should be signed by the individual and if the individual is met face-to-face, the documents should preferably bear a photograph of the individual. Where copies of documents are provided, appropriate authorities and professionals should certify the authenticity of the copies.

5.15 The business unit must verify that any person purporting to act on behalf of the customer is so authorised and must also identify and verify the identity of that person.

5.16 The business unit must identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner using relevant information or data in accordance with these procedures, such that it is satisfied that it knows who the beneficial owner is. For the purposes of this paragraph[4] –

"beneficial owner" -
(a) means the natural person –
  (i) who ultimately owns or controls a customer; or
  (ii) on whose behalf a transaction is being conducted and
(b) includes those natural persons who exercise ultimate control over a legal person or arrangement and such other persons as specified in regulations 6 or 7 of the FIAMLR 2018

"reasonable measures" means appropriate measures which are commensurate with the money laundering or terrorist financing risk;

"satisfied" where reference is made to a reporting person being satisfied as to a matter means the reporting person shall be able to justify his assessment to competent authorities, including a regulatory body, a supervisory authority, an investigatory body, or the FIU.

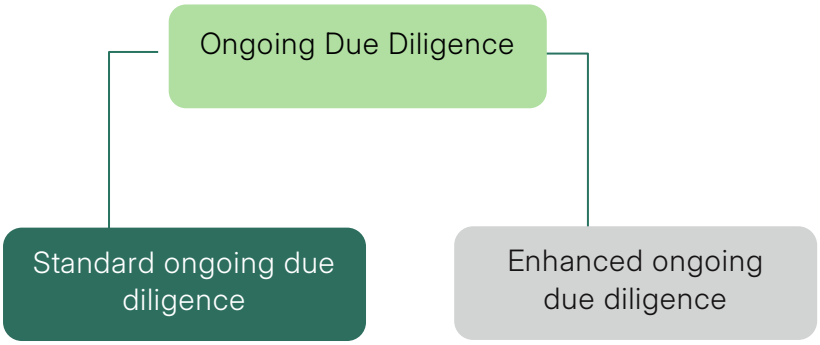
5.17 The business unit must also understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

[4] The terms are as defined in Regulation 2 of the FIAMLR 2018

Ongoing due diligence measures

5.18 In accordance with Regulation 3 1(e) of the FIAML Regulations, the Company shall conduct ongoing monitoring of all its business relationships. The ongoing due diligence process flow is set out in figure 5 below.

Figure 5. Ongoing due diligence process flow



Transaction Monitoring	Scrutinise transactions to ensure consistency with customer profile	▪ Scrutinise transactions at a frequency that is commensurate with the customer's risk profile ▪ Screen against UN sanctions lists and domestic list ▪ Select patterns of transactions that need further examination
CDD Updating	Ensure that CDD document, data or information on customers are kept up to date and relevant. Screen against UN sanctions list, domestic list, PEP, and adverse media reports	
Controls		Increase number and timing of controls applied

5.19 Ongoing due diligence shall involve a review of all transactions made throughout the course of the business relationship, including, where applicable the source of funds, to confirm that the transaction is consistent with the customer's knowledge and profile.

5.20 The proper monitoring of transactions is of utmost importance for an AML / CFT framework to function efficiently. Transaction monitoring must be done in a two-phased approach:

(i) Checking and verifying process before the transaction / financial service takes place

(ii) Monitoring transactions after it took place

Checking and verifying process before the transaction/financial service takes place

5.21 This process will involve the two Directors, the Compliance Officer and the Money Laundering Reporting Officer. In order to comply with the FIAML Regulations 2018 and to ensure proper payment process, BEX Mauritius Block Exchange shall have the following in place:

- A payment checklist shall cover different procedures such as call back to confirm the payment instructions; payments as per business activity; screening reports; supporting documents and bank balance check; and
- After filing out the payment checklist, the checklist will be reviewed by the Manager and approved by the Director

Monitoring transactions after it took place

5.22 The second approach will be to monitor transactions after they have been processed. This will be usually carried out during file reviews (depending on risk rating attributed) and audit process. The Compliance Officer and MLRO will additionally conduct random transactions review on a regular basis.

5.23 Staff members, in general, will have an important role to play in the transaction monitoring process. For instance, since some staff deal directly with clients and receive payment instructions on a regular basis, they are in a better position to know the client and his business and therefore, notice unusual behaviours, transactions or patterns in the business activity. Staff have therefore an obligation of operating with due diligence and, if anything suspicious is noticed, make an STR to the MLRO.

Screening against Domestic and UN Sanctions Lists

5.24 All transactions and customers (including beneficial owners) shall be screened against domestic and UN Sanctions Lists and other international sanctions lists. Any potential match shall be further investigated and escalated to the compliance officer. Any positive match on a UN Sanctions List shall be reported to the FSC, the NSSec and FIU. Pease refer to Chapter 12 of the Manual for further information.

Complex and unusual transactions

5.25 The background and purpose of all transactions that –

(a) are complex
(b) are unusually large
(c) are conducted in an unusual pattern or
(d) do not have an apparent economic or lawful purpose shall be examined.

The Company shall verify those types of transactions against the client profile established by the Company as part of the CDD process to determine whether this may amount to a suspicious transaction.

Adverse media screening

5.26 When screening customers, the business unit shall also consider "negative press" or "adverse media" reports or whether the customer is a "reputationally exposed person" (REP) in addition to whether the customer is classified as a PEP.

5.27 Negative press, as defined in the FSC Handbook, means any negative information, whether alleged or factual. This could be anything from an allegation of fraud by a disgruntled former customer to an article in a newspaper relating to a criminal investigation.

5.28 When analysing the media report, the business unit shall consider -

- the credibility of the information source,
- the severity of the negative press,
- how recent the information is and
- the potential impact the negative press would have on the business relationship with that customer

5.29 The business unit 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.

5.30 Through the ongoing due diligence monitoring all the data or information acquired as part of the CDD process will be reviewed to ensure that they are up to date and relevant. Periodic checks of existing records for higher-risk clients shall be prioritised.

5.31 The business unit shall pay attention to all requested changes to the exercise of rights under the terms of the contract. It should assess whether the change/transaction fits the risk profile category of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

5.32 For the purposes of ensuring that documents, data, or information collected under the CDD process is kept up-to-date and relevant existing records will be reviewed as follows, unless there is a material change in the risk rating of the customer which will require an earlier review.

Level of risk of customer	Frequency of review
Low	Every 3 years
Medium	Every 2 years
High	Yearly or depending on the volume of transaction

Identification/certification information for legal persons and legal arrangements

5.33 The business unit shall, when performing CDD measures in relation to customers that are legal persons or legal arrangements with respect to the customer, understand and document —

(iii) the nature of his business; and

(iv) his ownership and control structure.

5.34 Furthermore, the business unit shall, in accordance with Regulation 5 of the FIAML Regulations identify the customer and verify his identity by obtaining the following information:

(a) name, legal form and proof of existence;

(b) powers that regulate and bind the customer;

(c) names of the relevant persons having a senior management position in the legal person or arrangement; and

(d) the address of the registered office and, if different, a principal place of business.

5.35 The business unit shall identify and verify the identity of a legal person and collect information on legal persons in accordance with the procedures set out in the table below.

Persons to be identified	Data to be Identified	Methods of verification
Underlying persons who are individuals.	As per the requirements for natural person Where the individual persons are such by virtue of their status as members of the board of directors of a relevant legal person (or equivalent – for examples partners in a partnership, or council members in a foundation), financial institutions are required to identify and verify the identity of all such persons.	As per the requirements for natural person Where the legal person with which the underlying person is associated is low or standard risk, then the method of verification for each required piece of data will normally suffice and can be one of the above methods. However, where the legal person is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary
Private Companies Partnerships	10. Legal status of body 11. Legal name of body 12. Any trading names 13. Nature of Business	✓ Certificate of incorporation (or other appropriate certificate of registration or licensing); ✓ Memorandum and Articles of Association (or equivalent);

Persons to be identified	Data to be Identified	Methods of verification
Sociétés Foundations Other Legal Persons	14. Date and country of Incorporation 15. Official identification number (for example, company number) 16. Registered office address 17. Mailing address (if different from registered address) 18. Principal place of business / operations (if different) 19. Any other data which the Company considers to be reasonably necessary for the purposes of establishing the true identity of the legal person.	✓ Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; ✓ Latest audited financial statements or equivalent; ✓ Annual report or equivalent; ✓ Personal visit to principal place of business; ✓ Partnership deed or equivalent; ✓ Charter of Foundation; ✓ Acte de Société; ✓ Certificate of good standing from a relevant national body; ✓ Reputable and satisfactory third-party data, such as a business information service ✓ Any other source of information that to verify that the document submitted is genuine.

5.36 The business unit shall collect the identification data concerning a legal person listed in the left-hand column of the table below, and verify that data in accordance with the following:

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

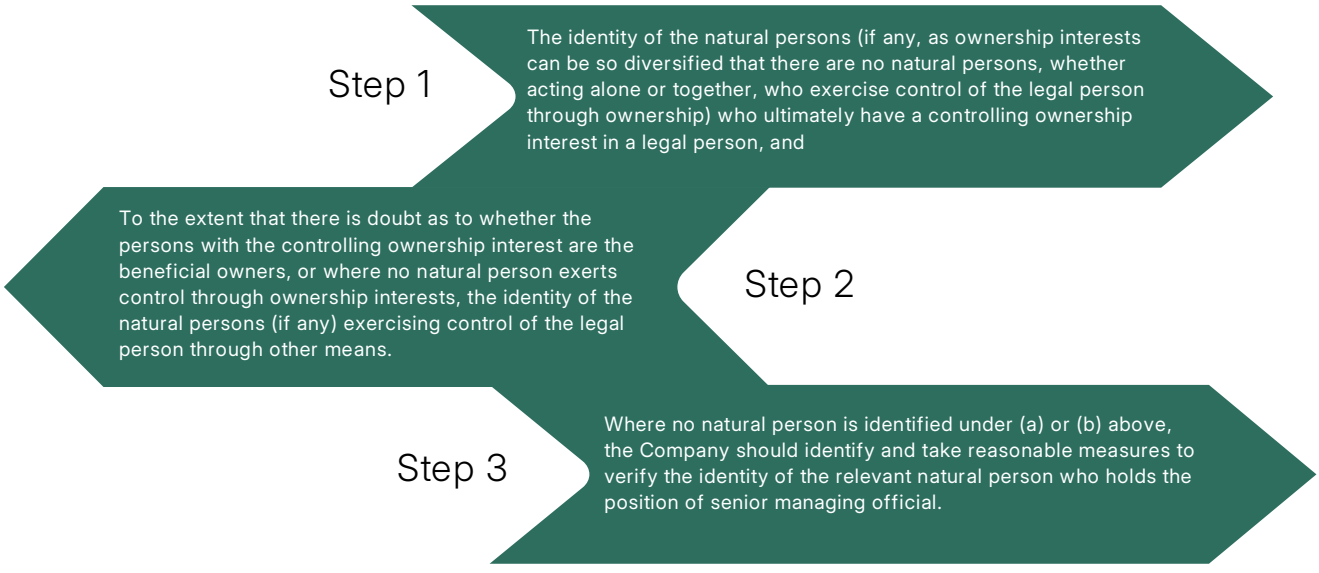
b) The appropriate number of methods for verifying the data will vary depending on the status of the person to be identified and the risk rating:
(i) For low-risk legal persons, verification of each piece of the required data may take place using one of the methods identified.
(ii) For standard and high-risk legal persons, verification of each item of the required data must take place using at least two such methods wherever practicable.

