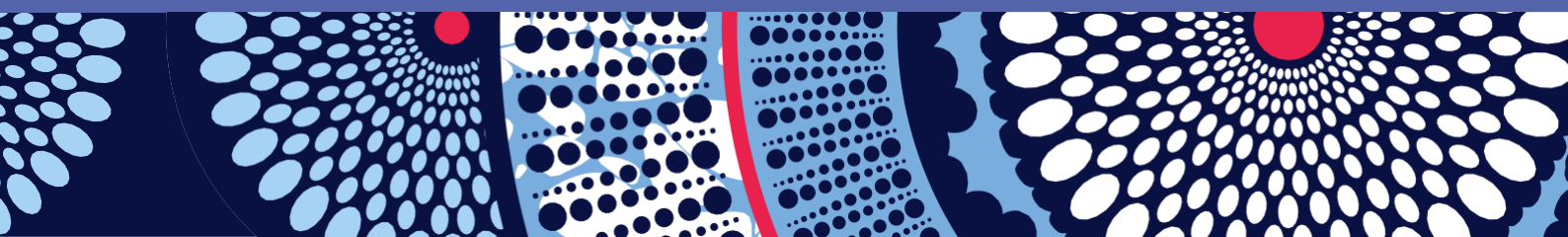
AXIAN
LET'S GROW TOGETHER

JUNE 2023

ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM ('AML CFT') POLICY

(the 'Policy')



GLOSSARY

Business Partner:	means a third party with whom the Company has an investment or business arrangement.
Company:	means any of the following companies: • **AXIAN Telecom Cluster:** AXIAN Telecom, Telma, Telco Comoros, TRM, Free Senegal, Honora Tanzania Plc (fka MIC Tanzania), Togocom, Connecteo, Towerco of Africa Ltd (TOA), Towerco of Africa DRC, Towerco of Madagascar, Towerco of Africa Tanzania Limited, Stellar-IX Tanzania Limited and any other affiliate • **AXIAN Energy Cluster:** AXIAN Energy, AXIAN Energy Green, JOVENA, New Energy Africa (NEA), NEA Madagascar, WeLight, CGHV, GES, and any other affiliate; • **Open Innovation & Fintech Cluster:** MVola, Telco Money, Free Money, TMoney, HTMSL (*Tigo Pesa*), Nexta, Pulse and any other affiliate; • **Real Estate Cluster:** First Immo, SGEM and any other affiliate; • **Financial Services Cluster:** BNI Madagascar, Sanko and any other affiliate; • **AXIAN Support Services**; and • ***Any other entity that is part of the current or future organizational structure of the Group, either by way of incorporation, merger or acquisition, joint venture, among others.*** Collectively referred as the 'Companies' or the 'Group'
Confidential Information:	includes, without limitation, all business-related strategic documents prepared by, owned by the Company, or related to the Group as well as all personal information held on third parties, including Employees.
Employee:	means any person hired by the Company or the Group or Suppliers, and working full time, part time or on a casual basis, including interns and contracted staff, as well as their management, including directors.
Ethics:	refers to a behavior that is based on morality, seriousness, honesty and Respect for all applicable rules and guidelines set out by the Group.
Ethics Line:	refers to the Group's ultimate reporting line with the mandate to undertake a high-level investigation on complex matters, which may not be resolved by the Local Compliance Officer/Champion. Matters shall be escalated to the Axian Ethics Line through the Axian Speak Up platform.
Integrity:	refers to behavior of honesty and absolute probity, without any ill intent and seeking the best interests of the Group.
IT:	stands for 'Information Technology'. IT relates to the internal system, including computers, telecommunications and other related tools and devices, used by the Suppliers to create, process, store, retrieve and exchange data or information on its stakeholders.

Money Laundering:	refers to the process of converting dirty proceeds of criminal activity into clean money, hiding where it came from.
Professional Conduct:	means a set of ethical rules and duties that govern a professional activity. It defines the conduct of the Employee practicing or conducting such business activities or transactions with its clients, Business Partners and other stakeholders.
Respect:	means consideration of the value of someone or something; treating others with respect and consideration, and not harming them physically or psychologically.
Responsibility:	refers moral, intellectual and professional necessity to carry out and meet one's obligations and commitments.
Senior Management:	refers to the Employees who are at the highest level of management and who have control over the day-to-day operations of the Group and/or the Supplier.
Supplier:	includes vendor, Business Partners, consultants and any other third party/ies (individual or entity) with whom the Group shares business interactions.
Values:	refers to the attributes defined and adopted by the Company to which the Employees must adhere. Defined Values shall be the reference points which shall guide the Employees in their daily work. The Company's Values include Boldness, Passion, Innovation and Commitment.

TABLE OF CONTENTS

1. **PURPOSE AND OBJECTIVES** **6**

2. **POINT OF CONTACT** **6**

3. **DEFINITION** **7**

   3.1. Money Laundering – A three staged process 7

   3.2. Importance of having anti-money laundering procedures 8

   3.3. What is financing of terrorism? 8

   3.4. Consequences of money laundering and terrorist financing 9

4. **CLIENT RISK SCREENING** **9**

   4.1. Risk Based Approach 11

   4.2. Acceptance of new clients 12

   4.3. Appropriate Certification 12

   4.4. Assessment of Source of Funds 13

   4.5. Independent Screening 13

   4.6. Handling of Politically Exposed Persons ('PEPs') 14

   4.7. Enhanced Due Diligence measures 16

   4.8. Ongoing monitoring 16

   4.9. Transaction monitoring 16

5. **EMPLOYEE SCREENING** **17**

6. **ROLES AND RESPONSIBILITIES** **18**

   6.1. Breach Management 19

7. **SUSPICIOUS TRANSACTION REPORTING PROCEDURE** **19**

   7.1. Importance of having suspicious transaction procedures 20

   7.2. Reporting of a suspicious transaction 20

   7.3. Tipping off 21

   7.4. Arousing Suspect 21

   7.5. Employee Protection 21

8. TRAINING AND AWARNESS....22

9. EXCEPTIONS AND VIOLATIONS....23

10. AMENDMENTS, REVIEWS AND CONTROLS....23

11. RELATED DOCUMENTS....23

APPENDIX 1 – Checklist of Documents (Clients)....24

APPENDIX 2 – Checklist of Documents (Suppliers)....26

APPENDIX 3 – Business Risk Assessment....27

APPENDIX 4 – Client Acceptance/Review Sheet....33

APPENDIX 5 – Supplier Acceptance/Review Form....34

APPENDIX 6 – Acceptance of Politically Exposed Persons....35

APPENDIX 7 – PEP register....36

APPENDIX 8 – Procedures to detect and report a suspicious transaction....37

APPENDIX 9 – Sample Internal Suspicious Transaction Report....38

APPENDIX 10 – Fit and Proper Declaration Form....39

APPENDIX 11 – Training log....40

APPENDIX 12 – Training Acknowledgement Form....41

1. PURPOSE AND OBJECTIVES

Aligned to the set of 40 recommendations of the Financial Action Task Force ('FATF'), identified as the international benchmark setter on matters relating to the 3 predicate offences, namely money laundering, terrorist financing and proliferation of dangerous drugs and weapons, this Policy outlines a set of standardised internal control policies and procedures to be adopted by the Company and its related entities. The control policies and procedures defined in this Policy must be adopted by the Company and always endorsed by the Employees.

