May 2022

License no. GB21026947

MEGA FINANCE

Anti-Money Laundering and Combatting of Financing of Terrorism Framework

Version 1.0

Table of Contents

1. Glossary of terms and acronyms

In this document the following terms and acronyms are referred to:

Term/Acronym	Meaning
Anti-Money Laundering ("AML")	Refers to a framework in which, money laundering is managed through adequate policies, processes, practices, procedures and plans to discharge statutory duties, regulatory obligations and agreed standards.
Associated Party	Refers to individuals/entities linked to the customer as follows: • the beneficial owner(s) of the serviced entity; • the controller(s) of the serviced entity; • person(s) on whom power of attorney has been vested to; • bank account signatory(ies); • persons on whose instructions we must or are authorised to act; • persons who can make a request to trustees, for e.g, beneficiaries; • providers of initial and ongoing wealth or funds into the serviced entity where different from the settlor.
Beneficial Owner / Ultimate Beneficial Owners ("BO")	BO is defined as: (a) the natural person who: (i) ultimately owns or controls a customer; or (ii) the person on whose behalf a transaction is being conducted; and (b) Where the customer is a legal person or legal arrangement, includes: (i) the natural person(s) who exercise ultimate control over a legal person or arrangement; (ii) natural person(s) who exercise control of the legal person or legal arrangement through other means as may be specified by the relevant regulatory body or supervisory authority; (iii) where no natural person is identified under (i) and (ii), the natural person who holds the position of senior managing official There could be more than one BO for a customer.
CDD	Customer Due Diligence
Certification of documents	Where reliance is placed upon verification of identity documentation that is not in an original form, the documentation must be appropriately certified as true copies of the original documentation. Documents certified by any one of the following is acceptable: □ A lawyer, notary and actuary; □ An accountant or any other person holding a recognized professional qualification; □ A member of the judiciary, a senior civil servant, or a serving police or customs officer; □ A director or secretary of a regulated financial institution in Mauritius or in an Equivalent jurisdiction;

	An officer of an embassy, consulate or high commission of the country of issue of documentary evidence of identity; The certifier should sign the copy document and clearly indicate his name, address and position or capacity on it together with contact details to aid tracing the certifier. Self-certification is not to be considered an appropriate certification even though the person meets one of the above criteria. Where a senior employee of the Company meets a Client face-to-face and has access to original documents confirming identity and/or permanent residential address (for example, during client visit), he/she can make copies of such documents and certify them as true copies of the originals. Where any of the documents is in a language other than English or French, it should be translated into either of these languages and certified by a qualified translator before submission to the Company Administrator.
Client /Customer / Investor (herein referred to as 'Customer')	'customer' means a natural person or a legal person or a legal arrangement for whom a transaction or account is arranged, opened or undertaken and includes – (a) an applicant for business; (b) a signatory to a transaction or account any person to whom an account or rights or obligations under a transaction have been assigned or transferred; (c) any person who is authorised to conduct a transaction or control an account;
Contact particulars	Includes (both domestic and foreign, where applicable) postal address, fax numbers, telephone numbers (home, work, mobile) and e-mail address of the investor/associated party. A minimum of one contact particular must be obtained.
Combatting the financing of terrorist and related activities ("CFT")	Refers to a framework in which, the combatting of the financing of terrorist and related activities is managed through adequate policies, processes, practices, procedures and plans to discharge statutory duties, regulatory obligations and agreed standards.
Eligible or Group Introducer	Reliance may be placed on a third party to introduce business or to perform the CDD measures as defined in Regulation 21 of the FIAMLR 2018 and chapter 8 of the FSC Handbook. The Introducers will however be limited, which is detailed further in this document.
Enforcer of a trust	Applicable to a purpose trust governed by the Mauritius Trusts Act 2001 (the "TA 2001") and whose duty is to enforce the trust in accordance with its objects.
Enhanced Due Diligence ("EDD")	Additional examination and cautionary measures aimed at identifying customers and confirming that their activities and funds are legitimate e.g. document and verify sources of wealth and funds.

Equivalent Jurisdictions	Jurisdictions having implemented CDD measures as recommended by the FATF.
FIAMLA 2002	The Financial Intelligence and Anti Money Laundering Act 2002, of Mauritius, as amended from time to time.
FIAMLR 2018	The Financial Intelligence and Anti-Money Laundering Regulations 2018 of Mauritius, as amended from time to time.
Financial Action Task Force ("FATF")	Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.
Financial Intelligence Unit ("FIU")	The FIU is the central agency in Mauritius responsible for receiving, requesting, analysing and disseminating to the investigatory and supervisory authorities disclosures of information – (a) concerning suspected proceeds of crime and alleged money laundering offences; (b) required by or under any enactment in order to combat money laundering; or (c) concerning the financing of any activities or transactions related to terrorism.
Financing of Terrorist and related activities	The financing of terrorist and related activities includes any activity that utilises Financial Institutional infrastructure which, has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of funds for the purposes of financing any act of terrorist and related activities as defined in legislation.
FSC or Regulator	The Financial Services Commission of Mauritius.
FSC Handbook	The FSC Anti-Money Laundering and Combatting the Financing of Terrorism Handbook issued in 2020, and updated on 31 March 2021, as amended from time to time.
Company	MEGA FINANCE
Company Administrator	IQ EQ Fund Services (Mauritius) Ltd, a company incorporated under the laws of Mauritius with company number C57472 and having its registered office at 33, Edith Cavell Street, Port-Louis, 11324, Mauritius.
Immediate owner	An "immediate owner" is the natural person, legal person or trust that holds a direct interest in the customer.
Intermediate owner	An "intermediate owner" is the legal person that holds an indirect interest in the customer.
Money Laundering or Money Laundering activity ("ML")	An activity that has, or is likely to have, the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest that anyone has in such proceeds, so that the proceeds appear to be derived from a legitimate source. There are three stages in the process of money laundering: • • Placement - the physical disposal of cash proceeds derived from illegal activities.

	• Layering - separation of illicit proceeds from their sources by creating complex layers of financial transactions designed to disguise the financial sources where the money came from, subvert the audit trail and provide anonymity. • Integration - creating the impression of apparent legitimacy of criminally derived wealth. In the event where the layering process is successful, integration schemes effectively return the laundered proceeds back in to the financial system as if the proceeds are from legitimate business actions.
Nature of business	Nature of business undertaken by the investor. Generic terms such as sales, imports and exports must be avoided.
Non face-to-face	The inability to have personal contact between the Company and/or Administrator or Agent and a prospective investor.
Third Party Reliance	Reliance by the Company on third parties to complete certain CDD measures, provided that there is a contractual arrangement in place with the third party, in accordance with Section 2.5.6 of this Framework.
Politically Exposed Person (PEP)	As per Section 2 of FIAMLR 2018, "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 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". A PEP is an individual who is or has been entrusted with a prominent public function such as: • heads of state; • heads of government; • ministers and deputy or assistance ministers; • members of parliament; • influential functionaries in nationalised industries and government administration; • judges and senior magistrates; • senior political party functionaries; • senior and/or influential officials, functionaries and military leaders and people with similar functions in international or super national organisations; • members of ruling royal families; The definition of PEP also includes: • 'Close associates', i.e.: (a) individuals who are 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'; i.e.: (a) individuals who are 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.
Power of Attorney	A written document in terms of which the customer (the principal) or officer of the Company appoints another person to act as an Agent on their behalf.
Protector of a Trust	Applicable to a trust governed by the Trust Act 2001 and whose functions are: • to advise the trustee of the trust as per such powers as may be conferred under the trust deed; • to ensure that the exercise by the trustees of any of their powers and discretions shall be subject to the prior consent of the protector where warranted under the trust deed.
Purpose of the account	Is the intended nature of the business relationship with the customer? The purpose of the account may be apparent from the product and/or services required and it is therefore not necessary, in all circumstances to request this from the customer separately.

Shell Entity	An entity that: • has no physical presence in the country in which it is incorporated; or • does not conduct business at a fixed address in a jurisdiction in which the shell entity is incorporated; or • does not employ one or more natural persons on a full time business address (the existence simply of a local agent or low level staff does not constitute physical presence); or • does not maintain operating records at this address.
Source of Funds	The origin of funds expected to be used in a business relationship or a single transaction with the Company. It includes both the activity, which generates the funds for a relationship e.g. a customer's occupation or business activities as well as the means through which the customer's funds were transferred to the Company. Source of funds can include but is not limited to the following activities or transactions: • salary or business proceeds; • interest payments; • dividends; • pension payments; • disability grants. In determining the source of funds, the following factors should be taken into consideration: • the source of daily/ monthly income/ revenue; • the customer's various revenue streams; • the business activities undertaken to give rise to the general income.
Source of Wealth	The source of wealth describes the activities/events that have generated the total net worth of the investor. To establish source of wealth no time frame is applied and the customers background must be understood to understand how the customer obtained the wealth i.e. the start-up capital to establish a business, or cash deposit on a house. Source of wealth can include but is not limited to: • maturing investments and encashment claims; • sale of shares; • sale of property; • sale of a company or of interest in a company; • sale of other assets; • salaries or business proceeds; • inheritance; • legal settlements; • loan; • gift or donation; [Note that obtaining information reporting investor's source of wealth, is one of the enhanced CDD measures to be applied in cases of high risk relationships]
Ultimate owner	An "ultimate" owner is the last identified legal person or trust that holds an indirect interest in the customer.

2. Anti-Money Laundering and the Combating of the Financing of Terrorist and related activities

2.1 Introduction

MEGA FINANCE (the "Company") is a Private Company. incorporated under the laws of the Republic of Mauritius.