5.37 The business unit shall identify and verify the identity of a legal arrangement and collect information on underlying principles that are legal arrangements in accordance with the procedures set out in the table below.

Data to be Identified	Methods of verification
1. Legal status arrangement (including date of establishment) 2. Legal name of arrangement (if applicable) 3. Trading or other given name(s) of arrangement (if applicable) 4. Nature of Business 5. Date and country of Incorporation 6. Any official registration or identification number (If applicable) 7. Registered office address (If applicable) 8. Mailing address (if different) 9. Principal place of business / operations (if different) 10. Any other data which the Company considers to be reasonably necessary for the purposes of establishing the true identity of the legal person.	✓ Trust deed or equivalent instrument ✓ Official certificate of registration (if applicable) ✓ Where the above proves insufficient, any other document or other source of information which it is reasonable to place reliance in all circumstances.

Identification/verification of beneficial owners of legal persons

5.38 The business units must ensure that the beneficial owners of legal persons are adequately identified and verified. Reasonable measures to verify the identity of such persons shall be conducted in accordance with Regulation 6 of the FIAML Regulations through the following steps:



5.39 The business unit shall ensure that records of the actions taken under above as well as any difficulties
encountered during the verification process is maintained.

Identification/verification of beneficial owners of legal arrangement

5.40 For customers that are legal arrangements, the business unit shall identify and take reasonable measures to verify the identity of beneficial owners by obtaining information —

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

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

Timing of Verification

5.41 The Company shall ensure that the verification of the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers is undertaken as prescribed under Regulation 9 of the FIAML Regulations.

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

5.43 It is to be noted that under the FIAMLR 2018, a reporting person may be allowed by the relevant supervisory authority or regulatory body to complete the verification of the identity of the customer and beneficial owner after the establishment of the business relationship, provided that —

(a) this is essential not to interrupt the normal conduct of business;
(b) the verification of identity occurs as soon as reasonably practicable; and
(c) the money laundering and terrorism financing risks are effectively managed by the reporting person.

Where the reporting person is allowed to establish the business relationship before the completion of the verification of identity of the customer and beneficial owner, he shall adopt and implement risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

Existing Customers

5.44 In accordance with section 17E of the FIAMLA, the Company shall apply the CDD requirements to customers and beneficial owners with which it had a business relationship prior to the amendments brought to the FIAMLA in 2018.

5.45 The Company shall determine when to take CDD measures in relation to existing customers by taking into account the following:

a) Where there is a change in the identity of the customer or the beneficial owner;
b) Where transactions are not reasonably consistent with the knowledge of the customer;
c) For any change in the purpose or intended nature of his relationship with the customer;
d) any other matter which might affect his assessment of the money laundering, terrorist financing or proliferation financing risk in relation to the customer.

Simplified Due Diligence

5.46 In accordance with section 17C (4) of the FIAMLA, where risks are lower, the Company may conduct simplified due diligence measures unless there is a suspicion of ML or TF in which case enhanced CDD measures shall be undertaken.

5.47 The simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by the FSC.

5.48 Furthermore, the low risk identified must be consistent with the findings of the national risk assessment or any risk assessment of the FSC, whichever is most recently issued.

Enhanced Due Diligence

5.49 Enhance due diligence (EDD) requires taking specified steps which include requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner, obtaining additional information on the intended nature of the business relationship and the source of fund/wealth, obtaining information on the intended or performed transactions, obtaining the approval of senior management to commence or continue the business relationship, conducting close monitoring of the business relationship and any other measures deem appropriate as part of the risk mitigation.

5.50 EDD requirements include establishing the source of funds, the source of wealth, undertaking further research on the customer's background and considering what additional identification information and verification should be obtained and ongoing monitoring carried out.

5.51 The Company shall, in line with Regulation 12(1) of the FIAML Regulations, undertake EDD in the following circumstances:

(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 country[5];
(d) in relation to correspondent banking relationships (if applicable);
(e) 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.

High risk country

5.52 Pursuant to Section 17H of the FIAMLA, the Company shall, with respect to business relationships or transactions involving a high risk country apply enhanced due diligence measures as prescribed under FIAMLR 2018.

5.53 In addition, the Company shall, where applicable and proportionate to the risks, apply one or more of the following additional mitigating measures to persons and legal entities carrying out transactions involving those high risk countries –

(a) the application of additional elements of enhanced due diligence;

(b) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;

(c) the limitation of business relationships or transactions with natural persons or legal entities from those high risk countries.

5.54 Under section 2 of the FIAMLA a "high risk country" means a jurisdiction identified under section 17H. In accordance with section 17H(1) of the FIAMLA the Minister has by way of Government Notice GN 587 of 2020 designed Democratic People's Republic of Korea (DPRK), Myanmar and Iran as high risk country. The FATF has identified these two jurisdictions as having strategic deficiencies in their AML/CFT measures

5.55 In accordance with the Government Notice, the Company shall –

(a) consult the FATF public documents which are published on the website of the FATF (https://www.fatf-gafi.org/) at least 3 times a year, namely in February, June and October, and apply the countermeasures recommended by the FATF in those documents;

(b) give special attention to business relationships and transactions with persons (both natural and legal persons) in those high risk countries, including companies, legal arrangements/trusts and financial institutions based in those countries; and

(c) strengthen systems and controls in managing their exposure to the vulnerabilities identified by FATF.

[5] Section 2 of the FIAMLA the term "high risk country" means a jurisdiction identified under section 17H. See GN 587 of 2020

5.56 Business units should be aware that any non-compliance with the directions and specifications contained in the Government Notice is a criminal offence under the FIAMLA and may further attract administrative sanctions and penalties imposed by the FSC.

Unusual activity

5.57 In accordance with Regulation 28(1) of the FIAMLR 2018, where a business unit identifies any unusual activity in the course of a business relationship or occasional transaction it shall –

- perform appropriate scrutiny of the activity;
- obtain enhanced CDD in accordance with regulation 12 of FIAMLR 2018 and
- consider whether to make an internal disclosure to the MLRO.

5.58 A business unit shall examine, as far as reasonably possible, the background and purpose of all transactions that –

(a) are complex transactions;
(b) are unusually large transactions
(c) are conducted in an unusual pattern; or
(d) do not have an apparent economic or lawful purpose.

5.59 Where the risks of money laundering or terrorism financing are higher, the business unit shall conduct enhanced CDD measures consistent with the risk identified. In particular, it shall increase the degree and nature of monitoring of the business relationship in order to determine whether those transactions or activities appear unusual or suspicious.

5.60 The business unit shall keep a record of all analysis undertaken under paragraph 5.55 above.

5.61 Examples of enhanced CDD measures that could be applied for higher-risk relationships are set out under Regulation 12(2) of the FIAMLR 2018 and include-

Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).	✓
Updating more regularly the identification data of the customer and the beneficial owner	✓
Obtaining additional information on the intended nature of the business relationship	✓
Obtaining information on the source of funds or source of wealth of the customer	✓
Obtaining information on the reasons for intended or performed transactions	✓
Obtaining the approval of senior management to commence or continue the business relationship	✓
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	✓

Failure to satisfactorily complete CDD

5.62 The business unit shall ensure that where there is a failure to satisfactorily complete CDD measures, the business unit shall, as provided under regulation 13 of the FIAMLR 2018:

Failure to satisfactorily complete CDD		
Not open the account, commence the business relationship, or perform a transaction.	Terminate the business relationship.	In relation to the customer, file make an internal disclosure to the MLRO/DMLRO who shall make a STR under section 14 of the FIAMLA.

Appropriate Certification

5.63 As pointed above, all documentation should be in original form or duly certified. Certification can be done by one of the following:

a) A lawyer, notary, actuary or an accountant holding a recognized professional qualification;
b) A serving police or customs officer;
c) A member of the judiciary;
d) A senior civil servant;
e) An employee of an embassy or consulate of the country of issue of identity documentation;
f) A director or secretary (holding a recognised professional qualification) of a regulated financial services business in Mauritius or in an equivalent jurisdiction; or
g) A Commissioner of Oaths.

5.64 If a business unit meets an applicant for business (face to face) where it had access to original documents, then it can make copies of these and have them certified as true copies of the original.

6. Politically Exposed Persons

6.1 Politically Exposed Persons (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. Regulation 2 of the FIAMLR 2018 defines PEP as follows-

"Politically Exposed Person" or "PEP" —

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

(b) for the purposes of this definition —

"domestic PEP" means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

"foreign PEPs" means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

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

6.2 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.

6.3 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.

6.4 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).

6.5 The relevant requirements of paragraphs 6.3 and 6.4 shall apply to family members or close associates of all types of PEP.

6.6 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

Step 1: Full and effective implementation of normal CDD measures under Reg 3-10 of FIAMLR 2018

For foreign and domestic/international organisation PEPs • Implement effective CDD measures in line with FIAMLR 2018 • CDD measures are the indispensable starting point for the effective implementation of Reg 15 of FIAMLR 2018. • Reg 15 imposes additional requirements for PEPs which are summarised in step 2 and 3	
Step 2: Determine if a customer is a PEP	
For foreign PEPs	**For domestic/international organization 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.	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 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.	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
	Determine the risk of the business relationship and in low risk cases. no further steps are required
Step 3: Take risk mitigation measures	
For Foreign PEPs	**For domestic/international organization PEP**
Apply the enhanced risk mitigation measures of Reg 15 (1)(b) to (d) in all cases	In cases of a higher risk business relationship with the PEP apply the enhanced risk mitigation measures of Reg 15 (1)(b) to (d).