This Policy reflects the state of the law as at this date. However, to ensure consistency with any update in the FATF recommendations or other enactments in the Company's country of registration/operation, this Policy shall be reviewed and updated. Approval from the Company's Senior Management will have to be sought along with a log of changes to be maintained by the Local Compliance Officer/Champion. As stated in the 'Training Section' below, the Local Compliance Officer/Champion shall ensure that timely training courses are delivered to the Employees.

2. POINT OF CONTACT

Except otherwise provided in the local laws under which the Company is governed, the Local Compliance Officer/ Champion shall be the main contact person in respect to the Company's compliance with the AML/CFT requirements and shall complement the roles of a designated money laundering reporting officer, which among others include the following:

a. Contributing to designing, implementing, and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing;

b. Undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

c. Ensuring continued compliance with the AML/CFT requirements as provided under the local laws;

d. Regular reporting, including reporting of non-compliance, to the Company's Senior Management;

e. Demonstrate a significant degree of responsibility and independence in the assessment of the ongoing transactions and compliance framework;

f. Implement a proper Continuous Professional Development (CPD) plan for the Employees at the front/middle and top level. Aim is to sensitize them on their duties and responsibilities towards the operating entities and own name in respect to the handling on ML/TF malpractices;

g. Run timely compliance checks on client files, with detailed findings to the Company's Senior Management;

h. Be the internal resource person to whom all suspicious transactions are to be reported;

i. Be the Company's liaison/contact person with the local competent authority in respect to the reporting of STRs and matters regarding AML/CFT compliance; and

j. Promote a compliance culture within the Company and provide timely feedback and relevant information/ statistics to Senior Management.

3. DEFINITION

Money laundering occurs whenever any person engages in a transaction that involves another person's direct or indirect benefit from crime. This, for the most part, concerns property bought with illegitimate funds rather than the original illegitimate funds.

Money laundering can occur in three stages namely: placement, layering and integration. It must be stressed out at the outset that the three stages are not always strictly segregated as the stages may overlap with each other and money laundering occurs at each stage taken separately.

3.1. MONEY LAUNDERING – A THREE STAGED PROCESS

There are three stages of the money laundering process: placement, layering and integration.

PLACEMENT

The injection of funds or the proceeds of a crime into the financial system

Examples:

i. the setting up a cash business as a cover,

ii. deposits of foreign currency, traveller's cheques, telegraphic transfers, and other negotiable instruments into client bank accounts,

iii. Depositing large amounts of cash in smaller pieces over a sustained period, particularly when the currency originates from overseas.

LAYERING

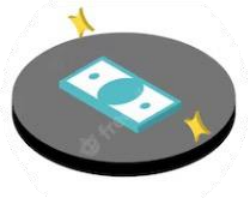
Once the funds have been fully injected, multiple layers of transactions are created to further separate the funds and to make it more difficult to trace them back to its illegal source.

Examples:

i. A Company creates fictitious clients and accounts to generate invoices with the sole intentions of producing additional transactions,

ii. Large and unusual 'one-off' transactions that is not consistent with the client's usual business activity,

iii. Use of letters of credit or bank loans assured on overseas deposits to break the connection with the illegitimate funds.



INTEGRATION

The reintroduction of the illegal funds into the legitimate economy. As the funds now appear as clean income, the integration stage will allow the criminal to use the funds without raising suspicion that might trigger investigation and pursuit.

Examples:

i. Using illegitimate funds to purchase a legitimate enterprise and running it as such, not undertaking in any illegal activity whatsoever.

3.2. IMPORTANCE OF HAVING ANTI-MONEY LAUNDERING PROCEDURES

There has been a concerted effort by the international community to tackle and eradicate money laundering and terrorist financing from all financial centres around the world. This impetus has increased in recent times and now, failure to implement adequate legislation to counter money laundering and combating the financing of terrorism has serious implications.

Countries worldwide have endorsed the FATF recommendations and have subsequently proclaimed a number of governing legislations which set out the legal requirement for an appropriate internal control and risk management system. These obligations are imposed on market operators in view of ensuring fair and transparent business practices.

The following include some of the compelling reasons to make it an absolute priority to combat money laundering, terrorist financing and proliferation:

- **Financial stability:** Money laundering is a threat to the integrity of the entire global financial community.
- **Ethics:** For a long-term success of a country's financial services sector, market operators and government authorities must work together in order to identify and expel any company engaging or participating in fraudulent activities.
- **Compliance:** Defined internal control procedures are adhered to and any suspicious transaction identified has to be reported through the proper channels.
- **Reputation:** If the Company or any of its related entity is exposed to money laundering offences, whether knowingly or unknowingly, it would cause severe damage to the reputation of the Company and its related entities, from which it would be almost impossible to recover.

In the event of failure to abide by the laws and regulations on money-laundering, the supervisory/regulatory authority in the country in which the Company has been registered or conducts business, may initiate such enforcement actions as it shall deem appropriate, not limited to suspension or revocation of licence.

Aligned to recommendation 35 of FATF, the local supervisory/regulatory authority may in case of failure to comply with the defined AML/CFT requirements impose a range of effective, proportionate, and dissuasive sanctions, whether criminal, civil or administrative. Such sanctions, to be quantified by the perceived severity and consequence of the implied AML/CFT breaches, should be applicable not only to the defaulting company but also to the appointed directors and senior management.

3.3. WHAT IS FINANCING OF TERRORISM?

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

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

Traditional terrorist financing model:

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

3.4. CONSEQUENCES OF MONEY LAUNDERING AND TERRORIST FINANCING

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

- reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere;
- attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction;
- damaging the legitimate private sector who may be unable to compete against front companies;
- weakening of financial institutions which may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.;
- economic distortion and instability; or
- increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts.

4. CLIENT RISK SCREENING

For an effective AML/CFT framework, it is mandatory that the Company and its related entities initiate timely verification and testing on the profiles of their respective clients and business counterparties. The customer due diligence measures to be taken are as follows:

a. Identifying the clients and business counterparties, and verifying their identity using reliable, independent source documents, data or information;

b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner(s), such that the Company is satisfied that it knows who the beneficial owner is; For legal persons and arrangements the identification exercise should be extended to understanding the ownership and control structure of the business counterparty;

c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of its clients/business counterparties, their respective business and risk profile, including, where necessary, the source of funds.

Note: Referring to the Company's business model, a distinction is made between actual clients (which includes business partners/associates/customers) and supplier of services (who are professional third-party service providers, solicited to provide support or guidance to the operating entities). Per se, based on the risk materiality, the degree of scrutiny on the suppliers may be different as compared to that applied on clients.

It is a fact that the foundation of any successful anti-money laundering policy is the verification of identity. Whether a long-term business relationship is being set up or it is simply a one-off transaction, all principals need to be vetted with the same astute due diligence. The due diligence screening on new clients shall encompass the below parameters of assessment: -

i. Proof of Existence;

ii. Address verification;

iii. Fitness & Propriety;

iv. Financial Integrity;

v. Source of Fund & Wealth

vi. Media Checks.

In principle, the Company's Local Compliance Officer/Champion must:

- identify and verify the identity of the legal person, including name, incorporation number, date and country of incorporation or registration;
- identify and verify any registered office address and principal place of business (where different from the registered office);
- verify the legal status of the legal person;
- identify and verify the identity of underlying principals (including beneficial owners, controllers, directors or equivalent) with ultimate effective control over the capital or assets of the legal person; and
- verify that any person who purports to act on behalf of the legal person is duly authorised and identify that person.