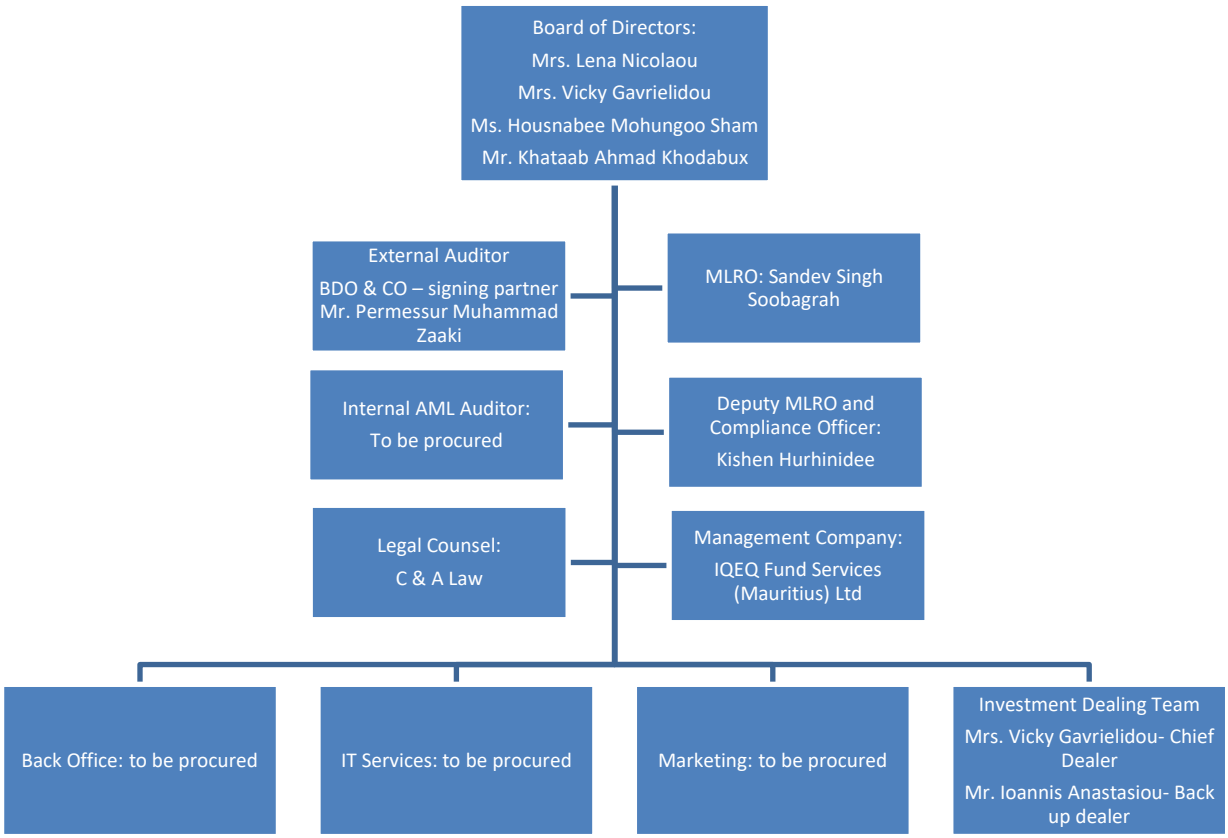
The Company holds a Global Business Licence and has been authorised to operate as an Investment Dealer (Full Service Dealer excluding Underwriting) license

In view of combatting money laundering and the financing of terrorism, the Company must comply with the following legislative requirements under Mauritian law, being the FIAMLA 2002, the FIAMLR 2018 and the FSC Handbook.

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

The Company is based in Mauritius with its registered office being located at the Company Administrator's office where records of the flow of customer's funds in and out of an investment, customer statements and customers' identification and verification data and or documents are maintained.

Company structure:



2.2 Objectives and scope

The objectives of this manual are to:

- establish a framework, within which AML, CFT and Sanctions are managed through adequate procedures, principles, processes, systems and training to discharge statutory duties and regulatory obligations;

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

- CDD;
- Preventing and detecting ML and TF;
- Screening of potential and existing customers for adverse media and sanctions
- Business and Customer Risk Assessment
- Transaction Monitoring
- Suspicious Transaction Reporting;
- Record-keeping;
- Training;

In order for the Company's Board to discharge its AML, CFT and sanctions risk management obligations, this document serves as part of the Company's risk management framework and it is supplemented with relevant processes which may be amended from time to time.

2.3 Legislation in Mauritius

Mauritius' AML and CFT legislative framework is provided for in the following:

a) FIAMLA 2002
b) FIAMLR 2018
c) The Financial Services Act 2007
d) FSC Handbook
e) FSC's Competency Standards
f) Prevention of Corruption Act 2002
g) Prevention of Terrorism Act 2002
h) The United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019

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

In addition, the offences of money laundering are contained within Part II, Section 3 of the FIAMLA 2002 as follows:

2.3.1 Any person who –

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

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

2.3.2 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.

2.4 Roles and responsibilities

The Company is made up of the following structures:

a) Board;
b) Money Laundering Reporting Officer;
c) Compliance Officer;
d) Company Administrator.

2.4.1 Board

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

- Design and implement an AML/CFT framework for the Company;
- undertake risk assessments of its business and its customers;
- Allocate responsibilities to ensure that AML/CFT policies, procedures, processes, systems and training are introduced and maintained;
- Promote a compliance culture.

2.4.1.1 The Board is responsible for managing the Company effectively and is in the best position to understand and evaluate all potential risks to the financial institution, including those of money laundering and financing of terrorism. The Board must therefore take ownership of, and ultimate responsibility for, the business risk assessments and ensure that they remain up to date and relevant, although. primarily, responsibility for the quality and execution of the risk analyses lies with the first line of defence, that is all relevant units of the Company and employees, as applicable, collectively performing their functions and identifying the risks at their level. On the basis of its business risk assessment, the Board must establish a formal strategy to combat money laundering and financing of terrorism. Where the Company forms part of a group operating outside Mauritius, that strategy may protect both its global reputation and its Mauritius business. The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for combatting money laundering and financing of terrorism, and, in particular, responsibilities of the Compliance Officer ("**CO**") and Money Laundering Reporting Officer ("**MLRO**").

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

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

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

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

2.4.1.6 The Board must document its systems and controls (including policies and procedures) and clearly apportion responsibilities for the money laundering and financing of terrorism, and, in particular, responsibilities of the MLRO and CO.

2.4.1.7 According to the FSC Handbook, the Board or senior management of the Company must establish documented systems and controls which:

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

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

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

d) require identification information to be accurate and relevant;

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

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

g) apply increased vigilance to transactions and relationships posing higher risks of money laundering and financing of terrorism;

h) ensure adequate resources are given to the CO to enable the standards within the FSC Handbook to be adequately implemented and periodically monitored and tested;

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

2.4.2 MLRO

In accordance with the FIAMLA 2002 and FIAMLR 2018, the Company must appoint an MLRO.

Pursuant to Regulation 27 of FIAMLR 2018, the Company must establish, document, maintain and operate reporting procedures that shall –

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

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

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

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

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

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

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

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

2.4.3 Compliance Officer

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

The CO shall have the following functions:

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

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

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

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

2.4.4 Company Administrator

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

The Company Administrator will perform:

- certain administrative functions, including but not limited to customer identification and verification, performing enhanced due diligence, screening and risk profiling;
- accounting;
- registrar;
- transfer agency services for the Company (E.g. Customer / Shareholder register); and
- transactional record keeping.

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

2.4.5 Outsourcing of compliance-related functions

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

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

2.5 Customer acceptance requirements

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

2.5.1 CDD Measures -

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

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

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

In that respect, all customers are categorised in three distinctive risk categories namely Low, Medium and High, which is in line with FSC's Effective Customer Risk Assessment.

Low Risk Customer

If the level of AML/CFT of the customer is assessed to be **Low**, it may be possible and appropriate to apply **Reduced or Simplified CDD**[1] measures.

Simplified CDD measures may be applied where lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors and in accordance with any guidelines issued by a regulatory body or supervisory authority.

Where the Company determines that there is a low level of risk, it shall ensure that the low risk identified is consistent with the findings of the national risk assessment[2] or any risk assessment of his supervisory authority or regulatory body, whichever is most recently issued.

---

[1] Please refer to Appendix 1 for the details of the Reduced CDD documents required

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

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

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

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

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

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

The Company can apply simplified CDD measures where:

(a) Lower risks have been identified and the simplified CDD measures shall be commensurate with the lower risk factors;
(b) there is a low level of risk, financial institutions shall ensure that the low risk identified is consistent with the findings of the national risk assessment or any risk assessment carried out, whichever is most recently issued;

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

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

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

Simplified CDD shall never apply where, the Company knows, suspects, or has reasonable grounds for knowing or suspecting that a customer or an applicant for business is engaged in money laundering or terrorism financing or that the transaction being conducted by the customer or applicant for business is being carried out on behalf of another person engaged in money laundering or where there are other indicators of ML/TF risk.

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

Therefore, simplified CDD may be applied in the following cases:

- Regulated financial services business based in Mauritius or in an Equivalent Jurisdiction;
- Public companies listed on recognised Stock/ Investment Exchanges;
- Government administrations or enterprises and statutory body; and
- A pension, superannuation or similar scheme which provides retirement benefits to employees where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

Medium Risk Customer

If the level of AML/CFT of the customer is assessed to be **Medium**, the **standard CDD measure**[3] is applicable.

High Risk Customer

If the level of AML/CFT of the customer is assessed to be **High**, in addition to the standard CDD measures, an appropriate level of **Enhanced CDD**[4] should also be performed, documented and evaluated prior to the acceptance.

[3] Please refer to Appendix 1 for the details of the standard CDD documents required

[4] Please refer to Appendix 1 for the details of the EDD documents required

Enhanced CDD shall be performed:

(a) where a higher risk of money laundering or terrorist financing has been identified;
(b) where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
(c) where a customer or an applicant for business is from a high risk third country;
(d) in relation to correspondent banking relationships, pursuant to regulation 16;
(e) subject to Regulation 15 of the FIAMLR 2018[5], 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.

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

(a) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of the customer and the beneficial owner;
(b) obtaining additional information on the intended nature of the business relationship;
(c) obtaining information on the source of funds or source of wealth of the customer;
(d) obtaining information on the reasons for intended or performed transactions;
(e) obtaining the approval of senior management to commence or continue the business relationship;
(f) conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
(g) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

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

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

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

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

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

It is most important for the Company that the procedures adopted to verify identity for non-face-to-face Customer relationships be at least as rigorous as those for face-to-face Customer relationships.

[5] Regulation 15 of the FIAMLR 2018 relates to a foreign PEP.

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

a) telephone contact with the Client at residential or business number that can be verified independently;
b) holding real-time video call with the Client;
c) confirmation of the Client's address through an exchange of correspondence or other appropriate method;
d) subject to the Client's consent, telephone confirmation of the client's employment status with the client's employer's department at a listed business number of the employer;
e) confirmation of the Client's salary details by requiring the presentation of recent bank statements from another bank;
f) performing screening in accordance with Section 2.6; or
g) provision of certified identification documents by public notaries or by such appropriate persons as provided in the definition section ('Certification of documents') above.

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

(i) regulated for money laundering purposes;
(ii) subject to rules of professional conduct pertaining to money laundering; and
(iii) from an Equivalent jurisdiction that has in place anti-money laundering legislation that is at least equivalent to the legislation in Mauritius.