Identification Process

6.7 The Company's PEP identification process will be proportionate to the risk and concentrate on customers that are PEPs. In addition, this will be supplemented with public record searches using the due diligence tools as well as other public record search options available through the internet. Continued monitoring will take place for all new customers who reach the threshold as above and periodically on a quarterly basis.

Notification

6.8 When it is found that the Company has entered into a business relationship with a PEP, the head of the business unit will notify its team of a business relationship with a PEP.

- The notification will include a risk assessment
- The Company's checks will include obtaining information about the individual PEP's business or status and their source of funds and wealth.
- Any ongoing relationship will be subject to enhanced on-going monitoring.

6.9 The business unit shall obtain the approval of senior management prior to establishing a business relationship with a PEP. Once the relationship is approved with a PEP, same shall be entered into the PEP register for monitoring purposes.

6.10 Where in the course of a business a client or the beneficial owner becomes a PEP, the business unit must thoroughly review the relationship and obtain senior management approval for continuing the business relationship and apply enhanced due diligence measures to establish the source of funds and source of wealth of such persons.

6.11 In case where 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.

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

7. New Technologies

7.1 In accordance with Regulation 19 of the FIAMLR 2018, the Company shall identify and assess the money laundering and terrorism financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

7.2 The Board of the Company shall ensure that a risk assessment prior to the launch of the product, practice, or technology, and shall take appropriate measures to manage and mitigate the risks identified.

7.3 The Compliance officer shall, with the assistance of such officers as may be required based on their skills, knowledge, and competency in the field of AML/CFT or new technologies, undertake such risk assessments.

7.4 The outcome of the risk assessment as well as the appropriate measures to manage and mitigate the risks identified will be approved by the Board.

8. Third Party Reliance

8.1 Section 17D of the FIAMLA allows a reporting person to rely on third parties to perform CDD measures to comply with the requirements under section 17C, subject to such terms and conditions prescribed in the FIAMLR 2018.

8.2 In accordance with Regulation 21 of FIAMLR 2018, when relying on a third party to perform CDD measures under Reg 3(1)(a), (c) and (d) or to introduce business, the business unit shall satisfy itself that the third party is regulated and supervised or monitored for purposes of combating money laundering and terrorism financing and has measures in place for compliance with CDD and record keeping requirements in line with the FIAMLA and the FIAMLR 2018.

8.3 The business unit shall –

- obtain and maintain documentary evidence that the third party is regulated for the purposes of combating money laundering and terrorism financing and

- be satisfied that the procedures laid down by the third party meet the CDD and record keeping requirements under the FIAMLA and FIAMLR 2018.

8.4 The business unit needs to be aware on the level of the country risk when determining in which country the third party can be based. In accordance regulation 21(3) of FIAMLR 2018, the Company shall not rely on a third party based in a high risk country.

8.5 Section 2 of the FIAMLA sets out the definition of a "high risk country" as meaning a jurisdiction identified under section 17H. In accordance with GN 587 of 2020, the Democratic People's Republic of Korea (DPRK), Myanmar and Iran have been identified as high risk countries under section 17H of the FIAMLA.

8.6 In determining the level of country risk of the third party the business unit shall be guided by Regulation 24(1) of the FIAMLR 2018, namely-

(a) strategic deficiencies in the anti-money laundering and combating the financing of terrorism legal and institutional framework, in particular in relation to –
  (i) criminalisation of money laundering and terrorism financing;
  (ii) measures relating to CDD;
  (iii) requirements relating to record-keeping;
  (iv) requirements to report suspicious transactions;
  (v) the availability of accurate and timely information of the beneficial
  (vi) ownership of legal persons and arrangements to competent authorities

(b) the powers and procedures of the country's competent authorities for the purposes of combating money laundering and terrorist financing including appropriately effective, proportionate and dissuasive sanctions, as well as the country's practice in cooperation and exchange of information with overseas competent authorities;

(c) the effectiveness of the country's system for combating money laundering and terrorism financing in addressing money laundering or terrorist financing risks.

8.7 The business unit shall also consider if the country of the third party is vulnerable to corruption or is politically unstable.

8.8 The business unit shall ensure that-

(a) there is a signed agreement between the third party and the Company in which, the third party consents to being relied upon for these purposes and undertakes to provide the required CDD information upon onboarding.

(b) the signed agreement contains clear contractual terms in respect of the obligations of the third party to-
(i) obtain and maintain the necessary CDD documentation and to provide the CDD documentation upon request;
(ii) retain CDD documentation and not dispose of them without the consent of the Company
(iii) provide timely access to such documentation (including inspection of documents) upon request and
(iv) promptly transfer to the custody of the Company if the third party ceases to act in that capacity

(c) the signed agreement does not contain any conditional language, whether explicit or implied, which may result in the inability of the third party to provide the CDD documents. For example, language which qualifies the obligation to provide the CDD documents, such as "to the extent permissible by law" or subject to regulatory request" is not acceptable.

8.9 The business unit shall ensure that periodic testing of the arrangements with the third party are conducted, and the compliance officer shall verify that such testing has been conducted and the conditions of the FIAMLA, FIAMLR 2018 and FSC Handbook have been met, including compliance with the requirement under Reg 14(3) of FIAMLR 2018.

9. Internal Controls and foreign branches and subsidiaries

9.1 Regulation 22 of the FIAMLR 2018 requires reporting persons to have in place and implement programmes and systems to prevent money laundering and the financing of terrorism. These programmes should include internal policies, procedures and controls which have regard to the risk of ML/TF and the size of the business, and which cover:

- designation of a compliance officer at senior management level to be responsible for the implementation and ongoing compliance of the reporting person with internal programmes, controls and procedures with the requirements of the FIAMLA and the FIAMLR;

- screening procedures to ensure high standards when hiring employees;

- an ongoing training programme for its directors, officers and employees to maintain awareness of the laws and regulations relating to money laundering and terrorism financing to —
  (a) assist them in recognising transactions and actions that may be linked to money laundering or terrorism financing; and
  (b) instruct them in the procedures to be followed where any links have been identified; and

- an independent audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the Act and these regulations.

Employee screening

9.2 The Company shall establish a screening process for all new recruits as prescribed under regulations 22 1(b) of the FIAMLR Regulations 2018. It is important that the employees recruited meet the requirement of the Company.

9.3 The Company shall undertake due diligence on prospective employees and throughout the course of employment. At a minimum, it shall:

9.4 Verify the applicant's identity and personal information including employment history and background;

9.5 Develop a risk-focused approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications;

9.6 Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of employees over a period of time.

9.7 To ensure that the employees meet the required standard of competence, the FSC Handbook provides a non-exhaustive list of requirements under Chapter 12.4 that must be considered by the Company prior to the on-boarding of the employee, these include:

- obtaining and confirming details of employment history, qualifications and professional memberships;
- obtaining and confirming appropriate references;
- obtaining and confirming details of any regulatory action or action by a professional body taken against the prospective employee;
- obtaining and confirming details of any criminal convictions, including the provision of a check of the prospective employee's criminal record; and (e) screening the employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions

9.8 The frequency of the screening of employees shall be at least on an annual basis.

Training

9.9 An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analysing potential illicit transactions. Therefore, in accordance with Regulation 22 1(b) of the FIAML Regulations, the Company is shall ensure that appropriate training is conducted with directors and all relevant employees (on an ongoing basis) to equip them to perform their obligations in respect of AML/ CFT requirements.

9.10 An on-going training program must be established to ensure that all relevant employees:

- maintain and enhance their AML/CFT knowledge, skills and abilities;
- are kept up to date with new AML/CFT developments, including the latest ML, TF and PF techniques, methods, and trends; and
- are trained on any changes made to the Company's AML/CFT policy, procedures, and controls.

9.11 The Company shall ensure that the training program is tailor made for each of its department and consistent with the level of seniority of employees. The method of training adopted includes in house trainings, workshops, webinars, email and/or periodic meetings. The Company will ensure that all relevant staff duly understand their role in at each level. This shall include ensuring that the Compliance Officer, MLRO and DMLRO complete at least 10 hour of training/CPD points on an annual basis in accordance with relevant provisions of the competency standards issued by the FSC.

9.12 The Compliance Officer shall ensure training is undertaken periodically, and/or at least annually. This is to ensure that employees are kept up-to-date and aware of AML/CFT developments so that the relevant person is able to manage and mitigate the money laundering, terrorism financing and proliferation financing risks.

9.13 The Company shall ensure that all records of training conducted and attended are duly kept. Chapter 8 of the FSC Handbook details the record keeping requirement for the training delivered to the employees. These are listed below:

- the dates on which the training was provided.
- the nature of the training, including its content and mode of delivery
- the names of the employees who received the training.

9.14 The effectiveness of each training conducted shall be evaluated to measure the understanding of the employees post the trainings. The evaluation enables the Company to:

- identify the gaps and ensure that adequate time and resources are allocated for more focused trainings;
- monitor the quality of reports of the relevant employees;

Compliance Officer

9.15 The functions of the Compliance Officer include—

(a) ensuring continued compliance with all AML/CFT legal and regulatory requirements subject to the ongoing oversight of the board of the Company and senior management;
(b) undertaking day-to-day oversight of the AML/CFT program of the Company;
(c) regular reporting annually, including immediate reporting of non-compliance, to the board and senior management; and
(d) contributing to designing, implementing, and maintaining internal compliance manuals, policies, procedures, and systems for combatting money laundering, the financing of terrorism and proliferation.

9.16 The compliance officer shall:

- ✓ submit quarterly reports to the Board or any committee established by the Board for purposes of overseeing the management of compliance in the entity;
- ✓ report on an ongoing basis to the Senior Management on all AML/CFT compliance related issues relevant to the Company and any other matters relevant to the responsibilities of the compliance function;
- ✓ submit compliance monitoring plans to Senior Management and the Board, including specific annual or other short-term goals being pursued and the performance against such goals;
- ✓ submit information on its resources, including an analysis on the appropriateness of those resources to the Board on a quarterly basis;
- ✓ escalate any matters that may require the attention of or a decision by Senior Management without delay.