Note:

a. A principal is considered to be anyone with a beneficial interest or has direct or indirect control over the entity and shall include the following: Settlors or Contributors of capital (whether named or otherwise), Trustees, Beneficiaries, Protectors, Enforcers, Directors, controlling shareholders, Account signatories, Significant Partners including Limited Partners and any person operating under a Power of Attorney;

b. For a proper assessment of the principal's profile, specific checklists of qualifying documents have been defined. Please refer to the table in Appendix 1 which illustrates the types of information that needs to be compiled and verified;

c. For identified suppliers, while the same due diligence screening logic is to be applied, relevant information on its existence and controlling person(s) must be obtained. Reference is to be made to the Appendix 2;

d. Irrespective of the defined checklist of documents for clients and suppliers, provision has been made for alternative documentation that can be acceptable to verify the identity of a direct individual personal client. Information/documents retrieved from the public domain including company websites, can been used to complete the screening process.

4.1. RISK BASED APPROACH

Risk Based Approach ("RBA") relates to a set of tailored measures in order to conduct a critical evaluation of one's risk exposure to ongoing business situations or transactions, and to apply preventive measures that are commensurate with the nature of risks.

For an effective implementation of a RBA, the Company should be in a position to identify, assess and understand the ML/TF risks to which it is exposed and take the required AML/CFT measures to effectively and efficiently mitigate and manage the risks.

The RBA is not a "zero failure" approach since there may still be some isolated instances. Although there are limits to any RBA, it is resolved that ML/TF is a real and serious problem in the world of business with impactful consequences, thus requiring significant and prompt consideration of the Company's Senior Management in order to ensure that it is not, unwittingly or otherwise, assisting or facilitating such an illegal activity.

Key elements of a RBA can be summarised as follows:

Risk Identification & Assessment	**Risk Management & Mitigation**	**Ongoing Monitoring**	**Documentation**
Identifying ML/TF risks facing a firm, relative to its customers, services, countries of operation, media reports, typologies, among others	Identifying and applying measures to effectively mitigate and manage ML/TF risks	Putting in place policies, procedures and information systems to monitor changes to ML/TF risks	Documenting risk assessments, strategies, policies and procedures to monito, manage and mitigate ML/TF risks

In light of the above, the local authorities have, through updates in the local AML/CFT laws and issuance of relevant guidance, put much emphasis on the need for a comprehensive 'Business Risk Assessment' ('BRA') to be approved by the Board of each operating entities (principally Financial Institutions).

Such required BRAs shall, among others, identify the different risk factors which may potentially expose the operating entity to ML/TF risk and an indication on the residual risk upon the relative preventive or mitigating control procedures have been applied (refer to Appendix 3).

4.2. ACCEPTANCE OF NEW CLIENTS

A company cannot perform its duties without possessing adequate knowledge about its clients and the nature of their business. Thus, the due diligence procedures stipulate that a company needs to obtain sufficient information so as to be able to assess the risk that a client relationship poses to it at the outset and in continuity of its duration.

As part of the screening process, the Company's operations team shall upon consultation with the Local Compliance Officer/Champion complete the Client Acceptance Form and request the Client Acceptance Committee, comprising of the Local Compliance Officer/Champion and 2 senior executive officers of the Company (can be the CEO, CFO) to sign the Client Acceptance Form (refer to Appendix 4).

It is to be ensured that the duly completed Client Acceptance Form be accompanied by the full customer due diligence pack and compliance observations/findings for the Client Acceptance Committee to deliberate.

Note: A similar approach shall be applied for accepting suppliers. Refer to Appendix 5 for review/approval of suppliers based on specific criteria defined.

4.3. APPROPRIATE CERTIFICATION

It is often impractical or, in fact, almost impossible to conduct global business in a face-to-face capacity and therefore be provided with the original documents. When this is the case, a certified copy of the original document is issued. However, the documents need to be certified by a suitable certifier, who holds relevant competencies and qualifications.

In the event that an Employee visits a principal, meets him face-to-face and has access to original identification documents, he may take copies of the original documents and certify them personally as being true copies of the original.

In line with the recommended certification standards: -

a. Approved certifiers shall include a Commissioner of Oath, Practising lawyer, Public Notary or a qualified professional;

b. Certified documents must bear 'Certified True Copy';

c. Mandatory to include the Certifier's name, address, position, contact no and registration no (if applicable);

d. Signature of Certifier;

e. Date on which document was certified.

In instances where documents are not in the English or French language, it is expected that officially certified translations of such documents/information in the English or French language must be obtained/ kept.

An exception to the above principle is where the document which is not in English or French can be read and understood by an Employee of the Company or any of its related Group company. In such a situation, the original document, or truly certified as under the law and regulations maybe accepted, provided the concerned officer within the Group, who does understand the language, translates the necessary points into a due diligence note and signs same, clearly stating his or her full name and date accordingly.

4.4. ASSESSMENT OF SOURCE OF FUNDS

This perspective of review is critical for any business model in controlling money-laundering activities. Consequently, operators such as the Company are required to take strict measures to ensure that criminals are not taken on board and to report any suspicion of money laundering, failing which severe penalties will follow including heavy fines and or imprisonment and revocations of the licence issued.

For this purpose, the checklist of documents defined for client entities does cater for a qualifying document to attest the source of fund and wealth of the shareholder and UBO. The operations team shall, as per the defined procedures, always enquire into the source and investment of funds made by the client.

Upon receipt of qualifying documents and/or discrepancies noted, the matter has to be escalated to the Local Compliance Officer/Champion for further screening. The Local Compliance Officer/Champion shall assess whether the client's background/profile matches the scale of his/her investment and wealth and shall document his findings/observations in a client/supplier risk assessment form (see Appendix 4 & 5), with the relative remedial actions to be taken.

Note: This aspect of assessment shall not be applicable for suppliers, who are to be regarded as support services and not as funders.

4.5. INDEPENDENT SCREENING

For an effective risk screening process, reliance on due diligence documents may be too restrictive. For this reason, the Local Compliance Officer/Champion is required to extend his screening to the public domain (e.g., Google) and other reference sources or databases.

The objective is to run an independent name check on the principals directly or indirectly linked to the Company's clients, suppliers (extended to their controlling persons – Director/Shareholder/UBO) and employees – reference is to be made to 'Employee Screening' process.

Extended search on the public domain and other reference sources shall also enable the Local Compliance Officer/Champion to screen for the following, which in turn shall determine the level of compliance scrutiny:

- Politically exposed persons (PEP), close associates, and family members;
- State owned entities and state invested enterprises;
- Global regulatory and law enforcement lists;
- Negative/adverse media report;
- Sanction and embargo list from around the world, including lists published by UNSC, OFAC, EU, TI, OECD and FATF.

Relating to the independent screening (either at time of acceptance or review), findings/observations and actions taken are to be properly documented and maintained on records by the Local Compliance Officer, with relevant remarks on the resolution of flagged hits (positive or false results). Reference is to be made to the acceptance/review forms (See Appendix 4 & 5).

4.6. HANDLING OF POLITICALLY EXPOSED PERSONS ('PEPS')

PEPs are individuals who are or who have been entrusted with prominent public functions (for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials). Companies should be aware that business relationships with PEPs, family members or close associates of PEPs are deemed to pose a greater than normal money laundering risk to companies by virtue of the possibility for them to have benefitted from the proceeds of corruption. See below an extended definition of PEP, extracted from the FATF's publication.