Please refer to Section 2.5.6.

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

Business activities and services listed[6] in Table 1 below which, whilst not automatically requiring escalation to the Board, are nonetheless considered to present a higher level of risk and which therefore need to be subject to enhanced oversight.

Table 1

Category	Higher risk activities	Rationale
Cash intensive business	Casinos Betting shops	Money laundering potential
Charitable organisations	Provision of fiduciary services to charitable organisations	Increased AML/CFT risks Potential reputational risk
Consultancy	Entities solely existing for the receipt of consultancy fees or commission payments	Money laundering potential Potential tax risk
Dealers & traders in high value goods and services	Antiques Diamonds Fine Arts	Money laundering potential Provenance/title issues

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

	Precious metals and gems	
High Risk Countries or Territories	Business involving a **material relevant connection to a prescribed higher risk country or territory**	Increased AML/CFT risks Potential reputational risk
Money Services Businesses	Exchange Bureaux Travel Bureaux	Increased AML/CFT risk
Natural Resources	Involvement, directly or indirectly, in mining, drilling or quarrying for natural resources	Increased Anti Bribery and Corruption risk Potential reputational risk
Public Enterprise Appointments	Provision of director/officer services to any entity whose securities are listed or traded on a public stock exchange (a "Public Enterprise") – this includes acting as a Director or Officer of subsidiaries of a publicly listed group.	Public interest dimension Potential legal liability Potential regulatory exposure Potential reputational risk
Reputationally Exposed Persons (REPs)	Any proposed new customers or prospects for whom other "relevant adverse information" (RAI) is identified during the course of the CDD/EDD process, for example: • other (unresolved) due diligence information or evidence that otherwise calls into question the integrity or bona fides of the customer/prospect, such as positive World Check hits, EDD reports, etc.	Potential reputational risk

2.5.3 Category of Higher risk customers for Board approval

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

Table 2

Category	Higher risk activities	Rationale
Government Contracts	Customers whose principal activity and/or purpose is the procurement and/or servicing of government contracts (Military, Defence, Technology, Outsourcing, Construction, etc.)	Increased potential for bribery Potential reputational risk

Initial Coin Offerings/Crypto-currencies	Provision of director/officer services to any structure engaged in initial coin offerings, cryptocurrencies or crypto exchanges.	Potential legal liability Potential reputational risk
Pharmaceuticals (including medicinal cannabis)	Manufacture, marketing or sale of pharmaceutical goods or devices which are not licensed or have not received marketing authorization in the jurisdiction where they are manufactured, marketed, sold or supplied.	Potential connection with criminal activity Potential reputational risk
Politically Exposed Persons (PEPs)	Customers/prospects that are identified as having prominent public functions or high political exposure, pose higher Money Laundering risk, particularly where connected to a region or country which is known to present a heightened risk of bribery & corruption and/or political instability.	Increased Anti Bribery and Corruption risk Potential reputational risk Regulatory requirement for enhanced oversight
Arms, armaments and ammunition	Manufacture, trading, transfer (importation/exportation) of Non Military / **Military grade** weapons, explosives, munitions or other controversial weapons	Potential connection with criminal activity Potential reputational risk
Exotic species	Dealing or trading in exotic species	Potential connection with criminal activity Potential reputational risk
Business involving a material relevant[7] connection to a country that is subject to FATF call to apply countermeasures with respect to money laundering and terrorist financing risks	The following countries are subject to a Financial Action Task Force (FATF) call to apply countermeasures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from these jurisdictions: **1. Islamic Republic of Iran** **2. Democratic People's Republic of Korea (North Korea)**	Potential regulatory enforcement and/or reputational damage.

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

	It is the Company's policy **not to deal with clients or structures connected to the above countries**, other than on an approved exceptional basis.	

2.5.4 Categories of Business that will NOT BE ACCEPTED

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

Table 3

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

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

Table 4

Prohibited Business	Additional Guidance
1. Business that violates the Company's **zero tolerance approach to non- compliance with applicable economic sanctions imposed by the European Union ("EU"), United Nations Security Council ("UNSC"), US Office of Foreign Assets Control ("OFAC")**	▪ The United Nations Security Council's website; ▪ U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") website; and ▪ European Commission's website.

2. Business that violates the Company's **zero tolerance approach to bribery**[8] **and corruption**[9]	Best Practices Paper: The Use of the FATF Recommendations to Combat Corruption (FATF Publication)
3. Business involving activities by serviced entities that would constitute **tax fraud or tax evasion** in the jurisdictions where those activities are taking place.	Best Practices: Managing the anti-money laundering and counter-terrorist financing policy implications of voluntary tax compliance programmes (FATF Publication)
4. Business involving activities by the Company's applicants for business that are illegal in the jurisdiction(s) in which the activities are carried out, and/or which would be illegal if carried out in the jurisdiction(s) from which the Company would be providing the services.	Reference to be made to FIAMLA 2002 and FIAMLR 2018

5. Business involving **"Unacceptable activities"**
*The following activities are illegal and/or considered to be reputationally unacceptable and are therefore **prohibited** by the Company:*

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

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

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

2.5.5 Inability to conduct CDD

If the Company is unable to:

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

the Company:

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

and shall consider submitting an STR if the circumstances which prevent the Company from conducting customer due diligence are suspicious or unusual.

For more details on the CDD documentation, please refer to the CDD checklist in Annexure 1.

2.5.6 Third Party Reliance

The Company may rely on relevant third parties to complete certain CDD measures, provided that there is a contractual arrangement in place with the third party. Where reliance is placed on a third party for elements of CDD, the Company shall ensure that the identification information sought from the third party is adequate and accurate. The third party must be regulated, supervised, monitored and subject to CDD in line with section 17C of the FIAMLA 2002 and record keeping requirements pursuant to section 17F of the FIAMLA 2002 and Regulation 21 of the FIAMLR 2018 which provides for third party reliance.

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

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

2.5.6.1 Introduced Business

Customers may be introduced to the Company by way of third parties, i.e. the introducers, with whom the customers already have established business relationships. Thus the Company may rely on the appropriate evidence of customer verification provided by the Introducer, as provided under Regulation 21 of the FIAMLR 2018.

Eligible Introducers are persons/ entities which refer businesses to the Company, and are regulated for money laundering purposes or/ are subject to rules of professional conduct pertaining to money laundering. Eligible introducers must be either in Mauritius or in a jurisdiction that has in place anti-money laundering legislation that is at least equivalent to the legislation in Mauritius.

A **Group Introducer** is an entity that is part of the same group of the Company and is subject for money laundering purposes either to the consolidated supervision of a regulator in Mauritius or in an Equivalent jurisdiction, or is subject to the anti-money laundering regulation in Mauritius or in an Equivalent jurisdiction.

The Company Administrator can rely on another group company to have completed CDD on an existing customer that is to be referred across or shared between units. However, where customers are to be shared by or referred between units, CDD documentation must always first have been obtained to the highest applicable standard.

To enable such reliance, the “referring” unit should at minimum:

- disclose in full the relevant customer identity and risk profile information;
- confirm in writing to the new unit that it has obtained CDD at least to the standard required under this Policy; and
- provide a written undertaking that it will deliver copies of the CDD documentary evidence it holds upon request and without delay

Under the right circumstances, the Company can rely on these introducers to undertake the identification and verification of identity procedures. The assumption here is that since the intermediary is regulated for anti-money laundering and the combating of terrorist financing in its own jurisdiction, it has already undertaken the required identification and verification of identity procedures on the introduced Customers.

However, before reliance is placed on such introducers, the Company shall:

- obtain and maintain documentary evidence that the introducer is regulated for the purposes of preventing money laundering and terrorist financing and ensure that it has access to such details as the name and country of the Introducer’s regulator;

- subject third-party introducers to the full identification and verification CDD measures for identification and verification as provided under Regulations 3(a), (c) and (d) of the FIAMLR 2018;

- be satisfied that the procedures laid down by the introducer meet the requirements specified in the FIAMLA 2002 and FIAMLR 2018;

- satisfy itself that the procedures followed by the eligible or group introducers are sufficiently robust to ensure that the CDD measures are in accordance with the AML/CFT requirements in Mauritius. In that respect, a copy of the AML/CFT policy or manual of the introducer shall be obtained or the Wolfsberg Group Financial Crime Compliance Questionnaire and Wolfsberg Group Correspondent Banking Due Diligence Questionnaire completed (as per Annexure 2A and Annexure 2B); and

- ensure that every Introducer signs a Third-Party Reliance Certificate (as per template under Annexure 3) setting out in writing its responsibilities and commitment.

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

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

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

- such data will be retained by the introducer and will not be disposed of without the Company’s consent;

- the Company will have timely access to such data (including inspection of documents) upon request without delay; and

- such data will be promptly transferred to the custody of the Company, if the introducer ceases to act in that capacity.

At the time of establishing the introducer relationship, the Company shall carry out a risk analysis of this relationship and monitor same. The Company shall also conduct periodic testing of the above arrangements to ensure that the Company is complying with the current legislative framework with respect to the above provision.
Reliance shall not be placed upon third parties for customers that are assessed to present a High level of ML/TF risk or in any situation where money laundering or terrorist financing is suspected. In addition, such exemptions only relate to obtaining certain documents, but they do not exempt us from our other CDD obligations.

It is also important to reiterate that even where the Company places reliance upon an Introducer for the identification and the verification of the identity of introduced Customers, the ultimate responsibility for identification and verification of identity rests with it at all times.

2.6 Screening

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

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

Any new employees of the Company shall also be screened.

2.6.1 Sanctions Screening

Sanctions are measures imposed by governments across the world in response to a variety of international issues including terrorism and nuclear weapons proliferation. Sanctions make it an offence to do business with persons or entities listed in such sanctions. Sanctions lists are local and/or international lists of persons and entities with whom a business relationship may not be established.

These lists include the Office of Foreign Assets Control (OFAC), United Nations Security Council (UNSC) and European Union (EU) which are incorporated into the World Check Compliance screening performed by the Company.

Sanctions screening of all customers and where possible suppliers against applicable local and international sanctions and PEP lists shall be conducted.

Where sanctions screening identifies a potential match, the result must be properly investigated in order to determine whether it is a positive match. In the event that the match is positive, it must be reported to the Compliance Officer for further investigation.