9.17 All officers and employees of the Company are required to cooperate and collaborate with the compliance officer.

9.18 Where the compliance officer identifies weaknesses within the monitoring arrangements, he should ensure that these are rectified in a timely manner.

Compliance Reviews

9.19 Under Regulation 31 of the FIAMLR 2018, the Company shall establish and maintain appropriate procedures for monitoring and testing compliance with the AML/CFT requirements, having regard to ensuring that –

- the Company has robust and documented arrangements for managing the risks identified by its business risk assessment conducted in accordance with section 17 of the FIAMLA for compliance with those requirements
- the operational performance of those arrangements is suitably monitored and
- prompt action is taken to remedy any deficiencies in arrangements.

9.20 The Compliance Officer shall be responsible for ongoing monitoring of the implementation of the measures, policies, controls and procedures adopted to ensure the Company's compliance with its AML/CFT obligations.

9.21 The Compliance Officer shall ensure the effectiveness of AML/CFT controls applied by business lines.

9.22 The Compliance Officer shall carry out sample testing to establish levels of compliance. Sample testing of customer data shall be conducted as follows-

Level of risk of customer	Frequency of review
Low	Annually
Medium	Semi-annually
High	Quarterly

9.23 The Compliance Officer shall ensure that the AML/CFT programme is assessed periodically and updated where necessary and, in any case, where deficiencies are detected, new risk emerge, or the legal or regulatory framework has changed.

9.24 The Compliance Officer shall have access to, and familiarise himself with, the results and output from the Company's monitoring processes. Such output shall be reviewed by the Compliance officer who in turn shall report regularly to the board, providing relevant management information, together with details of any trends and actions taken where concerns or discrepancies have been identified.

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

Independent Audit

9.26 In accordance with regulation 22 1(d) of the FIAML Regulations, the Company shall have in place an audit function which will allow evaluation of its AML/CFT programme and ascertain whether the established policies, procedures, systems, and controls are adapted with the money laundering and terrorism financing risks identified.

9.27 The Company shall ensure that the audit is tailor made to its requirements and should be risk-based. Chapter 13.2 FSC Handbook provides guidance on the scope of an audit, they are as follows:

- AML/CFT policies and procedures
- Internal risk assessment
- Risk assessment on the use of third-party service providers (Outsourcing)
- Compliance Officer function and effectiveness
- MLRO function and effectiveness
- Implementation and Effectiveness of Mitigating Controls including customer due diligence and enhanced measures
- Record keeping obligations
- Targeted Financial Sanctions
- Suspicious transaction monitoring and reporting
- AML/CFT training

9.28 The Company must ensure that the audit is carried out by an independent firm or person. In other words, the firm or person conducting the audit should not have been part of the establishment of the Company's AML/ CFT risk assessment, or the establishment, implementation, or maintenance of its AML/CFT programme. It important that the firm/person conducting the audit demonstrate the necessary skills, qualifications and has the experience as well as a thorough understanding of the legislations.

9.29 The frequency and extent of the audit must take into consideration the size, nature, context, complexity, and internal risk assessment of the Company. When determining the frequency of the audit.

9.30 The FSC Handbook provides that Financial Institutions should conduct an audit at a minimum annually or whenever material changes to the financial institution or legislative and regulatory obligations occur.

9.31 The audit report shall be considered and discussed by the Board at a meeting immediately after the submission of the report by the independent auditor and the Board shall ensure that immediate remedial actions are taken where required. The Compliance Officer shall submit regular reports to the Board on the status of the implementation of the remedial actions.

9.32 The Company shall ensure that the audit report, including all the documented workings are made available to the Financial Services Commission (FSC) upon request.

10. Record Keeping

10.1 In accordance with section 17F of the FIAMLA, the Company shall maintain books and records with respect to his customers and transactions as follows. Senior management shall with the approval of the Board make such arrangements whether electronic or physical as the Board deems appropriate for keeping and maintaining records.

10.2 Where the Board decides to keep records electronically it shall ensure that the relevant guidelines as specified in the FSC Handbook are adhered to. This shall include account files, business correspondence and results of any analysis undertaken in accordance with requirements of the FIAMLA 2002.

10.3 Senior management shall ensure that all CDD information and transaction records are kept in form and manner –

- That they can be made swiftly available to the FIU or any relevant regulatory body or supervisory authority or the other competent authority upon request;
- To enable the prompt reconstruction of each individual transaction;
- That when responding to a request under section 13(2) of the FIAMLA, the Company is able to provide for each transaction record the full name of the party making a payment; and the full name of the party receiving a payment.

CDD Records

10.4 The Company shall maintain all records obtained through CDD measures, including account files, business correspondence and copies of all documents evidencing the identity of customers and beneficial owners, and records and the results of any analysis/assessment undertaken in accordance with the FIAMLA, all of which shall be maintained for a period of not less than 7 years after the business relationship has ended.

Transaction Records

10.5 The Company will maintain records on transactions, both domestic and international, that are sufficient to permit reconstruction of each individual transaction for both account holders and non-account holders for a period of 7 years after the completion of the transaction.

10.6 The business unit handling the transaction will be responsible for keeping the following information for every transaction carried out in the course of a business relationship or occasionally:

(a) the name and address of the customer;
(b) if a monetary transaction, the kind of currency and the amount;
(c) if the transaction involves a customer's account, the number, name or other identifier for the account;
(d) the date of the transaction;
(e) details of the counterparty, including account details;
(f) the nature of the transaction; and
(g) details of the transaction.

Records of Suspicious Transaction Reports

10.7 The Company will maintain copies of all suspicious transaction reports made pursuant to section 14 or other reports made to FIU in accordance with the FIAMLA, including any accompanying documentation for a period of at least 7 years from the date the report was made.

Audit and Compliance Reports

10.8 Senior management shall ensure that records of audit or compliance reports are kept for such duration as the Board may determine.

Training records

10.9 The HR officer shall be responsible for keeping all AML/CFT training records as follows:

(a) Dates when AML/CFT training provided to employees and officers
(b) Nature and contents of the training
(c) Name of employees and officers who attended the training
(d) The name and bio of the trainer/facilitator/resource person

Employees should be aware of section 19(b) of the FIAMLA. Please refer to **Annex 2**.

Suspicious Transaction Reporting

11. What is a suspicious transaction?

11.1 Under section 14 of the FIAMLA the Company has the obligation to make a suspicious transaction report to the FIU as soon as he becomes aware of the suspicious transaction but no later than 5 working days after the suspicion arose.

11.2 A suspicious transaction is defined under section 2 of the FIAMLA as follows-

Section 2 FIAMLA- Definition of "suspicious transaction"

"suspicious transaction" means a transaction which –

a. gives rise to a reasonable suspicion that it may involve–
   i. the laundering of money or the proceeds of any crime; or
   ii. funds linked or related to, or to be used for, 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.

11.3 The term "transaction" is also defined under section 2 of the FIAMLA-

Section 2 FIAMLA- Definition of "transaction"

"transaction" includes -

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

b a proposed transaction or an attempted transaction

Money Laundering Reporting Officer and Deputy Money Laundering Reporting Officer

11.4 The Company has in accordance with Regulation 26(1) and (2) of the FIAMLR 2018 appointed a Money Laundering Reporting Officer (MLRO) and Deputy Money Laundering Reporting Officer (DMLRO). The DMLRO performs the duties of the MLRO in his absence.

11.5 Regulation 26 (4) of the FIAMLR 2018, requires that the Money Laundering Reporting Officer and the Deputy Money Laundering Officer shall —

- be sufficiently senior in the organization of the reporting person or have sufficient experience and authority; and
- have a right of direct access to the board of directors of the reporting person and have sufficient time and resources to effectively discharge his functions.

11.6 Directors and employees of the Company have the obligation to report any suspicious transaction that they may come across to the MLRO or the DMLRO in the absence of the MLRO.

11.7 Employees should be aware of Section 14(3) of the FIAMLA which reads as follows-

Section 14 (3) 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 fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Internal reports

11.8 A suspicious transaction can be identified both during the on-boarding or ongoing due diligence of a customer as well as during the transaction monitoring process.

11.9 Any employee of the Company who comes across a suspicious transaction must make an internal report to the MLRO and in his absence to the DMLRO.

11.10 Employees should be aware that the term "transaction" as defined under the FIAMLA includes a proposed transaction or attempted transaction.

11.11 The reporting requirement for reporting a suspicion stem from Regulation 26(1) of the FIAMLR 2018 which reads as follows-

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

11.12 A suspicion may arise as a result of the general behavior of the person in question which creates the knowledge or belief that he may be involved in illegal activities out of which revenue might be generated.

11.13 A suspicion may arise from a specific transaction, which creates the knowledge or belief that the transaction may relate to ML, TF, PF or proceeds of crime.

11.14 Where an employee identifies any suspicious activity in the course of a business relationship or occasional transaction the employee must

a. consider obtaining enhanced CDD in accordance with these procedures; and
b. make an internal disclosure in accordance with the procedures established under this Manual.

11.15 Where an employee identifies any unusual activity in the course of a business relationship or occasional transaction the employee must -

a. perform appropriate scrutiny of the activity;
b. obtain enhanced CDD in accordance with these procedures; and
c. consider whether to make an internal disclosure in accordance with the reporting procedures established under this Manual.

11.16 In order for a report to be useful for analysis and processing, it needs to be a quality report, that is, the information submitted must be sufficient and complete to enable a connection to be made between the person(s) and the suspicious activity/transaction.

11.17 All employees must ensure that reports of internal disclosures made to the MLRO/DMLRO contain any information or other matters that come to the attention of the employee handling that business and which in the employee's opinion gives rise to any knowledge or suspicion that another person is engaged in money laundering and terrorism financing activity.

11.18 Where an internal disclosure has been made, the MLRO/DMLRO he must assess the information contained within the disclosure to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to money laundering, terrorism financing or proliferation financing.

11.19 It is the duty of the MLRO or DMLRO to consider any report in the light of all relevant information available to him to determine whether or not it gives rise to any knowledge or suspicion of money laundering or terrorism financing or proliferation financing.

11.20 For this purpose, the MLRO/DMLRO will have full access to any other information that may be of assistance and that is available to Company. Every employee in the Company who hold or has in his possession any information that may be relevant to the MLRO/DMLRO must provide such information to the MLRO/DMLRO upon his request.