Definitions relating to the term "Politically Exposed Person":

- **Domestic PEP**

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

- **Foreign PEP**

  A "foreign PEP" 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

- **International Organisation PEP**

  An "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 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

Guidelines in identifying PEPs

1. Prominent public function is:
   a. Head of State or of Government;
   b. senior politicians;
   c. senior government/judicial/military officers;
   d. senior executives of state-owned-corporations;
   e. important political party officials

2. Immediate family member is:
   a. Spouse or a partner;
   b. Children;
   c. spouse or partner of the children; or
   d. close parent

3. Close associate is a natural person who is known to;

   a. be a jointly beneficial owner of a legal entity or legal arrangement (trust) with a person mentioned above in item 1 or 2,

   b. have close business associations with a person mentioned above in item 1 or 2,

   c. be the beneficial owner of a legal entity or legal arrangement (trust) set up.

As per the defined PEP policy, the Company's Local Compliance Officer/Champion must:

i. Establish the PEP's position in or relationship with the Company and accordingly apply the risk screening procedures (Note: Different categories of PEP and their involvement in the Company's operations shall bear different level of risk requiring specific consideration);

ii. With reference to the defined checklist of documents, to ensure that the relevant information/ documents are available for screening purposes;

iii. To complete the PEP acceptance form (see Appendix 6), with details on the findings/observations and mitigating controls applied';

iv. In view of completing the PEP acceptance form, advanced search is to be run on the public domain and reference databases in view of attesting the PEP's profile and origin of funds (Note: Perceived risk is that a PEP might have generated his proceeds from bribery and corruption. For this reason, relative to the rationale for being categorised as PEP, details on the latter' investment strategy (industry and country), projects completed or involved in as a PEP, among others are to be retrieved;

v. The duly signed PEP acceptance form and supporting documents are to be sent to the Client Acceptance Committee, which includes the Local Compliance Officer/Champion and 2 senior executive officers of the Company ;

vi. The Client Acceptance Committee shall deliberate and decide as to whether to 'Accept' the PEP on defined conditions or to 'Reject' the proposed relationship;

vii. On the PEP being accepted, the Compliance team shall ensure that the PEP Register (see Appendix 7) is updated accordingly.

Note:

i. As soon as a principal of an applicant for business is categorised as PEP, the applicant is automatically risk profiled as 'High';

ii. However, applying the concept of risk materiality, the relevancy of the assessment parameters as part of the enhanced due diligence (e.g. source of fund/wealth, financial integrity) may be readjusted. While it is perceived that the risk exposure may be higher for a direct PEP, as contributor/shareholder compared to a former/indirect PEP being a Director/representative only, such observation or remarks causing the assessment process to be altered must be documented by the Local Compliance Officer/ Champion and approved by the Client Acceptance Committee.

iii. On a due diligence perspective, we shall as per the expectation of the local regulators, apply reasonable checks on the identified PEPs. However, as a matter of fact, in cases where we hold no qualifying documents on the concerned parties, we shall explore the public domain and retrieve relevant information for the completion of our screening and records. Any discrepancy noted or element of doubt shall be escalated to the Client Acceptance Committee.

4.7. ENHANCED DUE DILIGENCE MEASURES

An Enhanced Due Diligence (EDD) screening shall apply to clients being perceived as high-risk, inclusive of Politically Exposed Persons (PEPs). Enhanced due diligence would imply taking additional steps in relation to identification and verification. This may include the following steps:

i. Obtaining further customer due diligence information (identification and relationship information) from either the customer or independent sources (such as the internet, public or commercially available databases);

ii. Verifying additional aspects of the customer due diligence information obtained;

iii. Obtaining additional information required to understand the purpose and intended nature of such a business relationship;

iv. Taking appropriate and reasonable measures to establish the source of funds and the wealth of the customer, any beneficial owner and the underlying principal.

v. Carrying out more frequent and more extensive ongoing monitoring on such business relationships with setting lower monitoring thresholds for transactions connected with such business relationships.

vi. Enhanced monitoring when a transfer of fund is involved and obtain all relevant information prior to entering to any transaction.

4.8. ONGOING MONITORING

In line with defined duties under local AML/CFT laws, the Local Compliance Officer/Champion, should monitor business relationships and transactions on an ongoing basis with particular attention to transactions monitoring, which shall include profile screening and completeness of relevant data records.

The Local Compliance Officer/Champion should have oversight of the ongoing monitoring process and regular reporting to the Board should be made. The Local Compliance Officer/Champion should identify discrepancies and thereafter take reasonable actions, including EDD to be initiated and escalation to Senior Management/Board of Directors, to address the issues.

4.9. TRANSACTION MONITORING

The regular monitoring of a business relationship, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing due diligence measures. Guided by the principles of audit, a real-time and post-event approach in monitoring transactions is applied.

All Employees, who are directly concerned with the conduct of a transaction by or on behalf to the Company and/or its clients, must pay specific attention in the review and processing of such transactions which are:

- Complex;
- Large and unusual;
- Inconsistent with the initial business purpose;
- Unusual pattern with no apparent economic or lawful purpose.

Each proposed transaction is to be properly reviewed, with relevant supporting documents to be made available on records.

Objective of the review shall be to check the adherence to the intended business purpose, identify the concerned business counterparties and no dealing with sanctioned countries.

Note: The bank statements and debit and credit advices are to be reviewed on a weekly basis by the operations team and any discrepancy is discussed with the superiors and escalated to the client should the need be.

5. EMPLOYEE SCREENING

Unless otherwise provided under the local laws, the Company's Local Compliance Officer/Champion shall in consultation with the human resource team conduct adequate screening on both existing and new Employees.

For the new recruits, they are expected to have a sound knowledge on the prevention and detection of financial crime and should be alert to the potential risks of ML and TF. Thus, when hiring employees, it must be ensured that the below screening measures are to be applied: -

- obtaining identification documents along with relevant references (e.g. past employers and/or other professionals);
- confirming and verifying employment history and the qualifications obtained (through a detailed Curriculum Vitae and academic/training certificates);
- Prior to the issue of an offer letter to the eligible candidate on the basis of his/her academics and experience, the latter is requested to provide details of any disciplinary action taken against him/her or past/ongoing court cases for gross negligence and/or misconduct or breach of law.

Reference is hereby made to Appendix 10 – Fit & Proper Declaration Form, inclusive of an undertaking to provide a recent Police Clearance or Certificate of Character (or its equivalent issued by the local authority) within One month from the date of offer.

6. ROLES AND RESPONSIBILITIES

Board of Directors

The Board of Directors of each operating entity within the Group is responsible for approving this AML/CFT Manual and ensuring a timely implementation of the general principles and requirements as defined hereunder. The Board shall work towards promoting a compliance culture and shall oversee the overall performance of the initiatives associated with AML/CFT, including, but not limited to, the day-to-day operations, training, monitoring and updates.

They will empower and allocate adequate resources, where appropriate, to ensure that the money laundering and terrorist financing risks are identified and managed.

Senior Management

The Board of directors may delegate its roles and responsibilities to Senior Management where appropriate. Senior Management would mean an officer or employee with sufficient knowledge of money laundering and terrorist financing risk exposure and having sufficient seniority to take decisions affecting its risk exposure.

The regulatory framework provides for approval from Senior Management in relationships involving PEP and those profiled as high risks. Consequently, it is the Company's designated Client Acceptance Committee which shall approve the PEP. It is to be highlighted that the said committee shall be comprised of the Local Compliance Officer and 2 senior executive officers.

Employee

Employees shall have and exhibit the highest degree of honesty and integrity in the performance of their duties. Each Employee must be familiar with this Policy and shall have zero tolerance for corrupt practices and fraud. Every Employee is expected to cooperate to the best of his or her ability in any preventive or investigative activity to prevent, detect or eliminate corrupt practices.