Section 23(1) of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (the "**UN Act**") provides that subject to the said Act, no person shall deal with the funds or other assets of a designated party or listed party, including –

(a) all funds or other assets that are owned or controlled by the designated party or listed party, and not just those that can be tied to –
    (i) a particular terrorist act, plot or threat;
    (ii) a particular act, plot or threat of proliferation;
(b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by the designated party or listed party;
(c) funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated party of listed party, and

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

In addition, section 23(2) of the UN Act provides that where a prohibition is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the accounts held by a listed party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the prohibition, provided that any such interest, earnings and payments continue to be subject to the prohibition.

Where a party is listed pursuant to UNSCR 1737 and the listing continues pursuant to UNSCR 2231, or is listed pursuant to UNSCR 2231, the National Sanctions Committee may authorize the listed party to make any payment due under a contract, an agreement or an obligation, provided that the National Sanctions Committee:

(a) is satisfied that the contract, agreement or obligation was entered prior to the listing of such party;
(b) is satisfied that the contract, agreement or obligation is not related to any of the prohibited items, materials, equipment, goods, technologies, assistance, training, financial assistance, investment, brokering or services referred to in UNSCR 2231 and any future successor resolutions;
(c) is satisfied that the payment is not directly or indirectly received from, or made to, a person or entity subject to the measures in paragraph 6 of Annex B to UNSCR 2231; and
(d) has, 10 working days prior to such authorization, notified the United Nations Sanctions Committee of its intention to authorize such payment.

In addition, any person who holds, controls or has in his custody or possession any funds or other assets of a designated party or listed party shall immediately notify the National Sanctions Secretariat of –

(a) details of the funds or other assets against which action was taken in accordance with subsection (1);
(b) the name and address of the designated party or listed party;
(c) details of any attempted transaction involving the funds or other assets, including –
    (i) the name and address of the sender;
    (ii) the name and address of the intended recipient;
    (iii) the purpose of the attempted transaction;
    (iv) the origin of the funds or other assets; and
    (v) where the funds or other assets were intended to be sent.

Any person who fails to comply with Section 23 (1) or (2) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees or twice the amount of the value of the funds or other assets, whichever is greater, and to imprisonment for a term of not less than 3 years.

Section 24(1) of the UN Act relating to prohibition on making funds or other assets available to designated party or listed party available, provides that subject to the UN Act, 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 designated party or listed party;
(b) a party acting on behalf, or at the direction, of a designated party or listed party; or
(c) an entity owned or controlled, directly or indirectly, by a designated party or listed party.

Section 26 of the UN Act provides with regard to the application for freezing order that:

"(1) (a) Where the Secretary for Home Affairs declares a party as a designated party, he shall, within a reasonable time of that declaration, make an ex parte application to the Designated Judge for a freezing order of the funds or other assets of the designated party.
(b) Where the Designated Judge is satisfied, on a balance of probabilities, that the designated party qualifies to be declared as such under this Act, he shall grant a freezing order which shall remain in force as long as the party is a designated party.

(2) Where a freezing order is in force, nothing shall prevent any interest which may accrue, or other earnings due, on the frozen accounts of the designated party, or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the freezing order, provided that any such interest, earnings and payments continue to be subject to the freezing order.
(3) For the purpose of this section, the Designated Judge shall, where required, examine, in camera, and in the absence of the designated party, any security or intelligence reports or other information or evidence considered by the National Sanctions Committee and these reports, information or evidence shall not, for security reasons, be disclosed to any other person, including the designated party or its legal representatives.
(4) The Secretary for Home Affairs shall give public notice, in 2 newspapers having wide circulation and in such other manner as he may determine, and notify any reporting person or any party that holds, controls or has in his or its custody or possession the funds or other assets of the designated party of any freezing order granted under this section."

The templates for the notification to the National Sanctions Secretariat under section 23(4) of the UN Sanctions Act 2019 and for the reporting on positive name match under section 25(2) of the UN Sanctions Act 2019 can be accessed via the following links:

- https://nssec.govmu.org/Documents/Guidelines/Template%20for%20Notification%20to%20the%20NSSec%20under%20section%2023(4)%20of%20the%20UN%20Sanctions%20Act%202019.xls?csf=1&e=Rk2Gvx

- https://nssec.govmu.org/Documents/Guidelines/Template%20for%20Reporting%20on%20Positive%20Match%20under%20section%2025(2)%20of%20the%20United%20Sanctions%20Act%202019.xls?csf=1&e=RINwkf

2.7 Ongoing monitoring for PEP

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

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

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

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

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

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

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

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

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

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

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

2.8.1 Connected persons that are PEPs

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

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

The Company must:

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

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

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

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

2.9 Adverse Media - Determining the level of significance of information

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

- Date of occurrence: The date of occurrence should be considered as the most recent date associated with the event/activity, as opposed to the first time it was reported. E.g., where the adverse media relates to alleged events, the date of the latest investigation or allegation should be used; where an offence has been confirmed, the date of conviction should be used. Although the length of time since an event occurred may not ultimately alter its significance, more recent events should be treated with additional caution, particularly in the case of alleged events as there may be less information available to validate the legitimacy of the event.
- Note: 'recent' means between 12 months to 5 years depending on the nature, severity and penalty of the alleged/confirmed offence.

- The nature of the allegation/fact: The full nature of the allegation, including any criminal or civil indictments should be recorded. It should be noted whether the allegation relates to money laundering or terrorist financing or potentially could result in money laundering or terrorist financing.
- Whether the information is allegation or fact: Consider whether the information identified is alleged, e.g. rumours, arrests but no charges brought, or whether actual involvement has been confirmed, e.g. through convictions or fines.
- Reliability of the source of the information: Identify and record each source consulted for information obtained.

2.10 Verification of source of funds and source of wealth

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

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

2.11 Customer Risk Profiling

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

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

- Nature and type of Customer;
- Geographical location of the customer;
- Customer's source and destination of funds;
- Customer's Activity and Transaction Frequency;
- Product type
- Automatic risk adjustment to 'High' based on High Risk Indicators such as: a) Incomplete CDD, b) Dealing with PEP, c) Dealing with Sanctioned countries, d) Unsupported bank transactions, e) World Check Hit or any adverse info from media or internet, f) Reliance on Third Parties (not meeting requirements of FIAMLR 2018).

Risk profiling is applicable to:

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

The following Risk Profiling Classification & Review Date:

- High risk: every 12 months;
- Medium risk: every 24 months; and
- Low risk: every 36 months.

Customer Risk profiling will be carried out by the Company Administrator for both new and existing customers.

The approval process will be as follows:

- Principal / Associate Principal level for Low and Medium risks
- Senior Management **/** Director level for High risk customers

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

2.12 Ongoing customer maintenance

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

Periodic reviews of customers shall be conducted to monitor business relationships on an on-going basis so that risk of money laundering and / or terrorist financing can be identified and mitigated. This will include review of CDD documents on a risk-based approach to ensure that up-to-date information is held in relation to business relationships. Any deficiencies noted will be reported to the Board of the Company with appropriate recommendations in compliance with the laws of Mauritius.

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

2.13 Transaction Monitoring

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

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

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

The over-riding principle is to ensure that unusual transactions and activity are identified and subject to a heightened level of scrutiny or examination within the shortest delay and properly documented. Where the risks of money laundering or terrorism financing are higher, enhanced CDD measures must be conducted which are consistent with the risks identified. Of note, Transaction Monitoring can trigger an Internal Investigation and warrant a STR report, in case a suspicious transaction is identified.

The Compliance Officer will conduct sample checks on the transaction monitoring process.

2.14 Enterprise Level AML/CFT Risk Assessment

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

Risk management requires a systematic approach; it is a cyclical process. The Company is expected to perform the whole cycle of identification, analysis and testing of the effectiveness of controls at

regular intervals, because risks are not static. Risks to the Company may change as a result of both internal and external factors.

Since the risks of AML/CFT vary from business to business and are not static, it is the responsibility of the Company to identify the vulnerabilities and risks faced, maintain an up to date understanding of these risks, and develop and implement appropriate strategies to mitigate and control those identified risks. This includes adjustment of such mitigation when needed. The appropriate strategy in order to manage and control those risks is to have an effective internal compliance culture. While the responsibility for the quality and execution of the risk analyses lies with the first line of defence, the ultimate responsibility for the Enterprise Level AML/CFT Risk Assessment lies with the Board of directors. The role of Compliance is process monitoring, facilitating and testing.

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

(a) all relevant risk factors including –

(i) the nature, scale and complexity of the reporting person's activities;

(ii) the products and services provided by the reporting person;

(iii) the persons to whom and the manner in which the products and services are provided;

(iv) the nature, scale, complexity and location of the customer's activities;

(v) reliance on third parties for elements of the customer due diligence process; and

(vi) technological developments; and

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

The risk factors under Section 2.14(a) above are non-exhaustive list and it is for the Company to assess and decide what is appropriate and relevant in the circumstances of the business. In cases, where not all the risk elements have been considered when conducting the business risk assessment, the Company has to demonstrate how effective and robust its business risk assessment is in line with its inherent risks and vulnerabilities and the FSC will assess to what extent the business risk assessment conducted reflect residual risks faced by the Company.

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

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

(i) identifying the inherent risks;

(ii) evaluating the risk control programs; and

(iii) assessing the residual risks.

3. Suspicious Transaction Reporting

3.1 Recognition of Suspicious Transactions

Section 2 of the FIAMLA 2002 defines a suspicious transaction as "*…. a transaction which* –

(a) gives rise to a reasonable suspicion that it may involve -

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, the financing of terrorism or proliferation financing or, any other activities or transaction related to terrorism as specified in the Prevention of Terrorism Act or under any other enactment, whether or not the funds represent the proceeds of a crime;;

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

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

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

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

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

""*transaction" includes -*

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

(b) a proposed transaction or attempted transaction."

This definition is not exhaustive.

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

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

3.2 Internal Reporting of Suspicious Transactions

It is a statutory obligation on all employees to report suspicious transactions promptly and directly to the MLRO or to his deputy in his absence. This should normally be done via an Internal STR Form ("ISF") as per ***Annexure 4***.

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

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

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

	MLRO	**Deputy MLRO**
Name	……..	…….
Email	……..	…….
Telephone	……..	……

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

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

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

3.3 Reporting of Suspicious Transactions to the FIU

Once the MLRO receives an ISF from the relevant staff member, he will determine whether the information contained in the internal STR gives rise to a suspicion that a Customer is engaged in ML and/ or TF. In this respect, the MLRO shall have unfettered access to any or all information which he may need in considering his report. In making his judgment, the MLRO will consider all relevant information that has been made available to him.