Procedure For Filing of STRs

11.21 In the event where an employee of the Company has a suspicion and needs to file a Suspicious Transaction Report, he or she should refer to the below procedure:

External reports

11.22 The MLRO/DMLRO must forthwith make a report in accordance with section 14 of the FIAMLA to the FIU where he knows or has reason to believe that an internal disclosure may be suspicious.

11.23 The MLRO must ensure that the filing of a suspicious transaction report is done through the 'GoAML system', which is the IT system that must be used to submit STRs with the FIU.

11.24 Where the MLRO/DMLRO knows or suspects that another person is engaged in money laundering or terrorism financing or proliferation activities he must as soon as practicable submit all the information or other matters contained in a report to the FIU.

Tipping Off

11.25 The MLRO/DMLRO and every director and employee of the Company should be aware of section 16 (1) of the FIAMLA which is reproduced below.

> Section 16(1) FIAMLA
> Any reporting person and auditor, and any of their officers shall not disclose to any person that a suspicious transaction report is being or has been filed, or that related information is being or has been requested by, furnished, or submitted to FIU.

11.26 Failure to comply with the obligation under section 16(1) of the FIAMLA is a criminal offence under section 16(3) of the FIAMLA. Upon conviction, a person shall be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

Registration with the FIU

11.27 The MLRO/DMLRO shall in accordance with section 14C of the FIAMLA and Regulation 3 of the FIAMLR 2019 make an application for registration by the FIU.

11.28 The MLRO/DMLRO shall immediately inform senior management if the FIU rejects the application for registration.

11.29 It is the duty of Senior Management to ensure that all remediation action as required by the FIU are put in place to ensure that the Company is registered by the FIU as required under section 14C of the FIAMLA.

11.30 Failure to comply with the obligation under section 14C of the FIAMLA is a contravention under section 32A of the Act. Upon conviction, a person is liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Other duties of the MLRO/DMLRO

11.31 It is the responsibility of the MLRO/DMLRO to -

- ensure that the suspicious activity monitoring and reporting policy of the Company is effective; and
- create and maintain a culture of compliance and ensure that employees adhere to the Company's policies, procedures and processes designed to limit and control risks.

Periodic Report to the Board

11.32 The MLRO shall submit an annual report, or such other periodic reports as may be required by the Board.

Registers of Internal and External disclosures

11.33 It is the responsibility of the MLRO and in his absence the DMLRO to, in accordance with Regulation 30 (1) of the FIAMLR 2018 establish and maintain separate registers of all internal disclosures and external disclosures. The registers must include details of—

The date on which the report is made.	✓
The person who makes the report.	✓
For internal disclosures, whether it is made to the MLRO or DMLRO.	✓
Information sufficient to identify the relevant papers.	✓
Assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek additional information.	✓
The rationale for deciding whether or not to proceed with an external report.	✓

Potential Red Flags

11.34 The FSC Handbook provides is a non-exhaustive list and its content is purely provided to reflect examples of possible ML and TF red flags that the Company should be mindful of when dealing with a business relationship or occasional transaction.

11.35 Business units as well as the officers of the Company shall familiarize themselves with the potential red flags contained in the FSC Handbook.

12. Targeted Financial Sanctions

12.1. In May 2019, Mauritius enacted the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act (the UNSA) which provides a legal framework for the implementation of targeted financial sanctions and other measures imposed by the United Nations Security Council (Security Council) under Chapter VII of the Charter of the United Nations (UN) in response to threats to international peace, breaches of the peace, and acts of aggression.

12.2. The Security Council can take action to maintain or restore international peace and security under Chapter VII of the UN Charter. Sanctions measures, under Article 41 of the UN Charter, encompass a broad range of enforcement options, including imposing sanctions, that do not involve the use of armed force. Security Council sanctions have taken a number of different forms, and the measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. There are currently 14 sanctions regimes which focus on supporting political settlement of conflicts, nuclear non-proliferation, and counterterrorism by virtue of the following United Nations Security Council Resolutions (UNSCR) and their respective successor resolutions, as set out in the Second Schedule of the UNSA –

	Year Adopted	UNSCR	Description
1	1992	UNSCR 751	concerning the situation in Somalia
2	1999 and 2011	UNSCR 1267 and 1989	concerning ISIL (Da'esh), Al-Qaida and associated individuals groups undertakings and entities
3	2003	UNSCR 1518	concerning Iraq
4	2004	UNSCR 1533	concerning the Democratic Republic of the Congo
5	2005	UNSCR 1591	concerning Sudan
6	2005	UNSCR 1636	concerning Lebanon
7	2006	UNSCR 1718	concerning Democratic People's Republic of Korea (DPRK)
8	2011	UNSCR 1970	concerning Libya
9	2011	UNSCR 1988	concerning individuals, groups, undertakings and entities associated with the Taliban in constituting a threat to the peace, stability and security of Afghanistan
10	2012	UNSCR 2048	concerning Guinea-Bissau
11	2013	UNSCR 2127	concerning the Central African Republic
12	2014	UNSCR 2140	concerning Yemen
13	2015	UNSCR 2206	concerning South Sudan
14	2017	UNSCR 2374	concerning Mali

12.3. Each sanctions regime is administered by a sanctions committee chaired by a non-permanent member of the Security Council.

12.4. UNSCR 2231(2015) provides for the termination of the provisions of previous Security Council resolutions on the Iranian nuclear issue and for specific sanctions measures that apply to targeted individuals and entities under the UN 2231 list.

12.5. Other than the UNSCR 2048 (2012) concerning Guinea-Bissau; all the other UN Sanctions Regimes and UNSCR 2231(2015) comprise, at a minimum, an arms embargo, targeted financial sanctions and a travel ban.

12.6. In the aftermath of the 11 September attacks against the United States in 2001, the Security Council unanimously adopted UNSCR 1373 (2001), requiring all UN Member States to criminalize various acts associated with terrorism, as well as the financing of such acts. The resolution emphasizes the need to bring terrorists to justice through effective criminalization and requires that Member States set up effective mechanisms to freeze funds, financial assets and economic resources of persons involved in or associated with terrorism, as well as to prevent those funds from being made available to terrorists.

12.7. A complementary requirement to the asset-freezing requirement under the UN Sanctions regimes and UNSCR 1373 (2001) is to prohibit any person from making funds, financial assets or economic resources and other related services available to a designated party.

Definition and Scope of Targeted Financial Sanctions

12.8. Amongst the restrictive measures imposed by the Security Council, reporting persons are primarily concerned with the implementation of targeted financial sanctions. In response to the threat against international peace and security, the Security Council imposes targeted financial sanctions under 13 out of the 14 ongoing sanctions regimes. Please refer to **Annex 1** for a summary of all the UN Sanctions Regimes.

12.9. Targeted financial sanctions also apply under UNSCR 1373(2001) and 2231 (2015).

12.10. The term “targeted financial sanctions” as defined by the FATF means both asset freezing and prohibitions to make funds or other assets available, directly or indirectly, for the benefit of designated persons and entities.

12.11. The UNSA provides the legal framework for the implementation of targeted financial sanctions against persons and entities designated domestically as well as under the UN sanctions regime.

National Sanctions Committee and National Sanctions Secretariat

12.12. Section 7 of the UNSA establishes the National Sanctions Secretariat (NSSec) which is the focal point for UN sanctions related matters in Mauritius. It supports the work of the National Sanctions Committee (NSC) which is established under section 4 of the UNSA. Among others, the NSC is the competent authority for-

(a) proposing to the relevant UN Sanctions Committee targets for designation;
(b) making decisions in relation to the declaration of a person or entity pursuant to UNSC 1373 (2001).
(c) coordinating and promoting effective implementation of the obligations under the United Nations Security Council Resolutions in Mauritius;
(d) coordinating the development of, review and implement national policies and activities for the effective implementation of UNSC Resolutions;
(e) coordinating international cooperation in the cross-border implantation of the UNSC Resolutions between Mauritius and other countries and foreign counterpart agencies; and
(f) approving guidelines developed by the National Sanctions Secretariat.

12.13. The UNSC has imposed sanctions to prevent and counter terrorism and terrorism financing and the proliferation of WMD ('Weapon Mass Destruction'), and its financing.

12.14. This includes targeted financial sanctions against specific persons and entities that have been identified as being connected to terrorism, terrorism financing and the proliferation of WMD. All UN member states are required to implement these measures.

Designation of persons and entities

12.15. Persons and entities (parties) subject to targeted financial sanctions may be designated domestically pursuant to sections 9 or 10 of the Act and internationally by or under the authority of the United Nations Security Council (UNSC).

Domestic Designations and Domestic List of Designated parties

12.16. The Act provides a legal framework for the freezing of terrorist funds and assets pursuant to UNSCR 1373 (2001) and establishes a designating mechanism with adequate due process consideration, as well as a dedicated mechanism to address foreign asset-freezing requests. The obligation to freeze, without delay, funds and assets linked to terrorist organizations or individual terrorists is a key element of UNSCR 1373 (2001). The resolution requires that States should be able to freeze funds, other financial assets or economic resources of persons and entities listed domestically without delay.

12.17. Designations pursuant to UNSCR 1373 (2001), are made pursuant to sections 9 and 10 of the Act. For this purpose, the National Sanctions Secretariat must, in accordance with section 12 of the Act, keep and maintain a list of parties declared as designed parties (the domestic list).

Designations by or under the authority of the Security Council

12.18. The names of parties designated by or under the authority of the Security Council are available on the relevant UN Sanctions List as maintained by the relevant United Nations Sanctions Committee or the Consolidated Sanctions List.

12.19. The Consolidated List includes all parties subject to measures imposed by the Security Council. The inclusion of all names on one Consolidated List is to facilitate the implementation of the measures does not imply that all names are listed under one UN sanctions regime. For each instance where the Security Council has decided to impose measures in response to a threat, a Security Council Committee manages the sanctions regime. Each sanctions committee established by the UNSC therefore publishes the names of individuals and entities listed in relation to that committee as well as information concerning the specific measures that apply to each listed name.

12.20. The current version of the Consolidated UNSC List and the UN Sanctions Lists are provided in .xml, .html and pdf formats.

12.21. Of note, the terms "designated party" and "listed party" are defined under section 2 of the Act and apply to parties identified under the domestic process and UN Sanctions regime respectively.