The hierarchy of procedures or documents to be followed by the employee in case of discrepancy between them is as follows:

a. The applicable national laws and regulations

b. The Code of Ethics & Professional Conduct

c. The Anti-Bribery and Corruption Policy

d. The employment contract, internal rules, internal memorandum and other procedures of AXIAN, including any disciplinary measures taken by the company.

Group Legal and Compliance team

The Group Legal and Compliance team, through the Local Compliance Officer/Champion shall oversee the implementation of this Policy in the Company. The team shall ensure that the Policy is disseminated and understood, by coordinating training courses. With the support of the Local Compliance Officer/Champion, it sets up a reporting and recording/documentation framework to fight potential cases of corruption. It sizes and supervises the support resources intended to carry out any investigations. As and when solicited by the Senior Management, it shall provide its guidance as to whether to approve any requests for exceptions or tolerances to this Policy or such remedial actions to be taken.

Local Compliance Officer/Champion

The Local Compliance Officer/Champion, with the support from the Group Legal and Compliance team, is responsible for the drafting, review, implementation of this Policy at the Company's level.

The overall objective of the compliance function is to ensure that the Company complies with the with the relevant legal and regulatory obligations as defined under relative local legislations. The local compliance function is also concerned with the Company's ability to demonstrate the existence and effectiveness of our systems and controls. The objective of the compliance policies, systems and controls is to ensure effective detection and management of the Company's compliance risk factors, i.e. the risk of legal and regulatory sanctions, material financial loss or reputational damage, caused by failure to comply with its regulatory and its anti-money laundering, terrorism and corruption obligations.

6.1. BREACH MANAGEMENT

While emphasis is on an effective compliance monitoring programme across the Group, employees are required to be cautious and act diligently in order to mitigate exposure to ML/TF risk. For this reason, Management shall be ensuring that timely training courses are provided to the employees. However, should any act of gross negligence be flagged, causing the Group or any of the related operating entities to face reputational damage or regulatory actions, the Board of Directors reserves the right to take such disciplinary actions against the defaulting employee. Possible actions may include demotion for lack of professionalism or operational performance, not eligible for performance bonus or review of the job description (in terms of tasks/duties/deliverables).

7. SUSPICIOUS TRANSACTION REPORTING PROCEDURE

A "suspicious transaction" is defined as a transaction or activity which:

i. Gives rise to reasonable suspicion that it may involve the laundering of money or the proceeds of any crime including any offence concerning the financing of any actives or transactions related to terrorism, as specified in part III of the Prevention of Terrorism Act 2002,

ii. Is made in circumstances or unusual or unjustified complexity,

iii. Appears to have no economic justification or lawful objective,

iv. 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

v. Gives rise to suspicion for any other reason.

For avoidance of doubt, reference to "Transaction" includes the following:

- 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
- a proposed transaction.

The following are some indicators of potentially suspicious activity, and should awaken the vigilance on the source of funds for the transaction:

a. Any activity that casts doubt over the true identity of an applicant for business or beneficial owners thereof;

b. Establishment of companies having no obvious commercial purpose.

c. Client uninterested in legitimate tax avoidance schemes;

d. Unwillingness to disclose source of funds;

e. Complex group structures with no obvious commercial purpose;

f. Unusually linked transactions;

g. Low-grade securities bought and sold, and high-grade securities bought with proceeds;

h. Frequent deposit of large sum bank drafts and traveller's cheques, in particular when issued overseas;

i. Activities that appear to be inconsistent with the KYC information and profile of the client;

j. Request for use of intermediary client accounts as bank accounts;

k. Regular transfers from FATF grey list of countries.

7.1. IMPORTANCE OF HAVING SUSPICIOUS TRANSACTION PROCEDURES

Not all unusual or suspicious transactions will be actual cases of money laundering and not all funds are derived from illicit activities. However, all employees are required to discharge their moral and legal obligations, as shall be provided under the local AML/CFT laws, by disclosing their suspicions to the Local Compliance Officer/Champion in accordance with the defined internal reporting procedures.

In order to sensitize the Employees on the reporting process, the Local Compliance Officer/Champion shall ensure that regular training sessions are run for all employees, including new recruits, are fully aware of their duty and are encouraged to bring up on suspicion that may arise. It is to be highlighted that the operations team is the first line of defence against potentially criminal activity/ies.

7.2. REPORTING OF A SUSPICIOUS TRANSACTION

For ease of reference, please refer to the flowchart in Appendix 8 for an illustration of how to report a suspicious transaction, including a list of potential indicators. Provisions have been made for an internal reporting to the Local Compliance Officer and external reporting to the local competent authority.

The main emphasis of suspicious transaction reporting is proper customer due diligence screening, documenting all stages and swiftness in the process of reporting. It is important that the process is completed as quickly as possible to ensure that the client is not tipped off by lengthy processes.

On any suspicion of ML/TF being detected, the Employee must complete an Internal Suspicious Transaction Report ('STR'), see Appendix 9, to be submitted to the Local Compliance Officer/Champion within the next 24 hours from the date the suspected activity identified. The duly completed internal STR must be accompanied by such relevant supporting documents or information causing the transaction to be suspicious.

The completed internal STR must be handed over to the Local Compliance Officer/Champion and an entry must immediately be made by the recipient in the Company's STR log along with all the relevant details.

At this stage, the matter becomes a priority at the level of the Local Compliance Officer/Champion and he must initiate an internal enquiry to assess the veracity of the reported case. All due diligence documents relating to the client's profile and ongoing business transactions need to be rigorously examined by the Local Compliance Officer/Champion and any other officers of the Company who may be more familiar with the client's profile and transactions.

If the internal enquiry can unequivocally be found to be without foundation, then the matter can be closed and the relevant details entered into the STR Log. The Local Compliance Officer/Champion shall accordingly inform the reporter on his course of action.

However, if there is any validated ground for suspicion, no matter how insignificant, then a full report must be processed and submitted by the Local Compliance Officer/Champion to the local competent authority though such defined means (either by way of letter or electronically) for further investigation. The Local Compliance Officer/Champion shall accordingly update the STR Log with the relevant details.

7.3. TIPPING OFF

"Tipping off" is defined as the deliberate act of informing the party under suspicion that they are being investigated. As per the recommended AML/CFT framework, tipping off is a serious offence liable to heavy sanctions. It is therefore important for the Employees to be made aware on their responsibilities and be advised to seek guidance from the Local Compliance Officer/Champion when dealing with such situations so as not to tip off the client and/or any other third party.

7.4. AROUSING SUSPECT

When the Local Compliance Officer/Champion has filed a suspicious transaction report with the local competent authority, due care must be taken during subsequent enquiries so as not to alert the concerned party about the said reporting. Appropriate measures must be taken to ensure that the offence of tipping off is not committed.

Should a client enquire about the reason for a delayed processing of his instructions, the Employee should seek guidance from the Local Compliance Officer/Champion without taking the risk of tipping off the client. The Local Compliance Officer/Champion shall in turn liaise with the local competent authority for advice as to how to handle the current situation.

7.5. EMPLOYEE PROTECTION

While the Company encourages all the Employees to report suspected cases, the Company wishes to highlight that it shall not tolerate false or malicious reports made simply to harm another Employee or business associate.

Provided that the reporting is made in good faith, any Employee who reports information of unethical or illegal business conduct using proper channels will be protected from any action against his employment status and/or any whatsoever risk of retaliation.