If, after completing the review he believes that there is (are) no fact(s) which can negate the suspicion, he has the obligation to report the transaction in writing to the FIU through the latter's online platform, goAML. If, on the other hand, the MLRO does not find it appropriate to report a transaction to the FIU, he will document the reasons for not doing so. This information may be

required to supplement the initial report or as evidence of good practice and best endeavours if, at some future dates, there is an investigation and the suspicions are confirmed. On-going communication between the MLRO and the reporting staff is important.

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

3.4 Reporting Obligations and Offences

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

Pursuant to section 14(3) of the FIAMLA -

"Where a reporting person or an auditor –

(a) becomes aware of a suspicious transaction; or

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

and he fails to make a report to FIU of such transaction not later than 5 working days after the suspicion arose he shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years."

3.5 Registers of Internal and External Disclosures

The Company must establish and maintain separate registers of –
(a) all internal disclosures; and
(b) all external disclosures.

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

The registers must include details of:

(a) the date on which the report is made;
(b) the person who makes the report;
(c) for internal disclosures, whether it is made to the Money Laundering Reporting Officer or Deputy Money Laundering Reporting Officer; and
(d) information sufficient to identify the relevant papers.

4. Training

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

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

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

The training shall cover the following:

(i) Money laundering & Terrorist Financing

(ii) Risk Based Approach to AML/CFT

(iii) Mauritius AML/CFT Legislative Framework

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

(v) Sanctions

(vi) Responsibilities of Board of Directors

(vii) AML/CFT Business Risk Assessment

(viii) Suspicious Transactions Reporting Obligations;

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

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

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

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

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

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

5. Record Keeping

Record keeping obligations are applicable to CDD, transactional and other information required to manage ML, TF and sanctions risks in relation to the investor.

When the Company establishes a business relationship with a customer, the Company must keep record of:

- the identity and address of the customer;
- if the customer is acting on behalf of another person:
  - the identity and address of the person on whose behalf the customer is acting; and
  - the customers authority to act on behalf of that other person;
- if another person is acting on behalf of the customer:
  - the identity and address of that other person; and
  - that other person's authority to act on behalf of the customer;
- the nature of the business relationship or transaction;
- the intended purpose of the business relationship; and
- the source of funds which the prospective customer is expected to use in concluding transactions in the course of the business relationship;
- in the case of a transaction:
  - the amount involved and the currency in which it was denominated;
  - the date on which the transaction was concluded;
  - the parties to the transaction;
  - the nature of the transaction; and
  - business correspondence;
- any document or copy of a document obtained by the Company in order to verify a person's identity.

Furthermore, the Company must keep records of:

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

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

Period for which records must be kept

The Company must keep all the records which relate to:

- the establishment of a business relationship, for at least seven years from the date on which the business relationship is terminated;
- a transaction which is concluded, for at least 7 years from the date on which that transaction is concluded; and
- reports made by and to the MLRO/Compliance Officer, for at least 7 years from the date on which the report is made.

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

6. Independent Audit

6.1 Introduction

Regulation 22(1) (d) of the FIAMLR 2018 requires that financial institutions shall have in place an audit function to review and verify compliance with and effectiveness of the measures taken in accordance with the FIAMLA 2002 and FIAMLR 2018.

An AML/CFT independent audit is a vital element of any effective compliance programme for financial institutions. By virtue of the FIAMLA 2002 and FIAMLR 2018, there is a statutory obligation on every financial institution to have in place an audit function which will allow the reporting entity to evaluate its AML/CFT programme and to ascertain whether the established policies, procedures, systems and controls are adapted with the money laundering and terrorism financing risks identified. The objective of an independent audit is to form a view of the overall integrity and effectiveness of the AML programme, including policies, procedures and processes.

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

6.2 Scope of independent audit

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

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

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

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

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

6.3 Choosing the Audit Professional

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

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

The person or firm conducting the audit should have the necessary skills, qualifications, relevant experience of the audit process, have a proper understanding of the FIAMLA 2002 and its supporting regulations as well as sufficient knowledge of the Financial institution's industry. In order to ensure that the audit is properly conducted as required under the FIAMLA 2002 and FIAMLR 2018, the audit professional needs to provide quality recommendations, so that the financial institution can use the findings and recommendations to improve upon deficient areas.

6.4 Assessing the "independence" of the audit professional

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

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

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

- Was the audit professional involved in the development of the entity's risk assessment? Or the creation, implementation or maintenance of the AML/CFT programme?

- Does the audit professional have financial interest in the business? If yes, would their interests be harmed by the results of the audit, or could there be influence over the audit outcome?

- Does the audit professional have any relationship with any shareholder, director, senior management and or employees?

6.5 Frequency of the Independent Audit

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

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

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

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

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

6.6 Key components of the AML/CFT programme

The independent audit report must express views on whether the AML/CFT risk assessment and the AML/CFT programme comply with the requirements of FIAMLA 2002 and supporting legislations and whether the programme is functioning effectively in practice as required and intended, and has been over the course of the period. The independent audit will involve obtaining a good understanding of the Company's business, reviewing relevant core documents, file testing, testing of the live application of policies and procedures, and interviewing a cross-section of players. The audit process must have sufficient depth and breadth to support the findings and to make the report worthwhile.

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

- address the adequacy of AML/CFT risk assessment, including whether it addresses the specific business activities of that particular Company;
- test compliance of the Company's AML/CFT programme, policies and procedures with the FIAMLA 2002, FIAMLR 2018, and the FSC Handbook and a general review of the effectiveness of the compliance function considering the risks identified through the risk assessment;
- assess the employees' adherence to the AML policies and procedures;
- assess employees' knowledge of the AML/CFT laws, regulations, guidance, and policies & procedures;
- examine the adequacy of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) policies, procedures and processes, and whether they comply with higher-level internal requirements in the Company. This may include considering the adequacy of on

boarding paperwork and considering the adequacy of enhanced measures against the findings of the risk assessment;

- conduct appropriate customer file testing, with particular emphasis on high risk operations (products, service, customer and geographical locations);

- examine the adequacy of the policies and procedures as well as the processes for identifying and reporting suspicious transactions promptly;

- if an automated system is not used to identify or aggregate large transactions, the audit should include sample test of how the compliance officer conducts monitoring;

- conduct appropriate transaction file testing, including a review of 'not filed' (closed as not suspicious) internal suspicious transactions reports, to determine the adequacy, completeness and effectiveness of the STR filing process;

- examine the adequacy of the policies and procedures as well as the processes for screening for targeted financial sanctions as well as implementing prohibitions, freezing assets, and reporting to competent authorities;

- review how the financial institution is screening for targeted financial sanctions without delay when on boarding clients or conducting transactions and when the lists are updated (within hours), and the appropriateness of periodic screening frequency;

- conduct appropriate testing of TFS screening records, including a review of false positives, to determine the adequacy, completeness and effectiveness of the TFS process;

- examine the integrity and the accuracy of the management information systems use in the AML compliance programme; and

- assess training adequacy including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

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

6.7 Audit outcome, report and recommendations

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

- covers all relevant components of the compliance programme as required under FIAMLA 2002 and relevant regulations;

- was adequate and effective throughout a specified period;

- identifies areas where the Company did not meet minimum legal or regulatory standards, and include actions that are required to rectify non-compliance as well as identifying areas for recommended changes in behaviour and practice to improve the effectiveness of the AML/CFT programme's implementation. This includes an indication of where there are potential failings and a recommended course of action.

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

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

6.8 Filing to the FSC

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

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

The FSC may inter-alia, request the following information:

i. whether the Company has adequate policies and procedures in place for independent audit exercise;

ii. what AML/CFT issues have been identified;

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

iv. when the Company has conducted its last independent audit;

v. when the next independent audit exercise would be scheduled;

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

Annexure 1

Customer Due Diligence Checklist

	Documents required
(1)	Business plan of entity to be set up/Rationale for Trust set up
(2)	Structure chart of entity to be set up

List A for Individual

Information to be verified[10]:

(1) For a customer who is a natural person, a reporting person[11] shall obtain and verify –
(a) the full legal and any other names, including, marital name, former legal name or alias;
(b) the date and place of birth;
(c) sex
(d) the nationality;
(e) the current and permanent address; and
(f) such other information as may be specified by a relevant supervisory authority or regulatory body.

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

	Documents required
(1)	**Verification of identity[12]:** Certified true copy[13] of either: ▪ a national identity card; ▪ a current valid passport; or ▪ a current valid driving licence[14].
(2)	**Verification of current and permanent residential address[15]:** Original or certified true copy of either a: ▪ recent[16] utility bill (gas, water, electricity or landline telephone); or ▪ recent bank or credit card statement; or ▪ recent reference or letter of introduction from (i) a financial institution that is regulated in Mauritius; (ii) a regulated financial services business which is operating in an equivalent jurisdiction or a jurisdiction that complies with the FATF standards; or

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

[11] As per Section 2 of FIAMLA, a reporting person means a bank, financial institution, cash dealer or member of a relevant profession or occupation which also includes IQ EQ Mauritius.

[12] Where the legal person with which the natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.

[13] The term 'certified true copy" implies that the document must be appropriately certified as a true copy of the original document either by a lawyer, notary, actuary, accountant or any other person holding a recognized professional qualification, director or secretary of a regulated financial institution in Mauritius or in an equivalent jurisdiction, a member of the judiciary or a senior civil servant.

The certifier should clearly state his/her name, address and position/capacity on it together with contact details to aid tracing of the certifier.

[14] Where IQ-EQ Mauritius is satisfied that the driving licensing authority carries out a check on the holder's identity before issuing the licence.

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

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

	(iii) a branch or subsidiary of a group headquartered in a well-regulated overseas country or territory which applies group standards to subsidiaries and branches worldwide, and tests the application of, and compliance with, such standards.
(3)	**Source of funds:** ▪ Individual Questionnaire (to provide the basic personal details as required by the law) ▪ Declaration of source of fund *(for shareholders, beneficial owners, ultimate beneficial owners, investors, settlors/contributors)* ▪ Evidence of source of fund
(4)	**Fit and proper requirement (for Principals of companies which will provide financial services only)** ▪ Curriculum Vitae; ▪ Personal Questionnaire Form; and ▪ Recent bank reference letter from a recognized banking institution which has known the person for at least two (2) years or alternatively a professional reference letter confirming the current and permanent residential address.
(5)	**FATCA and CRS Due Diligence documents including the self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy) -** *(for shareholders, beneficial owners, ultimate beneficial owners, investors, settlors/contributors)*
(6)	**For any public position held and, where appropriate, nature of employment (including self-employment) and name of employer** A letter or other written confirmation of the individual's status from the public body in question and or any enhanced CDD; a letter or other written confirmation of employment.
(7)	**Government issued personal identification number or other government issued unique identifier** The relevant government document
(8)	**World Check reports**
(9)	**Internet Check reports**

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

List B for Company

Information to be verified[17]:

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

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

	Documents required
(1)	**Verification of existence:** ▪ Original or certified true copy of the Certificate of Incorporation or Certificate of Registration as applicable; and ▪ Details of the registered office address and principal place of business; ▪ Company registry search, including confirmation that the person is not in the process of being dissolved, struck off, wound up or terminated; ▪ Personal visit to principal place of business.