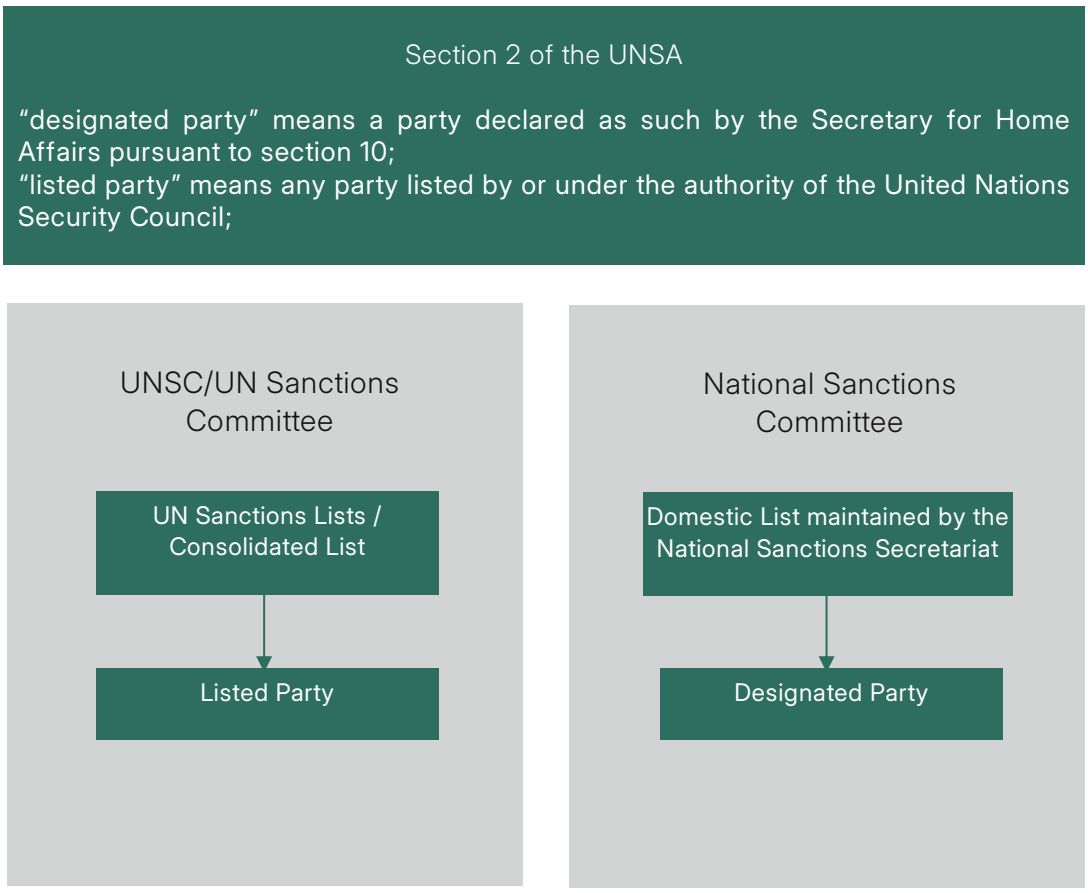


Figure 6 Designation of Parties

12.22. In response to the terrorism and terrorism financing threats, the UNSC imposes TFS related to terrorism financing under the ISIL (Da'esh) and the 1988 sanctions regimes.

The ISIL (Da'esh) and Al-Qaida sanctions list and the 1988 sanctions list contains the names of the persons and entities currently listed under the two sanctions regimes.

12.23. With regard to identified WMD proliferation threats, the UNSC currently imposes TFS related to proliferation under the following sanctions regimes:

12.23.1. Islamic Republic of Iran – UNSC Resolution 2231 (2015) replaced all previous UNSC Resolutions related to Iran and WMD proliferation, and imposes assets freeze measures against certain individuals and entities. The assets freeze measures will apply until October 2023 or earlier as provided in the UNSCR.

12.23.2. The 2231 List contains the names of the persons and entities listed under UNSC Resolution 2231.

12.23.3. Democratic People's Republic of Korea (DPRK) – UNSC Resolution 1718 (2006) and all successor resolutions related to the DPRK.

12.23.4. The 1718 List contains the names of the persons and entities currently listed related to DPRK.

Prohibition to deal with and make funds or other assets available

12.24. In Mauritius TFS measures are implemented through Section 23 and Section 24 of the UNSA.

12.25. Mauritius implements the assets freeze measures under the UN sanctions regimes and UNSCR 1373 through section 23(1) of the UNSA. Where a dissemination is made under section 11(1) or 18(1) of the UNSA, the prohibition to deal with the funds and other assets of a listed party under section 23(1) of the Act applies immediately (see definition below). The terms "deal" and "immediately" are defined under section 2 of the UNSA. Employees should pay particular to the definition of these two terms.

Section 23(1) of the UNSA

No person shall deal with the funds or other assets of a listed party, including:

a) All funds and other assets that are owned or controlled by the designated or listed party,

b) Those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated or listed party;

c) Funds or other assets derived or generated from funds or other assets, owned, or controlled directly or indirectly, by the designated or listed party, and

d) Funds or other assets of a party acting on behalf of, or at the direction of, the designated or listed party.

Section 24 of the UNSA

No person shall make any funds or other assets or financial or other related services available, directly, or indirectly, or wholly or jointly, to or for the benefit of:

a) A listed party;

b) A party acting on behalf, or at the direction, of a listed party; or

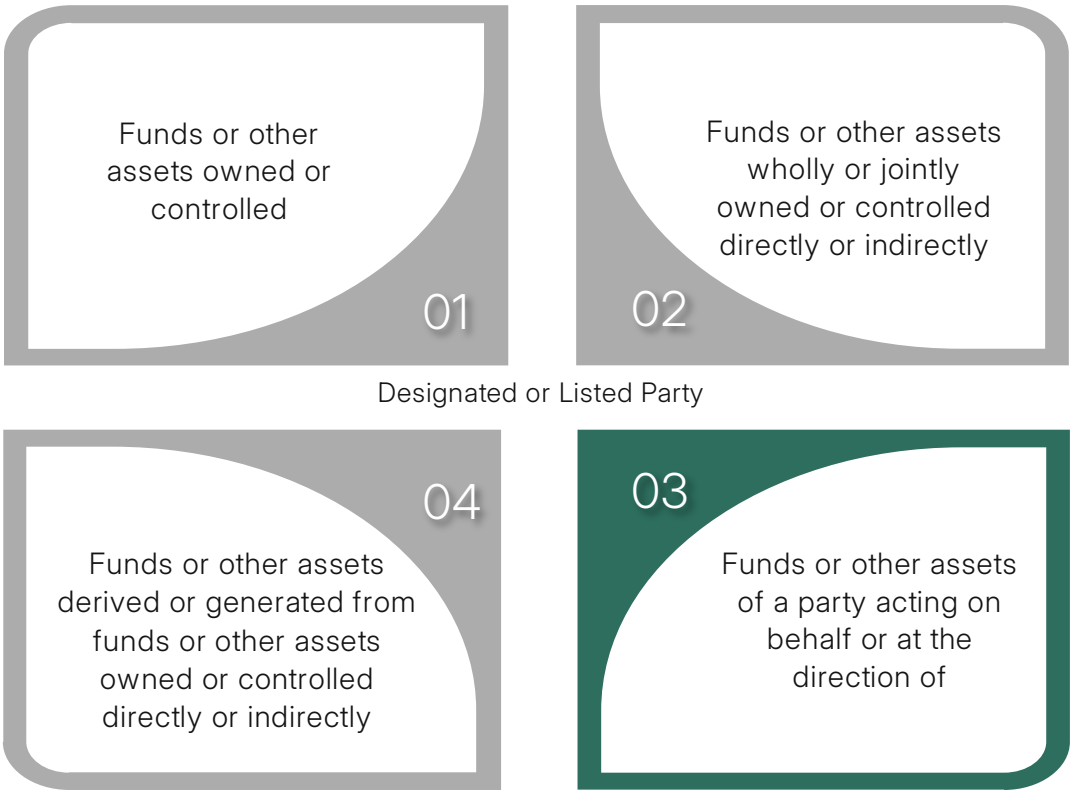
c) An entity owned or controlled, directly or indirectly, by a listed party

Section 2 of the UNSA

"deal" includes to sell, supply, lease, transfer, convert, dispose, move, use, or withdraw.

"immediately" means without delay and not later than 24 hours.

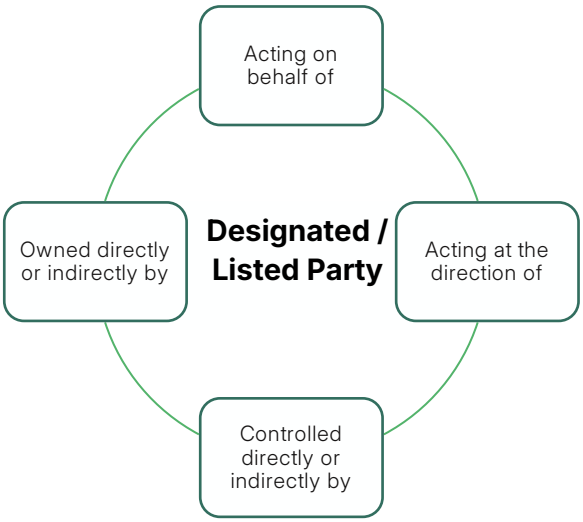
12.26. TFS implementation should not only focus on the funds or assets held by a designated or listed party but to funds and other assets as described under section 23(1)(a) to (d) of the UNSA.



12.27. It is important to note that TFS provisions are applicable to designated and listed parties as well as those who are:

- Acting on behalf of or at the direction of listed persons or entities.
- Owned or controlled by listed persons or entities.

12.28. As a result, TFS implementation should not only focus on the names of persons and entities listed on UNSC lists, but also identify the persons and entities linked to them.



12.29. Employees should also be aware of the definitions of 'funds', 'assets' and 'economic resources', as they may determine, and potentially expand, the scope of TFS implementation beyond just financial transactions and funds.