8. TRAINING AND AWARNESS

In line with the AML/CFT requirements, the Company is required to provide on-going training courses to its Employees, with emphasis on the following:

i. legal obligations as well as all aspects of AML/CFT laws, regulations and guidelines;

ii. the money laundering and terrorist financing vulnerabilities of the products and services offered;

iii. the due diligence requirements and the requirements for the internal and external reporting of suspicion;

iv. recognition and handling of suspicious transactions/activities;

v. the criminal sanctions in place for failing to report information;

vi. new developments including information on current money laundering and terrorist financing techniques, methods, trends and typologies; and

vii. information on the changing behaviour and practices amongst money launderers and those of financing terrorism.

Taking note of the mandatory requirement for the Employees to attend relevant training courses (as part of the Continuous Training Development programme), the below arrangement shall be made:

- Provisions for in-house working sessions, at least on a quarterly basis, by the Local Compliance Officer/ Champion;

- For new recruits, the Local Compliance Officer/Champion shall in collaboration with the human resources team ensure that an induction session be ran within one month from that date joined, with the ultimate objective of sensitizing the attendees on their AML/CFT duties and obligations; and

- An annual refresher course on the general legal framework and operational aspect of business shall be dispensed to all Employees, including an evaluation exercise (MCQ test).

In line with the AML/CFT requirements, there is a need to maintain proper record of the internal and external training courses attended by the Employees. Per se, the Local Compliance Officer/Champion shall at all times maintain a training log (see Appendix 11) copies of the certificates of participation for each attendee must be available on records.

New employees must receive AML/CFT awareness training and should be briefed on the relative internal control policies and procedures defined. This must be done before the employee engages into providing financial services to clients. The training provided should ensure that the new employee is aware of the legal and regulatory obligations placed upon him/her. The training should enable the new employee to recognise a suspicious transaction and the procedures to be followed to adequately handle the reporting.

All new Employees attending the induction course must acknowledge that they have read and understood all the information they have been presented with, and that they also accept that they are personally responsible for their own actions and must comply with the internal control procedures. See 'Training Acknowledgement Form' in Appendix 12.

9. EXCEPTIONS AND VIOLATIONS

Any circumstance that requires exceptional consideration must obtain approval from the Local Compliance Officer and the Senior Management of the Company. Any violation of this policy is deemed serious and will be considered as such in any disciplinary proceedings including termination of employment for misconduct. It will be dealt with under the terms of the applicable disciplinary procedures as well as appropriate legal action.

Employees are expected to alert and report any unethical behavior to the Local Compliance Officer/Champion and/or the Ethics Line through the OneTrust platform. Such reporting will be treated with the utmost confidentiality and investigations will then be conducted. However, the alert system can only concern the revelation of facts of which the author of the alert has personal knowledge and of which s/he is able to demonstrate the reality by all means.

10. AMENDMENTS, REVIEWS AND CONTROLS

The Local Compliance Officer/Champion shall monitor the effective application of this Policy as well as the methods of its application.

Reviews are carried out when any of the following circumstances occurs:

i. Lapse of three years from the last approval date;

ii. Material audit findings/ gaps in this Policy;

iii. Major cases of policy violations, measures taken and need for additional measures to be implemented;

iv. Recommendations of auditors;

v. Changes in the economic, legal and social environment;

vi. The addition of new business activities or the company's presence in new, more sensitive markets.

11. RELATED DOCUMENTS

- Code of Ethics & Professional Conduct
- Supplier Code of Conduct
- Anti–Bribery & Corruption Policy
- Gifts & Hospitality Policy
- Conflict of Interest Policy
- Fraud Management Policy
- Investigation Policy
- Third Party Management Policy
- Whistleblowing Policy
- Sponsorships & Donations Policy

APPENDIX 1 – Checklist of Documents (Clients)

NATURAL PERSONS

- Original Certified copy of current valid national identity document or passport
- Certified Copy of utility bill (less than 3 months old) showing name and residential address
- Signed updated Curriculum Vitae/Biography, with details on employment and entrepreneurial ventures (to specify name of investee co, activity and country)
- Bank Reference letter from a recognized banking institution which has known the persons for at least two years and stating whether the account has been maintained satisfactorily (Bank reference must not be more than 3 months old)
- Documentary evidence on proceeds generated (e.g. statements of accounts or SOF/W confirmation letter from lawyer)

COMPANY OR LEGAL ARRANGEMENT

- Structure chart showing the corporate structure up to the ultimate beneficial owner
- Certified Copy of the Certificate of Incorporation/Registration
- Original or Certified copy of a recent Certificate of Incumbency
- Original of Certificate of Good Standing / Current Standing if available
- Audited Financial Statements for the last 2 years
- Recent Bank Reference Letter
- Register of Directors, Members and UBO; OR
- Detailed Corporate Profile, with Name of entity/Date of formation/Country of formation/Registered Address/Issued Capital and Committed Capital/controlling shareholders-members/Directors-managing principals/description of business activity/indication on total assets-total liabilities
- Certified Copy of the Identity Document/Passport of at least 1 appointed Director, the Authorised Signatory and the UBO OR the one identified as the Controlling Person

REDUCED OR SIMPLIFIED DUE DILIGENCE SHALL BE APPLICABLE AS PER BELOW:

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

i. Proof of existence of the financial services business

ii. Proof of Regulated status of the financial services business

iii. Proof that the financial services business is not acting on behalf of underlying principals

iv. Certified true copy of the list of authorized signatories

v. AML/CFT Comfort letter, with an undertaking to allow onsite testing and upon request, to share relevant due diligence documents on its principals

APPENDIX 2 – Checklist of Documents (Suppliers)

NATURAL PERSONS

Proof of Existence

- Original Certified copy of current valid national identity document or passport
- Valid proof of address

PROFESSIONAL PROFILE

- Updated Curriculum Vitae or Biography
- Duly signed service agreement

COMPANY

Proof of existence:

- Certified Copy of the Certificate of Incorporation/Registration (as applicable);
- Certified Copy of Licence (specifically for licensed and regulated entities);

CONTROL AND MANAGEMENT

- Original or certified copy of a recent extract of file/Extrait Kbis; or
- List of appointed Directors/Authorised Person(s)/Signatory(ies), Shareholders and UBOs;
- At least an identification document on the identified controlling person(s)
- Duly signed service agreement

Note: For instances where the qualifying documents (as per above checklist) are not available. The compliance screening exercise may be conducted on the basis relevant information retrieved from external sources, including the public domain.

APPENDIX 3 – Business Risk Assessment

Business Risk Assessment

This business risk assessment is designed to assist NAME OF OPERATING ENTITY ('the Company') in making such an assessment and provide a method by which it can identify the extent to which its risk factors are exposed to money laundering and terrorist financing.

SECTION A – EVALUATION OF RISK FACTORS

A. Client risk

ASSESSMENT OF RISK

To assess whether the clients and concerned stakeholders have characteristics associated with money laundering, financial crime and terrorist financing. This list is not exhaustive, but some points to be considered include:

- Details on the latter's' professional and business profile
- Type of ownership structures
- Description of products and services
- Mode and frequency of dealings and transactions
- Indication on target market, with profile and industry

Inherent risk rating	Mitigating actions	Residual risk rating

B. Politically Exposed Person Risk

ASSESSMENT OF RISK

To assess the PEP profile in relation to the latter's position and involvement in the shareholding and governance structure

Inherent risk rating	Mitigating actions	Residual risk rating

C. Geography risk

ASSESSMENT OF RISK

Country check being one of the critical factors to be considered, it is to be ensured that there is a proper screening performed on the source and destination of business relationships and dealings. Reference is to be made to the reference list published from time to time by the following international authorities: -

- FATF's high-risk and other monitored jurisdictions
- European Commission list of countries with weak anti-money laundering and terrorist financing regimes
- OECD country classification
- Transparency International - Corruption Perception Index
- OFAC and UNSC sanctions lists

Any intended dealing with claimed medium-high risk countries should be discussed and approved by the Board of Directors, with an EDD screening to be applied on the concerned parties.