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

(2)	**Identification and verification of identity of underlying Principals[18]:** ▪ Original or certified true copy of the register of directors; ▪ Original or certified true copy of the register of shareholders/members; ▪ Certified true copy of identity and address verification documents as listed in List A above for the directors and authorized signatories; and ▪ Original or certified true copy of CDD documents[19] on the natural persons who ultimately have a controlling ownership interest in the company as per Lists A, B, C, D, E or F (as applicable)
(3)	**Identification and verification of senior management official[20] of the Company:** ▪ Original or certified true copy of CDD documents on the senior managing official.
(4)	**Verification with the relevant companies registry that the Company continues to exist:** ▪ Recent Certificate of Good Standing[21]; or ▪ Verification on the website of the Registrar of Companies in the jurisdiction where the Company is incorporated; ▪ Any other source of information to verify that the document submitted is genuine.
(5)	**Verification of the powers that regulate and bind the Company:** ▪ Certified true copy of the Constitution of the Company; or ▪ Certified true copy of the Memorandum and Article of Association (M&A) of the Company; and ▪ Certified true copy of the licence of the Company, where the latter is a regulated entity.
(6)	**Verification of person(s) who purport to act on behalf of the Company is/are so authorized, and identifying the person(s):** ▪ Original Certificate of Authority signed by the director(s) or an extract of the minutes of the board meeting/ resolutions; ▪ Certified true copy of either valid passport, national identity card or driving licence of the authorized person(s); and ▪ Original or certified true copy of recent utility bill of the authorized person(s).
(7)	▪ Latest audited annual report and accounts (if available); or ▪ Original signed Corporate Profile.
(8)	**FATCA and CRS Due Diligence documents including the self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)**
(9)	**World Check reports on the Company and its Principals**
(10)	**Internet Check reports on the Company and its Principals**
(11)	**Source of fund:** ▪ Declaration of source of fund; and ▪ Evidence of source of fund.

[18] **[18] Where the legal person with which the underlying natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.**

[19] Reference should be made to the identification and verification requirements for individuals, companies, trusts, partnership, societe and foundations as may be relevant and outlined in either lists A, B, C, D, E or F.

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

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

List C for Trusts

Information to be verified[22]:

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

	Documents required
(1)	**Verification that the trust exists and identification of its Principals[23]:** ▪ Original or certified true copy of the trust deed; or ▪ Original or certified true copy of the pertinent extracts thereof, containing the name of the trust, name of the settlor, name of the trustees, names of the protectors and enforcers (if any), beneficiaries[24] (if identified) and powers that regulate and bind the trust.
(2)	**Identifying and verifying the identity of the Principals:** ▪ Certified true copy of CDD documents as listed in List A or List B (as applicable) on the settlor, trustees, protectors, enforcers and the beneficiaries.
(3)	**Identification and verification of senior management official[25]:** ▪ Original or certified true copy of CDD documents on the senior managing official.
(4)	**Verification that the trust is registered (where applicable):** ▪ Certified true copy of Certificate of Registration ▪ Where the above proves insufficient, any other document or other source of information on which it is reasonable to place reliance in the circumstances.
(5)	**Details of the registered office and place of business of the trustee**
(6)	**FATCA and CRS Due Diligence documents including self-certification form (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)**
(7)	**World Check reports on the Trust and its Principals**
(8)	**Source of fund:** ▪ Declaration of source of fund of the settlor/contributor; and ▪ Evidence of source of fund of the settlor/contributor.

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

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

[23] **Where the legal person with which the natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.**

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

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

List D for Partnerships

Information to be verified[26]:

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

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

	Documents required
(1)	**Verification of existence, nature of business and powers that regulate and bind the business:** ▪ An original or certified true copy of the partnership deed; and ▪ A certified true copy of the Certificate of Registration (if registered); ▪ Personal visit to principal place of business; ▪ Reputable and satisfactory third party data, such as a business information service; ▪ Any other source of information to verify that the document submitted is genuine.
(2)	**Identification and verification of the identity of the Principals[27]:** ▪ Certified true copy of CDD documents as listed in Lists A, B, C, D, E or F (as applicable) on the General Partner and the Limited Partners.
(3)	**Verification of person(s) who purports to act on behalf of the partnership is/are so authorized and identification of the person(s):** ▪ Original Certificate of Authority signed by the General Partner(s) and proof of identity of the authorized persons as outlined in List A or List B above.
(4)	**Identification and verification of senior management official[28] of the Partnership:** Original or certified true copy of CDD documents on the senior managing official
(5)	**Copy of latest report and accounts of the partnership**
(6)	**FATCA and CRS Due Diligence documents including self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)**
(8)	**World Check reports on the Partnership and its Principals**
(7)	**Source of fund:** ▪ Declaration of source of fund of the General Partner and Limited Partners; and ▪ Evidence of source of fund.

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

[27] **Where the legal person with which the natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.**

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

List E for Sociétés

Information to be verified[29]:

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

	Documents required
(1)	**Verification of existence:** ▪ Original or certified true copy of an acte de société, including profile of the société; ▪ In the case of Mauritian sociétés, verify with the Registrar of Companies if the société is registered and continues to exist; ▪ In the case of foreign sociétés, obtain a Certificate of Good Standing; ▪ Personal visit to principal place of business; ▪ Reputable and satisfactory third party data, such as a business information service; ▪ Any other source of information to verify that the document submitted is genuine.
(2)	**Verification of the identity of the Principals[30], administrators or gérants:** ▪ Certified true copy of CDD documents as listed in List A, B, C, D, E or F (as applicable).
(3)	**Verification of person(s) who purports to act on behalf of the société is/are so authorized and identification of the person(s):** ▪ Original Certificate of Authority signed by the Administrator(s) or Gérant(s) and proof of identity of the authorized persons as outlined in List A or List B above.
(4)	**Identification and verification of senior management officials[31]:** Original or certified true copy of CDD documents on the senior managing official
(5)	**FATCA and CRS Due Diligence documents including self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)**
(6)	**World Check reports on the société, Principals, administrators or *gérant*(s) of société**
(7)	**Source of fund:** ▪ Declaration of source of fund; and ▪ Evidence of source of fund.

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

[30] **Where the legal person with which the natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.**

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

List F for Foundations

Information to be verified[32]:

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

	Documents required
(1)	**Verification of existence:** ▪ Certified true copy of legal document establishing the Foundation/Foundation Charter; ▪ Certified true copy of the Certificate of Registration or its extract from the public register (if registered); ▪ Personal visit to principal place of business; ▪ Reputable and satisfactory third party data, such as a business information service; ▪ Any other source of information to verify that the document submitted is genuine.
(2)	**Identification and verification of identity of the Principals[33]:** ▪ Certified true copy of CDD documents as per Lists A, B, C, D, E or F as applicable on the Founder(s), members of the Council and beneficiaries.
(3)	**Identification and verification of senior management official[34]:** ▪ Original or certified true copy of CDD documents on the senior managing official
(5)	**Copy of the latest report and accounts of the Foundation**
(6)	**FATCA and CRS Due Diligence documents including self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)**
(7)	**World check reports on the Foundation, Foundation board members and beneficial owners or beneficiaries**
(8)	**Source of fund:** ▪ Declaration of source of fund from the Founder; and ▪ Evidence of source of fund from the Founder.

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

[33] **Where the legal person with which the natural person is associated is high risk, or where a high risk rating would otherwise be attached to the individual principal, then the methods of verification will depend on the riskiness of the relationship and more than one method will be necessary.**

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

Reduced or Simplified CDD[35]

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

	Documents required
(1)	Proof of existence of the financial services business
(2)	Proof of regulated status of the financial services business
(3)	FATCA and CRS Due Diligence documents including self-certification forms (refer to Appendix C as per IQ-EQ Mauritius' CAPP policy)

IQ-EQ Mauritius need to be satisfied that the applicant is not acting on behalf of underlying principals.

Public companies listed on Recognised Stock / Investment Exchanges

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

Government administrations or enterprises and statutory body

	Documents required
(1)	Certified true copy of the Charter Or Constitutive Document or Enactment which established the body
(2)	**Verifying that any person(s) that purport(s) to act on behalf of the government body is/are so authorized and identify the person(s):** ▪ Original Certificate of Authority signed by the directors or an extract of the minutes of the board meeting/ resolutions and proof of identity of the authorized person(s) as outlined in List A above.

A pension, superannuation or similar scheme which provides retirement benefits to employees where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme

	Documents required
(1)	In all transactions undertaken on behalf of an employer-sponsored scheme, Licensees must at a minimum identify and verify the identity by requesting CDD on the: (i) employer (where applicable); and (ii) trustees of the scheme (where applicable).

[35] Chapter 7 of the FSC's AML and CFT Handbook. IQ-EQ Mauritius' Risk and Compliance Team may be consulted for advice on conducting Reduced or Simplified CDD.