Section 2 of the UNSA

"funds or other assets" means-

b. any assets, including, but not limited to, financial assets, economic resources and property of every kind, whether tangible, intangible, movable or immovable, however acquired;
c. legal documents or instruments in any form-
   i. including electronic or digital, evidencing title to, or interest in, such funds or other assets; and
   ii. including, but not limited to, bank credits, traveler's cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit

d. any interest, dividends, or other income on or value accruing from or generated by such funds or other assets, virtual or digital currencies, including cryptocurrencies
e. any other assets which potentially may be used to obtain funds, goods, or services

"Economic resources" includes assets of every kind, whether movable, immovable, tangible, intangible, actual or potential, which are not funds but potentially may be used to obtain funds, goods, or services, such as –

(a) land, buildings and other real estate;
(b) equipment, including computers, computer software, tools, and machinery;
(c) office furniture, fittings and fixtures and other items of a fixed nature;
(d) vessels, aircraft and motor vehicles;
(e) inventories of goods;
(f) works of art, precious stones, jewellery and gold;
(g) commodities, including oil, minerals and timber;
(h) arms and related materiel;
(i) patents, trademarks, copyrights, trade names, franchises, goodwill and other forms of intellectual property;
(j) internet hosting and other related services used for the support of listed parties;
(k) direct and indirect trade in oil and refined products, modular refineries and related material, including chemicals and lubricants and other natural resources;
(l) any other assets, whether tangible, intangible, actual or potential

Freezing order

12.30. With regard to a domestic designation, section 26(1) of the Act provides that where he declares a party as a designated Party, the Secretary for Home Affairs must within a reasonable time apply for a freezing order of the funds or other assets of the designated party. Once the freezing order is granted, section 34(2) of the Act provides that the prohibition under section 23 shall lapse. However, the prohibition under section 24 of the Act will continue to apply.

Variation order

12.31. A designated party may access assets subject to a freezing order for ordinary or extra ordinary expenses if approved by a Designated Judge. A Designated Judge may, under section 27 of the Act, grant a variation of the freezing order to authorize a designated party to use funds or other assets subject to a freezing order.

Exemptions to the prohibitions

12.32. Despite the expanded scope of which persons and entities, and what funds and assets, are covered by TFS implementation, there are also important exceptions to TFS which should be consulted. This includes the ability for a designated or listed party to access assets under limited circumstances, including the provision of basic living expenses, or extraordinary expenses if approved by UNSC committees for the UN sanctions regimes (see sections 30 and 31 UNSA) or by a Designated Judge for designations pursuant to UNSR 1373 (see section 27 UNSA). For UNSC Resolution 2231 on Iran, certain payments due under contracts entered prior to a party being listed can also be approved. See Section 4 below for more details.

12.33. Section 23(3) of the UNSA also has a specific exemption relating to Iran. It states that the National Sanctions Committee may authorize the listed party to make any payment due under a contract, an agreement or an obligation entered prior to the listing of such party.

12.34. All authorization and exemption requests should be submitted to the National Sanctions Secretariat: nssec@govmu.org

Additions to frozen accounts

12.35. Pursuant to sections 23(2) and 26(2) of the UNSA where a prohibition or a freezing order is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a designated party or a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition or freezing order, provided that any such interest, earnings and payments continue to be subject to the prohibition or freezing order.

Obligations of reporting persons

12.36. As stated in Section 41 of the UNSA, reporting persons are required to implement internal controls and other procedures to effectively comply with their obligations under the Act, including counter proliferation financing obligations.

12.37. The UNSA also establishes several reporting obligations which reporting persons must implement. The internal controls and procedures required for implementation are outlined below.

Dissemination and consultation of sanctions lists and declaration

12.38. The NSSec has, under section 18(1) of the UNSA, the responsibility to immediately give public notice of any changes to any UN sanctions lists. This includes new designations, changes to existing designations, and removed designations. Similarly, the NSSec has, under section 11(1) of the UNSA, the responsibility to give public notice of any declaration made under section 9 or 10 of the UNSA.

12.39. All updates to sanctions lists are posted on the NSS's website: http://nssec.govmu.org.

12.40. Following the dissemination of the lists or declaration, the Company must monitor and immediately implement any changes to UN sanctions lists or a declaration and must not deal[6] with or make funds or other assets available to a designated party or listed party.

12.41. Sanctions lists may also be consulted directly with the UNSC, or with the FIU who acts upon the direction of the NSS. Under sections 11(1)(b) and 18(1)(b) of the UNSA, the FIU must disseminate a declaration or the public notice issued by the NSSec, UN sanctions lists as well as any changes thereto to the supervisory authorities, the investigatory authorities, the reporting persons and any other relevant public or private agency.

Sanctions Screening

12.42. Sanctions apply to all customers and transactions, and there is no minimum financial limit or other threshold for when to conduct screening. Section 25 of the UNSA requires that when a party is declared as a designated party or listed as a listed party, every reporting person shall, immediately, verify whether the details of the designated party or listed party match with the particulars of any customer, and if so, to identify whether the customer owns any funds or other assets in Mauritius.

12.43. The business unit of the Company must therefore screen all customers and transactions for potential matches.

Customer screening

12.44. The Company has implemented the BEX/KnowMeKnow IT solution to screen customers during on boarding and through the life cycle of the customer relationship. The screening should also extend to directors and beneficial owners of corporate customers, and any other parties with access to the account. The business unit must screen customers when establishing a new relationship, and at regular intervals either upon a trigger event (change in directors or ownership) or when a sanctions list changes.

[6] Under section 2 of the UNSA the term "deal" includes to sell, supply, lease, transfer, convert, dispose, move, use, or withdraw.

Transaction monitoring

12.45. Each incoming and outgoing transaction must be screened for a potential match with UN sanctions lists or domestic designations and all screening must be conducted prior to completing a transaction.

Sanctions Match and Resolving False Positives

12.46. Screening is the comparison of one string of text against another to detect similarities which would suggest a potential match. If a match is detected, and the Company maintains accounts, or otherwise holds or controls funds and other assets for designated or listed parties (or anyone owned or controlled by designated or listed parties, or acting on their behalf of for their benefit), the employee should immediately:

- Not deal with those funds and other assets.
- Not make funds and other assets available to or for the benefit of listed parties.
- Investigate further.

12.47. If an alert is generated with a potential match, this is not an automatic indication of a sanction's violation. It should be confirmed or discounted with additional information gained through further investigation.

12.48. Determining a true match can often prove difficult due to a range of variables including language, spelling, abbreviations, and aliases. UN sanctions lists are provided with other identifying information to assist in the identification of a true match or false positive.

12.49. In cases where no match is obtained after verification of the customer data base following a notice received from the FIU pertaining to a change on the UN Sanction list, the Company shall make a NIL report to the NSSec and put the relevant email address of the FSC in copy.

Sanctions Reports

12.50. If a true match is identified, the MLRO/DMLRO will be responsible for submitting a report to the NSSec, and in some cases also to the Financial Services Commission. The specific reporting obligations contained in the UNSA are outlined below.

12.51. Reports may be completed using the template which can be downloaded from the NSSec website: http://nssec.govmu.org

12.52. Reports must be submitted to the following email address: nssec@govmu.org

Rights of bona fide third parties

12.53. Safeguards for the rights of bona fide third parties are provided for under sections 28 and 29 of the UNSA. Accordingly, any freezing order or prohibition under the Act applies without prejudice to the rights of bona fide third parties.

12.54. Pursuant to section 28(1) of the UNSA, any person who has an interest in any funds or other assets which is subject to a freezing order may apply to the Designated Judge to exclude his interest from the freezing order.

12.55. Where such an application is granted, the order will be publicised by the Secretary for Home Affairs and any person who holds, controls or has in his custody or possession funds or other assets of a bona fide third party must immediately comply with the order granted by a Designated Judge. Failure to comply with the order is, under section 28(6) of the Act, an offence punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

12.56. In accordance with section 29(1) of the UNSA, any person who has an interest in any funds or other assets which is subject to a prohibition under the Act may apply to the NSC to exclude his interest from the prohibition.

12.57. An order from the NSC to vary the prohibition will be publicised by the Secretary for Home Affairs. Any person who holds, controls or has in his custody or possession funds or other assets of a bona fide third party must immediately comply with the order of the NSC. Failure to comply with the order is, under section 29(6) of the Act, an offence punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Lapse of Freezing Orders and Prohibitions

12.58. Where the name of designated party has been removed from the list of designated party or where the name of a listed party has been removed from the relevant UN Sanctions List, any freezing order against the designated party or the prohibitions against the listed party lapses with immediate effect. In such cases, the Company must in accordance with section 34(1)(a) of the Act, immediately unfreeze any funds or other assets, it holds, controls or has in his custody or possession, that belongs to the designated party or listed party.

Record keeping

12.59. The Company shall establish and maintain records of all alerts and outcome and analysis of all investigations related to the alerts.

12.60. The record keeping requirements under the FIAMLA shall equally apply in the context of targeted financial sanctions.

Training

12.61. The Company believes that an effective training program is an integral component of a successful sanctions compliance programme.

12.62. An ongoing training programme shall be developed and provided to all appropriate employees and personnel on a periodic basis and at a minimum, annually.

12.63. The training programme should generally accomplish the following:

- provide job-specific knowledge based on need;
- communicate the sanctions compliance responsibilities for each employee; and
- hold employees accountable for sanctions compliance training through assessments

Suspicious Transaction Reports

12.64. In addition, Section 39 of the UNSA states that any information related to a designated party or listed party shall be immediately submitted by the reporting person to the FIU or by any other person in writing to the FIU.

12.65. The MLRO/DMLRO will be responsible for submitting any information related to a designated party or listed party to the FIU.

12.66. The MLRO/DMLRO must keep a record of all reports submitted pursuant to the UNSA.

Penalties for non-compliance with sanctions requirements under the UNSA

12.67. Some of the penalties for failure to comply with the requirements of the UNSA are set out in the table below. In addition, the Company may be subject to regulatory action by the FSC.

12.68. The FSC is required to ensure strict compliance with the requirements imposed under the UNSA and is empowered to take necessary action for the implementation of the freezing order and financial prohibitions thereunder. Pursuant to section 40(2) of the UNSA, the FSC has the mandate to supervise and enforce compliance with the requirements under the Act.