Inherent risk rating	Mitigating actions	Residual risk rating

D. Products and services risk

ASSESSMENT OF RISK

Are the offerings as a service provider, in terms of products or services exposed to ML/TF risk? To outline the key safeguards to mitigate exposure to instances of being exploited for potential financial crime and illicit transactions.

Inherent risk rating	Mitigating actions	Residual risk rating

E. Transactions/Dealing risk

ASSESSMENT OF RISK

As stated in s. 25 (1) of the FIAML Reg 2018 the following components are highlighted as factors which are to be actively considered in the risk assessment considerations of ongoing transactions monitoring. It is expected that the Company's personnel should consider and document 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.

Is it a cash-intensive business?

Objective is to review the legitimacy of business transactions and profile of concerned business counterparties; To assess whether the dealings are coherent with the intended business purpose and that same are economically justified.

Inherent risk rating	Mitigating actions	Residual risk rating

F. Delivery channels risk

ASSESSMENT OF RISK

Did the Company meet its clients face to face? If not, the Company may face greater money laundering or terrorist financing risks because it can be more difficult to determine the identity and credibility of a client, both at the start of a relationship and throughout its course. The Company should also consider how and why the client has come to the Company.

Inherent risk rating	Mitigating actions	Residual risk rating

G. IT & Technological Development risk

ASSESSMENT OF RISK

Referring to the IT infrastructure and related control policies defined/implemented, is the Company covered against any potential IT threat? Malware, Phishing, Virus, Hacking, among others

Are the access control policies and data management processing effective? Is retrieval of data records ensured?

Inherent risk rating	Mitigating actions	Residual risk rating

H. Third Party Reliance/Outsourcing Risk

ASSESSMENT OF RISK

- Is there reliance on third party in terms of due diligence screening?
- In the affirmative, have we critically assessed the working arrangement in place?

Inherent risk rating	Mitigating actions	Residual risk rating

Is there any outsourced function to third party service providers? Is there enough assurance in terms of governance and compliance?

Inherent risk rating	Mitigating actions	Residual risk rating

I. COVID 19 risk

ASSESSMENT OF RISK

Is there an effective Disaster Recovery and Business Continuity Plan in place? Are the mitigating control procedures adapted to the current business context/environment and relative exigencies? To what extent the WFH concept has been effective? To outline the different challenges and constraints, both on an operational and commercial point of view.

Inherent risk rating	Mitigating actions	Residual risk rating

J. Data Protection Risk

ASSESSMENT OF RISK

In accordance with the prescribed Data Protection laws, both locally and internationally (reference made to EU GDPR), to assess the Company exposure in terms of handling/processing and safeguarding of records

Inherent risk rating	Mitigating actions	Residual risk rating

K. Human Capital Risk

ASSESSMENT OF RISK

Is the Company equipped with adequate and qualified resources in view of an effective service delivery, in accordance with the prevailing legal and regulatory requirements

Inherent risk rating	Mitigating actions	Residual risk rating

SECTION B – GENERAL OBSERVATION AND RECOMMENDATION

General Observation	Actual risk rating	Recommendation/ Action plan	Risk Owner	Residual risk rating	Implementation date

Business Risk Assessment conducted on

Completed by

Approved by

Next review date

APPENDIX 4 – Client Acceptance/Review Sheet

Name of Client

Contracting Party/ies

Last date reviewed

Latest risk score assigned

	Check (Y/N/NA)	Remarks
Has there had change in the client shareholding structure?	☐ Y ☐ N ☐ NA	
Was approval sought from the authorities sought?	☐ Y ☐ N ☐ NA	
Qualifying CDD documents on the principals are available on records	☐ Y ☐ N ☐ NA	
CDD documents on records are properly certified	☐ Y ☐ N ☐ NA	
Principals have been screened on World Check	☐ Y ☐ N ☐ NA	
Checks ran on Google	☐ Y ☐ N ☐ NA	
Principals are screened against the sanction list issued by OFAC, UNSCPEP(s)	☐ Y ☐ N ☐ NA	
PEP match identified (to specify reason why PEP)	☐ Y ☐ N ☐ NA	
Adverse media report flagged on the principals	☐ Y ☐ N ☐ NA	
EDD performed on PEP and/or concerned principal	☐ Y ☐ N ☐ NA	

Compliance Remarks

AML/CFT Risk Level ☐ Low ☐ Medium ☐ High

CLIENT ACCEPTANCE

On the basis of the above findings and observations, it is resolved that the client be:

☐ Approved without condition ☐ Approved with conditions ☐ Rejected

Compliance Officer

Name

Signature

Date

Director

Name

Signature

Date

APPENDIX 5 – Supplier Acceptance/Review Form

Name of Supplier

Contracting Party

Category/Company Number/Licence number

Date of Incorporation

Name of Beneficial owner(s)

Director/Authorized Signatory

Description of Service

	Check (Y/N)	Remarks
CDD documents are valid and properly certified	☐ Y ☐ N	
Principals have been screened on World Check	☐ Y ☐ N	
Checks ran on Google	☐ Y ☐ N	
Principals have been screened against the sanction list issued by OFAC, UNSC	☐ Y ☐ N	
Adverse report flagged on principals	☐ Y ☐ N	
Principal identified as PEP (Directly or Indirectly)	☐ Y ☐ N	
EDD performed on principals (PEP hit or adverse report or high risk)	☐ Y ☐ N	

Compliance Remarks

AML/CFT Risk Level ☐ Low ☐ Medium ☐ High

SUPPLIER ACCEPTANCE

On the basis of the above findings and observations, it is resolved that the supplier be:

☐ Approved without condition ☐ Approved with conditions ☐ Rejected

Compliance Officer

Name

Signature

Date

Director

Name

Signature

Date

APPENDIX 6 – Acceptance of Politically Exposed Persons

Client Name

PEP Name

PEP Position

Reason why PEP

ENHANCED DUE DILIGENCE – OBSERVATIONS AND ACTION PLAN

Assessment of Source of fund

Source of wealth established

Media/Press review

Details on Ongoing screening set

Monitoring strategy

Profile check

Transaction Monitoring

PEP Register updated ☐ Y ☐ N

Prepared by	**Approved by**
Name	Name
Capacity	Capacity
Date	Date

APPENDIX 7 – PEP register

SN	PEP Name	Nature of relationship	Name of Company	Reason why PEP	Last date reviewed	Remarks

APPENDIX 8 – Procedures to detect and report a suspicious transaction

Indicative list of indicators

i. Complex and opaque corporate shareholding structure;

ii. Belligerent approach on request for qualifying due diligence documents;

iii. Proposed transaction is not consistent with the nature of the client's business;

iv. Invoices of high value for services that do not seem to warrant such high amounts;

v. No valid justification has been obtained on the actual purpose of the proposed transaction;

vi. Beneficiary of the proposed transaction is not disclosed;

vii. Loss making company that seems to carry on trading without UBO injecting funds;