Enhanced Due Diligence

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

Type	EDD measures
	• Bank reference • Verify source of funds and source of wealth • Bank statements for last 6 months • Close monitoring of transactions
Individual	• Ensure supporting documents for transactions, such as invoices and agreements are obtained • Criminal records checks and internet checks at time of CAPP and thereafter quarterly • Consider more than one form of verification of ID
	• Certificate of Good Standing
Corporate	• Copy of latest audited financial statements • Verify source of funds and source of wealth of UBO • Bank reference on UBO • Close monitoring of transactions • Ensure supporting documents for transactions, such as invoices and agreements are obtained • Criminal records checks and internet checks at time of CAPP and thereafter quarterly
Trust	• Bank reference on settlor • CV of settlor • Verify source of funds and source of wealth of settlor • Check regulated status, where applicable • Close monitoring of transactions • Criminal records checks and internet checks on CAPP and thereafter quarterly
Partnership	• CV of general partner/controlling partner • Bank reference on general partner/controlling partner • Verify source of funds and source of wealth • Latest audited accounts • Close monitoring of transactions • Criminal records checks and internet checks on CAPP and thereafter quarterly
Société	• Certificate of good standing (for foreign Société) • Latest audited accounts • CV on Gérants /UBO • Close monitoring of transactions • Criminal records checks and internet checks on CAPP and thereafter quarterly
Foundation	• Latest audited accounts • Check regulated status • CV on the founder • Bank reference on the founder • Close monitoring of transactions • Criminal records checks and internet checks on CAPP and thereafter quarterly

Annexure 2a

Wolfsberg Group Financial Crime Compliance Questionnaire (FCCQ) v1.1

the Wolfsberg Group

Financial Institution Name:

Location (Country):

No #	Question	Answer
1. ENTITY & OWNERSHIP		
1	Full Legal name	
2	Append a list of foreign branches which are covered by this questionnaire (if applicable)	
3	Full Legal (Registered) Address	
4	Full Primary Business Address (if different from above)	
5	Date of Entity incorporation / establishment	
6	Select type of ownership and append an ownership chart if available	
6 a	Publicly Traded (25% of shares publicly traded)	
6 a1	If Y, indicate the exchange traded on and ticker symbol	
6 b	Member Owned / Mutual	
6 c	Government or State Owned by 25% or more	
6 d	Privately Owned	
6 d1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more	
7	% of the Entity's total shares composed of bearer shares	

8	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL) ?	
8 a	If Y, provide the name of the relevant branch/es which operate under an OBL	

2. AML, CTF & SANCTIONS PROGRAMME		
9	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:	
9 a	Appointed Officer with sufficient experience / expertise	
9 b	Cash Reporting	
9 c	CDD	
9 d	EDD	
9 e	Beneficial Ownership	
9 f	Independent Testing	
9 g	Periodic Review	
9 h	Policies and Procedures	
9 i	Risk Assessment	
9 j	Sanctions	
9 k	PEP Screening	
9 l	Adverse Information Screening	
9 m	Suspicious Activity Reporting	
9 n	Training and Education	
9 o	Transaction Monitoring	
10	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?	
11	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?	
11a	If Y, provide further details	

3. ANTI BRIBERY & CORRUPTION		
12	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption?	
13	Does the Entity's internal audit function or other independent third party cover ABC Policies and Procedures?	
14	Does the Entity provide mandatory ABC training to:	
14 a	Board and Senior Committee Management	
14 b	1st Line of Defence	
14 c	2nd Line of Defence	
14 d	3rd Line of Defence	
14 e	3rd parties to which specific compliance activities subject to ABC risk have been outsourced	
14 f	Non-employed workers as appropriate (contractors / consultants)	

4. AML, CTF & SANCTIONS POLICIES & PROCEDURES		
15	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:	
15 a	Money laundering	
15 b	Terrorist financing	
15 c	Sanctions violations	
16	Does the Entity have policies and procedures that:	
16 a	Prohibit the opening and keeping of anonymous and fictitious named accounts	
16 b	Prohibit the opening and keeping of accounts for unlicensed banks and / or NBFIs	
16 c	Prohibit dealing with other entities that provide banking services to unlicensed banks	
16 d	Prohibit accounts / relationships with shell banks	
16 e	Prohibit dealing with another Entity that provides services to shell banks	
16 f	Prohibit opening and keeping of accounts for Section 311 designated entities	
16 g	Prohibit opening and keeping of accounts for any of unlicensed / unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	
16 h	Assess the risks of relationships with domestic and foreign PEPs, including their family and close associates	
16 i	Define escalation processes for financial crime risk issues	
16 j	Specify how potentially suspicious activity identified by employees is to be escalated and investigated	
16 k	Outline the processes regarding screening for sanctions, PEPs and negative media	
17	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	
18	Does the Entity have a record retention procedures that comply with applicable laws?	
18 a	If Y, what is the retention period?	

5. KYC, CDD and EDD		
19	Does the Entity verify the identity of the customer?	
20	Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days	
21	Which of the following does the Entity gather and retain when conducting CDD? Select all that apply:	
21 a	Ownership structure	
21 b	Customer identification	
21 c	Expected activity	
21 d	Nature of business / employment	
21 e	Product usage	
21 f	Purpose and nature of relationship	
21 g	Source of funds	
21 h	Source of wealth	
22	Are each of the following identified:	
22 a	Ultimate beneficial ownership	
22 a1	Are ultimate beneficial owners verified?	
22 b	Authorised signatories (where applicable)	
22 c	Key controllers	
22 d	Other relevant parties	
23	Does the due diligence process result in customers receiving a risk classification?	
24	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
25	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
26	Does the Entity have a process to review and update customer information based on:	
26 a	KYC renewal	
26 b	Trigger event	

27	From the list below, which categories of customers or industries are subject to EDD and / or are restricted, or prohibited by the Entity's FCC programme?	
27 a	Non-account customers	
27 b	Non-resident customers	
27 c	Shell banks	
27 d	MVTS/ MSB customers	
27 e	PEPs	
27 f	PEP Related	
27 g	PEP Close Associate	
27 h	Correspondent Banks	
27 h1	If EDD or EDD & restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2014?	
27 i	Arms, defense, military	
27 j	Atomic power	
27 k	Extractive industries	
27 l	Precious metals and stones	
27 m	Unregulated charities	
27 n	Regulated charities	
27 o	Red light business / Adult entertainment	
27 p	Non-Government Organisations	
27 q	Virtual currencies	
27 r	Marijuana	
27 s	Embassies / Consulates	
27 t	Gambling	
27 u	Payment Service Provider	
27 v	Other (specify)	
28	If restricted, provide details of the restriction	

6. MONITORING & REPORTING		
29	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
30	What is the method used by the Entity to monitor transactions for suspicious activities?	
31	Does the Entity have regulatory requirements to report suspicious transactions?	
31 a	If Y, does the Entity have policies, procedures and processes to comply with suspicious transactions reporting requirements?	
32	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	

6. MONITORING & REPORTING		
29	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
30	What is the method used by the Entity to monitor transactions for suspicious activities?	
31	Does the Entity have regulatory requirements to report suspicious transactions?	
31 a	If Y, does the Entity have policies, procedures and processes to comply with suspicious transactions reporting requirements?	
32	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	

7. PAYMENT TRANSPARENCY		
33	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	
34	Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:	
34 a	FATF Recommendation 16	
34 b	Local Regulations	
34 b1	Specify the regulation	
34 c	If N, explain	

8. SANCTIONS		
35	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and / or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and / or masking, of sanctions relevant information in cross border transactions?	
36	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?	
37	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	
37 a	Consolidated United Nations Security Council Sanctions List (UN)	
37 b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	
37 c	Office of Financial Sanctions Implementation HMT (OFSI)	
37 d	European Union Consolidated List (EU)	
37 e	Lists maintained by other G7 member countries	
37 f	Other (specify)	
38	Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries / regions against which UN, OFAC, OFSI, EU and G7 member countries have enacted comprehensive jurisdiction-based Sanctions?	

9. TRAINING & EDUCATION		
39	Does the Entity provide mandatory training, which includes :	
39 a	Identification and reporting of transactions to government authorities	
39 b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	
39 c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	
39 d	New issues that occur in the market, e.g., significant regulatory actions or new regulations	
40	Is the above mandatory training provided to :	
40 a	Board and Senior Committee Management	
40 b	1st Line of Defence	
40 c	2nd Line of Defence	
40 d	3rd Line of Defence	
40 e	3rd parties to which specific FCC activities have been outsourced	
40 f	Non-employed workers (contractors / consultants)	

10. AUDIT		
41	In addition to inspections by the government supervisors / regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	

Signature Page

Wolfsberg Group Financial Crime Compliance Questionnaire 2020 (FCCQ V1.1)

(Financial Institution name)

I, (Senior Compliance Manager- Second Line representative), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg FCCQ are complete and correct to my honest belief.

(Signature & Date)

Annexure 2b

Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ) V1.3

the Wolfsberg Group

Financial Institution Name:	
Location (Country):	

The questionnaire is required to be answered on a Legal Entity (LE) Level. The Financial Institution should answer the questionnaire at the legal entity level including any branches for which the client base, products and control model are materially similar to the LE Head Office. This questionnaire should not cover more than one LE. Each question in the CBDDQ will need to be addressed from the perspective of the LE and on behalf of all of its branches. If a response for the LE differs for one of its branches, this needs to be highlighted and details regarding this difference captured at the end of each sub-section. If a branch's business activity (products offered, client base etc.) is materially different than its Entity Head Office, a separate questionnaire can be completed for that branch.		
No #	**Question**	**Answer**
1. ENTITY & OWNERSHIP		
1	Full Legal Name	
2	Append a list of foreign branches which are covered by this questionnaire	
3	Full Legal (Registered) Address	
4	Full Primary Business Address (if different from above)	
5	Date of Entity incorporation/ establishment	
6	Select type of ownership and append an ownership chart if available	
6 a	Publicly Traded (25% of shares publicly traded)	
6 a1	If Y, indicate the exchange traded on and ticker symbol	
6 b	Member Owned/ Mutual	
6 c	Government or State Owned by 25% or more	
6 d	Privately Owned	
6 d1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more	
7	% of the Entity's total shares composed of bearer shares	
8	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL) ?	

8 a	If Y, provide the name of the relevant branch/es which operate under an OBL	
9	Name of primary financial regulator / supervisory authority	

10	Provide Legal Entity Identifier (LEI) if available	
11	Provide the full legal name of the ultimate parent (if different from the Entity completing the DDQ)	
12	Jurisdiction of licensing authority and regulator of ultimate parent	
13	Select the business areas applicable to the Entity	
13 a	Retail Banking	
13 b	Private Banking / Wealth Management	
13 c	Commercial Banking	
13 d	Transactional Banking	
13 e	Investment Banking	
13 f	Financial Markets Trading	
13 g	Securities Services / Custody	
13 h	Broker / Dealer	
13 i	Multilateral Development Bank	
13 j	Other	
14	Does the Entity have a significant (10% or more) portfolio of non-resident customers or does it derive more than 10% of its revenue from non-resident customers? (Non-resident means customers primarily resident in a different jurisdiction to the location where bank services are provided.)	
14 a	If Y, provide the top five countries where the non-resident customers are located.	
15	Select the closest value:	
15 a	Number of employees	
15 b	Total Assets	
16	Confirm that all responses provided in the above Section ENTITY & OWNERSHIP are representative of all the LE's branches	
16 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
16 b	If appropriate, provide any additional information / context to the answers in this section.	