Relevant obligation in UNSA	Description	Sanctions for non-compliance
Section 23(4)- Notification of compliance with prohibition to deal requirement	Details of any funds or other assets subject to a prohibition to deal under section 23(1) of the Act must be immediately reported to the National Sanctions Secretariat in terms of section 23(4) of the Act. The report must provide- a) Details of the funds or other assets against which action was taken in accordance with section 23(1) of the Act; b) The name and address of the designated or listed party; c) Details of any attempted transaction involving the funds or other assets, including – i. The name and address of the sender ii. The name and address of the intended recipient iii. The purpose of the attempted transaction iv. The origin of the funds or other assets v. Where the funds or other assets were intended to be sent Reporting persons can use the template provided on the NSS website.	Failure to comply with this requirement is an offence under section 45 of the Act. See section 45 of the Act below
Section 25– Reporting Obligations	1 - Where a party is declared as a designated party or listed as a listed party, every reporting person shall, immediately, verify whether the details of the designated party or listed party match with the particulars of any customer, and if so, to identify whether the customer owns any funds or other assets in Mauritius, including the funds or other assets referred to in section 23(1) of the UNSA.	Failure to comply with this requirement is an offence under section 45 of the UNSA.
	2 – a) Where funds or other assets or no funds or other assets are identified by the reporting person, the reporting person shall make a	Under section 25(3) of the UNSA, any person who fails to comply with subsection (2)(a) or (b) shall commit an offence and shall, on

Relevant obligation in UNSA	Description	Sanctions for non-compliance
	report to the National Sanctions Secretariat. b) Where a report is made under paragraph (a), the reporting person shall, in addition, report same to its relevant supervisory authority.	conviction, be liable to a fine not exceeding 5 million rupees and to a term of imprisonment not exceeding 10 years.
Section 45- Offences	Any person who contravenes this Act shall commit an offence and shall on conviction be liable, where no specific penalty is provided, to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 10 years.	

Summary Table: Implementing Targeted Financial Sanctions

Consult UN Sanctions Lists and Domestic List	Name Screening and Due Diligence	Freeze/Reject	Report
You are required to consult the UN Sanctions Lists and Domestic List upon dissemination by the NSSec[7] and the FIU.	Conduct sanctions screening on existing, potential or new customers including (beneficial owner and beneficiary) against the lists.	In the event of a true match Existing/new customer- Identify funds or assets owned by the listed party in Mauritius Apply the prohibitions under sections 23 and 24 of the UNSA In the case of a positive match on the domestic list please a freezing order will be issued and shall supersede the prohibition to deal under section 23 of the Act.	In the event of a positive match- Report to the NSSec using the template that may be downloaded from the NSSec website File a copy of the report with the FSC
The UN Sanctions Lists contain names and particulars of parties listed by the UN and the Domestic List contains the name and particulars of the parties listed under the UNSA.	Ensure that potential matches are true matches and not false positives	Potential customer- Reject business relationship	File suspicious transaction report with the FIU

[7] NSSec- the National Sanctions Secretariat established under section 7 of the UNSA
FIU- the financial intelligence unit

You may refer to the Lists from the National Sanctions Secretariat website- https://nssec.govmu.org **or the UN Sanctions Lists on the UN website https://www.un.org/securitycouncil/ Or you may receive them from the FIU if you are registered with the FIU**	Conduct due diligence on any related party[8]		You should also submit an STR when you suspect that an account or transaction (including attempted transaction) is linked to a designated or listed party

[8] Persons related to the funds or other assets that are wholly or jointly owned or controlled directly or indirectly, by designated or listed parties and persons acting on behalf of or at the direction of designated or listed parties.

Annex 1 – Summary of United Nations Security Council - 14 Sanctions Regimes Adopted under Chapter VII of UN Charter May 2022

Sanction Regime	Somalia	ISIL (Da'esh)&Al-Qaida	1518 (Iraq)	Democratic Republic of Congo	Sudan	1636 (Lebanon)	1718 (DPRK)	Libya	1988 (Afghanistan)	Guinea-Bissau	Central African Republic	2140 (Yemen)	South Sudan	Mali
Date of First Resolution	24 April 1992	15 October 1999	24 Nov 2003	12 March 2004	29 March 2005	31 Oct 2005	14 October 2006	26 February 2011	17 June 2011	18 May 2012	5 December 2013	26 February 2014	3 March 2015	5 Sept 2017
First and Latest Resolution	Res 751 (1992), Res 2551 (2020)	Res 1267 (1999), Res 2560 (2020)	Res 1518 (2003), Res 1546 (2004)	Res 1533 (2004), Res 2528 (2020)	Res 1591 (2005), Res 2562 (2020)	Res 1595 (2005), Res 1748 (2007)	Res 1718 (2006), Res 2397 (2017)	Res1970 (2011), Res 2571 (2021)	Res 1988 (2011), Res 2557 (2020)	Res 2048 (2012), No Successor Resolution	Res 2127 (2013), Res 2536 (2020)	Res 2140 (2014), Res 2564 (2021)	Res 2206 (2015), Res 2521 (2020)	Res 2374 (2017), Res 2541 (2020)
Types of Sanctions	Assets Freeze, Travel Ban & Arms Embargo		Arms Embargo and assets freeze	Assets Freeze, Travel Ban & Arms Embargo		Assets Freeze & Travel Ban	Assets Freeze, Travel Ban & Arms Embargo			Travel Ban	Assets Freeze, Travel Ban & Arms Embargo			Assets Freeze and Travel Ban
Competent Authority for administering the sanctions regime	Somalia Sanctions Committee	ISIL (Da'esh) &Al-Qaida Sanctions Committee	1518 Sanctions Committee (Iraq)	Democratic Republic of Congo Sanctions Committee	The Sudan Sanctions Committee	1636 Sanctions Committee (Lebanon)	1718 Sanctions Committee (DPRK)	Libya Sanctions Committee	1988 Sanctions Committee	Guinea-Bissau Sanctions Committee	Central African Republic Sanctions Committee	2140 Sanctions Committee (Yemen)	South Sudan Sanctions Committee	Mali Sanctions Committee
UN Sanctions List As of 19 April 2022	Individuals: 19 Entities: 1	Individuals: 255 Entities: 87	Individuals: 74 Entities: 10	Individuals: 36 Entities: 9	Individuals: 3 Entities: None	Individuals: None Entities: None	Individuals: 80 Entities: 75	Individuals: 28 Entities: 3	Individuals: 135 Entities: 5	Individuals: 10 Entities: None	Individuals: 14 Entities: 1	Individuals: 9 Entities: 2	Individuals: 8 Entities: None	Individuals: 8 Entities: None
Assets Freeze Exemptions	Basic and extraordinary expenses are allowed under Res 1452 (2002) – except for													
	as amended by para 4 (a) and (b) of Res 1844 (2008)	as amended by para 81 (a) and (b) of Res 2368 (2017)	No Exemption	as amended by para 12 (a) to (c) of resolution 1807 (2008)	as amended by para 3 (g) (i) and (ii) of Res 1591 (2005)	as amended by para 2 of Annex in Res 1636 (2005)	as amended by para 9 (a) and (b) of Res 1718 (2006)	as amended by para 19 (a) and (b) of Res 1970 (2011)	as amended by para18 (a) and (b) of Res 2255 (2015)	Travel Ban exemptions only	as amended by para 33 (a) and (b) of Res 2134 (2014)	as amended by para12 (a) and (b) of Res 2140 (2014)	No Exemption	Set out in paragraphs 5, 6 and 7 of resolution 2374 (2017)
Delisting Mechanism	Focal Point Mechanism	Ombudsperson Process	Focal Point Mechanism											

ANNEX 2 - Offences under the FIAMLA

Relevant extracts of the FIAMLA

Section 14(3) FIAMLA- Reporting of suspicious transaction by reporting person or auditor

(3) 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 fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Section 18(3) FIAMLA- Regulatory action in the event of non-compliance

Where it appears or where it is represented to the Financial Services Commission that any financial institution has refrained from complying or negligently failed to comply with any requirement of this Act or regulations, the Financial Services Commission may proceed against the financial institution under section 7 of the Financial Services Act 2007.

Section 19 FIAMLA- Offences relating to obligation to report and keep records and to disclosure of information prejudicial to a request

(1) Any reporting person, or any director, employee, agent or other legal representative of a reporting person who, knowingly or without reasonable excuse –

(a) fails to comply with section 17, 17A, 17B. 17C, 17D, 17E, 17F or 17G;
(b) destroys or removes any record, register or document which is required under this Act or any regulations; or
(c) facilitates or permits the performance under a false identity of any transaction falling within this Part,

shall commit an offence and shall, on conviction, be liable to a fine not exceeding 10 million rupees and to imprisonment for a term not exceeding 5 years.

(2) Any person who -

(a) falsifies, conceals, destroys or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or
(b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced,

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

Section 32A FIAMLA-Offence in respect of contravention of Act

Any person who contravenes this Act shall commit an offence and shall, on conviction, be liable, where no specific penalty is provided, to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Extract of the FIAMLR 2018

Regulation 33 of the FIAMLR 2018

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

Extract of FIAMLR 2019

Regulation 7 of the FIAMLR 2019

Any reporting person who fails to register with FIU under these regulations shall commit an offence and shall on conviction be liable to a fine not exceeding one million rupees.

Annex 3 - Internal Disclosure Form

BEX Mauritius Block Exchange
Suspicious Transaction Internal Disclosure Form Regulations 27 (c) of the Financial Intelligence and Anti Money Laundering Regulations 2018

Reporting Employee
Name:
Designation/Position:
Telephone:
Email:

Client Details
Client Reference:
Client Name:
Address:
Contact Name:
Contact Telephone Number:
Date Client Relationship Commenced:

Information to be collected	
Suspected Information/transaction	
The identification of the party or parties to the transaction.	
The amount of the transaction	
The description of the nature of the transaction	
All the circumstances giving rise to the suspicion.	
The business relationship of the suspect with the Company	
Where the suspect is an insider, any information as to whether the suspect is still affiliated with the Company	
Any voluntary statement as to the origin, source or destination of the proceeds.	
The impact of the suspicious activity on the financial soundness of the Company	
The names of all the officers, employees or agents dealing with the transaction.	
☐ The relevant documentation has been attached to this form.[9]	

[9] *Attach any supporting documentation that is relevant to the case.*

Information to be collected	
Employee's/Director's Signature	
Date	

For MLRO use only
Date received:
Time received:
FIU advised: ☐ Yes ☐ No
Date:

For example, this may include copies of correspondence, customer files or information that you have obtained on the matter.
For each file attached, ensure that an explanation is provided of what it is, as this will help the MLRO when reviewing the case.