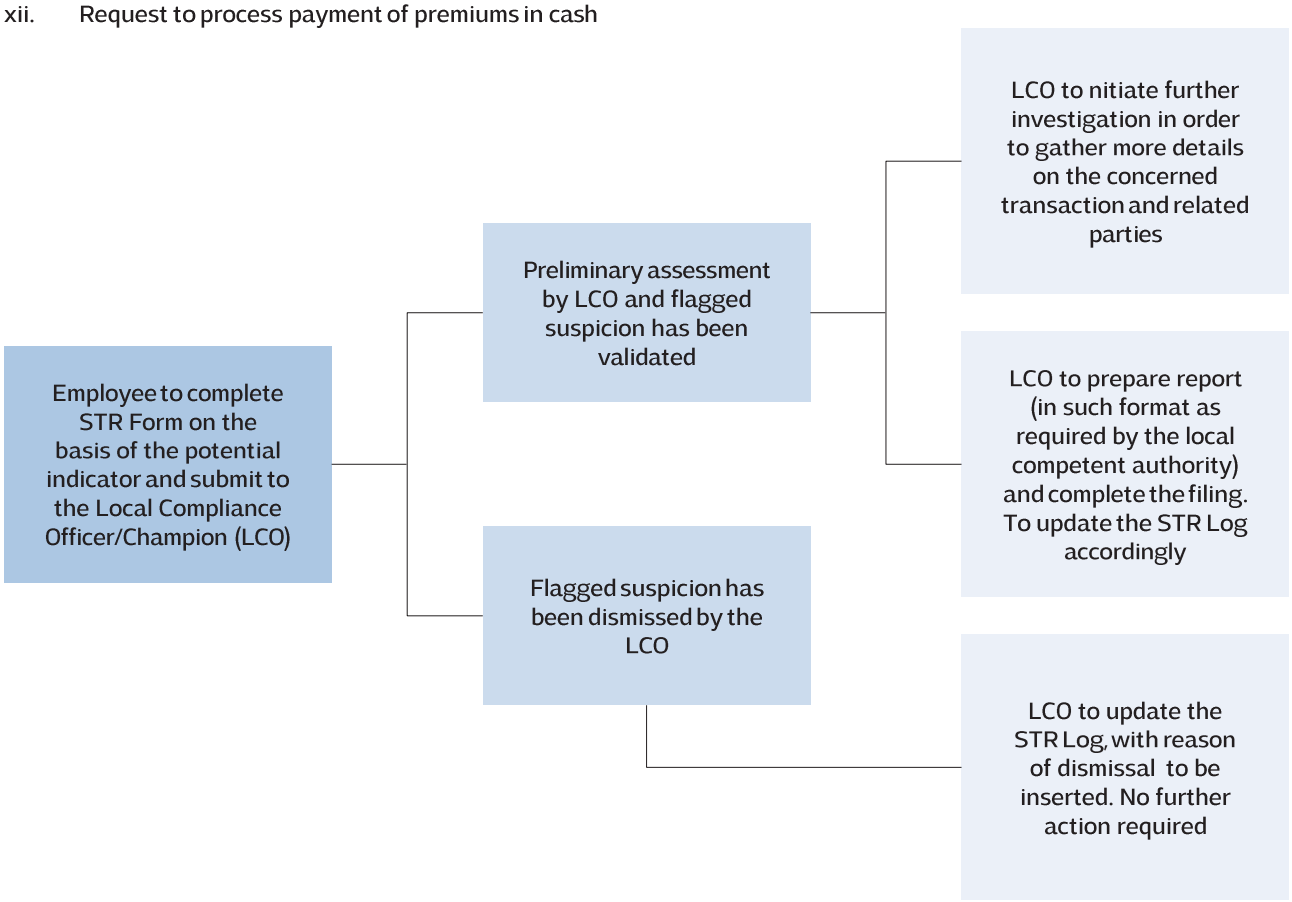
viii. Loans to the company from unusual or simply unidentified sources;

ix. Payment of invoices to jurisdictions with deficiencies in AML/CFT policies OR high-risk jurisdictions supporting terrorism;

x. UBO, delegated officers or controlling persons does not appear to be conversant with the finer details of the company and its relative transactions;

xi. Use of multiple bank accounts or foreign accounts without a valid reason;

xii. Request to process payment of premiums in cash



APPENDIX 9 – Sample Internal Suspicious Transaction Report

INTERNAL SUSPICIOUS TRANSACTION REPORT - CONFIDENTIAL

REPORTING EMPLOYEE

Name _____ Position _____

COMPANY UNDER SUSPICION DETAILS

Company Name _____

Company Address _____

Company Phone No _____

Contact Name _____

Type of Relationship _____ Date Commenced _____

DETAILS ON SUSPICION (to attach copies of relevant documents)

Suspected Information/Transaction _____

Reasons for Suspicion _____

Reporter's signature _____ Date _____

Important Note

i. Tipping Off, i.e. advising the concerned customer/client/business counterparty or anyone else of your suspicion and report, is regarded as a serious offence under FIAMLA, with defined sanctions, both in terms of fines and terms of imprisonment.

ii. This report, along with its supporting documents, will be treated in the strictest confidence.

MLRO USE ONLY

Date Received _____ Time _____

Details on actions _____

(Attach copies of relevant documents)

Date Completed _____

Reported to FIU Report? ☐ Y ☐ N

If No, to provide details _____

APPENDIX 10 – Fit and Proper Declaration Form

DECLARATION FORM - FIT AND PROPER PERSON

Name of Employer _____ Position _____

Important Note: The information provided below shall be used solely for our selection process and shall be kept confidential by the Company except in cases provided otherwise by law.

1. PERSONAL INFORMATION OF APPLICANT [1]

Full Name (Mr. /Ms.) _____

National Identity card Number/Passport No _____

Nationality _____

Physical Residential Address _____

Telephone number _____

Email address _____

2. FIT AND PROPER CONFIRMATION

2.1. Have you at any time been prosecuted for any criminal or civil offence in Mauritius or in any other jurisdiction? If so, please provide details on the offence and status/outcome of the court case (as applicable). In case of conviction, to specify sanctions inflicted.

_____

2.2. Have you ever been dismissed from any office for gross misconduct and/or subject to disciplinary proceedings by your current/previous employer(s)? If so, please share details on the reprimanded actions.

_____

3. DECLARATION

3.1. I hereby certify that the above information and confirmation provided are true and there are no other facts influencing my fitness and propriety to be disclosed;

3.2. I have been made aware that it is an offence to knowingly or recklessly provide any information which is false or misleading and that the Company reserves the right to take appropriate legal actions in case of default;

3.3. I undertake to provide a recent Certificate of Character (or its alternative) issued by the competent authorities within One (1) month from the Company's letter of offer.

Name _____

Signature _____ Date _____

[1] Upon request, relevant supporting documents and referees are to be provided for further processing

APPENDIX 11 – Training log

SN	Course Title	No of Hours	Date dispensed	Resource Person	Attendee(s)	CPD	Certificate Received (Y/N)

APPENDIX 12 – Training Acknowledgement Form

Name _____

Position _____

I, the above mentioned, hereby acknowledge that the internal control policies and procedures as defined in the AML/CFT Manual has been read and understood in view of their effective implementation and enforcement.

I further confirm that a dedicated training session dispensed as part of the induction programme has been duly received, with the below fundamental explained and understood:

- Introduction to Money Laundering/Terrorist Financing and its consequences;
- Obligation to comply with the Financial Intelligence and Anti-Money Laundering Act 2002;
- Duties and Responsibilities – Due Diligence Screening;
- Handling of Suspicious Transactions;
- Internal Suspicious Transaction Reporting – Role of Money Laundering Reporting Officer;
- Record Keeping;
- Offences and Sanctions.

Additionally, I understand that it is my responsibility to act diligently and responsibly. Should I become suspicious of a particular transaction, I undertake to follow the procedures laid down with respect to internal suspicious transaction reporting.

Signature _____ Date _____