2. PRODUCTS & SERVICES		
17	Does the Entity offer the following products and services:	
17 a	Correspondent Banking	
17 a1	If Y	
17 a2	Does the Entity offer Correspondent Banking services to domestic banks?	
17 a3	Does the Entity allow domestic bank clients to provide downstream relationships?	
17 a4	Does the Entity have processes and procedures in place to identify downstream relationships with domestic banks?	
17 a5	Does the Entity offer correspondent banking services to Foreign Banks?	
17 a6	Does the Entity allow downstream relationships with Foreign Banks?	
17 a7	Does the Entity have processes and procedures in place to identify downstream relationships with Foreign Banks?	
17 a8	Does the Entity offer correspondent banking services to regulated MSBs/MVTS?	
17 a9	Does the Entity allow downstream relationships with MSBs/MVTS?	
17 a10	Does the Entity have processes and procedures in place to identify downstream relationships with MSB /MVTS?	
17 b	Private Banking (domestic & international)	
17 c	Trade Finance	
17 d	Payable Through Accounts	
17 e	Stored Value Instruments	
17 f	Cross Border Bulk Cash Delivery	
17 g	Domestic Bulk Cash Delivery	
17 h	International Cash Letter	
17 i	Remote Deposit Capture	
17 j	Virtual /Digital Currencies	
17 k	Low Price Securities	
17 l	Hold Mail	
17 m	Cross Border Remittances	
17 n	Service to walk-in customers (non-account holders)	
17 o	Sponsoring Private ATMs	
17 p	Other high risk products and services identified by the Entity	
18	Confirm that all responses provided in the above Section PRODUCTS & SERVICES are representative of all the LE's branches	
18 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
18 b	If appropriate, provide any additional information / context to the answers in this section.	

3. AML, CTF & SANCTIONS PROGRAMME		
19	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:	
19 a	Appointed Officer with sufficient experience/expertise	
19 b	Cash Reporting	
19 c	CDD	
19 d	EDD	
19 e	Beneficial Ownership	
19 f	Independent Testing	
19 g	Periodic Review	
19 h	Policies and Procedures	
19 i	Risk Assessment	
19 j	Sanctions	
19 k	PEP Screening	
19 l	Adverse Information Screening	
19 m	Suspicious Activity Reporting	
19 n	Training and Education	
19 o	Transaction Monitoring	
20	How many full time employees are in the Entity's AML, CTF & Sanctions Compliance Department?	
21	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?	
22	Does the Board or equivalent Senior Management Committee receive regular reporting on the status of the AML, CTF & Sanctions programme?	
23	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?	
23 a	If Y, provide further details	
24	Confirm that all responses provided in the above Section AML, CTF & SANCTIONS Programme are representative of all the LE's branches	
24 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
24 b	If appropriate, provide any additional information / context to the answers in this section.	

4. ANTI BRIBERY & CORRUPTION		
25	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption?	
26	Does the Entity have an enterprise wide programme that sets minimum ABC standards?	
27	Has the Entity appointed a designated officer or officers with sufficient experience/expertise responsible for coordinating the ABC programme?	
28	Does the Entity have adequate staff with appropriate levels of experience/expertise to implement the ABC programme?	
29	Is the Entity's ABC programme applicable to:	
30	Does the Entity have a global ABC policy that:	
30 a	Prohibits the giving and receiving of bribes? This includes promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly, if improperly intended to influence action or obtain an advantage	
30 b	Includes enhanced requirements regarding interaction with public officials?	
30 c	Includes a prohibition against the falsification of books and records (this may be within the ABC policy or any other policy applicable to the Legal Entity)?	
31	Does the Entity have controls in place to monitor the effectiveness of their ABC programme?	
32	Does the Entity's Board or Senior Management Committee receive regular Management Information on ABC matters?	
33	Does the Entity perform an Enterprise Wide ABC risk assessment?	
33 a	If Y select the frequency	
34	Does the Entity have an ABC residual risk rating that is the net result of the controls effectiveness and the inherent risk assessment?	
35	Does the Entity's ABC EWRA cover the inherent risk components detailed below:	
35 a	Potential liability created by intermediaries and other third-party providers as appropriate	
35 b	Corruption risks associated with the countries and industries in which the Entity does business, directly or through intermediaries	
35 c	Transactions, products or services, including those that involve state-owned or state-controlled entities or public officials	
35 d	Corruption risks associated with gifts and hospitality, hiring/internships, charitable donations and political contributions	
35 e	Changes in business activities that may materially increase the Entity's corruption risk	
36	Does the Entity's internal audit function or other independent third party cover ABC Policies and Procedures?	

37	Does the Entity provide mandatory ABC training to:	
37 a	Board and senior Committee Management	
37 b	1st Line of Defence	
37 c	2nd Line of Defence	
37 d	3rd Line of Defence	
37 e	3rd parties to which specific compliance activities subject to ABC risk have been outsourced	
37 f	Non-employed workers as appropriate (contractors/consultants)	
38	Does the Entity provide ABC training that is targeted to specific roles, responsibilities and activities?	
39	Confirm that all responses provided in the above Section Anti Bribery & Corruption are representative of all the LE's branches	
39 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
39 b	If appropriate, provide any additional information / context to the answers in this section.	

5. AML, CTF & SANCTIONS POLICIES & PROCEDURES		
40	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:	
40 a	Money laundering	
40 b	Terrorist financing	
40 c	Sanctions violations	
41	Are the Entity's policies and procedures updated at least annually?	
42	Are the Entity's policies and procedures gapped against/compared to:	
42 a	US Standards	
42 a1	If Y, does the Entity retain a record of the results?	
42 b	EU Standards	
42 b1	If Y, does the Entity retain a record of the results?	
43	Does the Entity have policies and procedures that:	
43 a	Prohibit the opening and keeping of anonymous and fictitious named accounts	
43 b	Prohibit the opening and keeping of accounts for unlicensed banks and/or NBFIs	
43 c	Prohibit dealing with other entities that provide banking services to unlicensed banks	
43 d	Prohibit accounts/relationships with shell banks	
43 e	Prohibit dealing with another entity that provides services to shell banks	
43 f	Prohibit opening and keeping of accounts for Section 311 designated entities	
43 g	Prohibit opening and keeping of accounts for any of unlicensed/unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	
43 h	Assess the risks of relationships with domestic and foreign PEPs, including their family and close associates	
43 i	Define escalation processes for financial crime risk issues	
43 j	Define the process, where appropriate, for terminating existing customer relationships due to financial crime risk	
43 k	Specify how potentially suspicious activity identified by employees is to be escalated and investigated	
43 l	Outline the processes regarding screening for sanctions, PEPs and negative media	
43 m	Outline the processes for the maintenance of internal "watchlists"	
44	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	
45	Does the Entity have a record retention procedures that comply with applicable laws?	
45 a	If Y, what is the retention period?	
46	Confirm that all responses provided in the above Section POLICIES & PROCEDURES are representative of all the LE's branches	
46 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
46 b	If appropriate, provide any additional information / context to the answers in this section.	

6. AML, CTF & SANCTIONS RISK ASSESSMENT		
47	Does the Entity's AML & CTF EWRA cover the inherent risk components detailed below:	
47 a	Client	
47 b	Product	
47 c	Channel	
47 d	Geography	
48	Does the Entity's AML & CTF EWRA cover the controls effectiveness components detailed below:	
48 a	Transaction Monitoring	
48 b	Customer Due Diligence	
48 c	PEP Identification	
48 d	Transaction Screening	
48 e	Name Screening against Adverse Media & Negative News	
48 f	Training and Education	
48 g	Governance	
48 h	Management Information	
49	Has the Entity's AML & CTF EWRA been completed in the last 12 months?	
49 a	If N, provide the date when the last AML & CTF EWRA was completed.	
50	Does the Entity's Sanctions EWRA cover the inherent risk components detailed below:	
50 a	Client	
50 b	Product	
50 c	Channel	
50 d	Geography	

51	Does the Entity's Sanctions EWRA cover the controls effectiveness components detailed below:	
51 a	Customer Due Diligence	
51 b	Transaction Screening	
51 c	Name Screening	
51 d	List Management	
51 e	Training and Education	
51 f	Governance	
51 g	Management Information	
52	Has the Entity's Sanctions EWRA been completed in the last 12 months?	
52 a	If N, provide the date when the last Sanctions EWRA was completed.	
53	Confirm that all responses provided in the above Section AML, CTF & SANCTIONS RISK ASSESSMENT are representative of all the LE's branches	
53 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
53 b	If appropriate, provide any additional information / context to the answers in this section.	

7. KYC, CDD and EDD		
54	Does the Entity verify the identity of the customer?	
55	Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days	
56	Which of the following does the Entity gather and retain when conducting CDD? Select all that apply:	
56 a	Ownership structure	
56 b	Customer identification	
56 c	Expected activity	
56 d	Nature of business/employment	
56 e	Product usage	
56 f	Purpose and nature of relationship	
56 g	Source of funds	
56 h	Source of wealth	
57	Are each of the following identified:	
57 a	Ultimate beneficial ownership	
57 a1	Are ultimate beneficial owners verified?	
57 b	Authorised signatories (where applicable)	
57 c	Key controllers	
57 d	Other relevant parties	
58	What is the Entity's minimum (lowest) threshold applied to beneficial ownership identification?	
59	Does the due diligence process result in customers receiving a risk classification?	

60	If Y, what factors/criteria are used to determine the customer's risk classification? Select all that apply:	
60 a	Product Usage	
60 b	Geography	
60 c	Business Type/Industry	
60 d	Legal Entity type	
60 e	Adverse Information	
60 f	Other (specify)	
61	Does the Entity have a risk based approach to screening customers for adverse media/negative news?	
62	If Y, is this at:	
62 a	Onboarding	
62 b	KYC renewal	
62 c	Trigger event	
63	What is the method used by the Entity to screen for adverse media / negative news?	
64	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
65	If Y, is this at:	
65 a	Onboarding	
65 b	KYC renewal	
65 c	Trigger event	
66	What is the method used by the Entity to screen PEPs?	
67	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
68	Does the Entity have a process to review and update customer information based on:	
68 a	KYC renewal	
68 b	Trigger event	
69	Does the Entity maintain and report metrics on current and past periodic or trigger event due diligence reviews?	

70	From the list below, which categories of customers or industries are subject to EDD and/or are restricted, or prohibited by the Entity's FCC programme?	
70 a	Non-account customers	
70 b	Non-resident customers	
70 c	Shell banks	
70 d	MVTS/ MSB customers	
70 e	PEPs	
70 f	PEP Related	
70 g	PEP Close Associate	
70 h	Correspondent Banks	
70 h1	If EDD or EDD & restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2014?	
70 i	Arms, defense, military	
70 j	Atomic power	
70 k	Extractive industries	
70 l	Precious metals and stones	
70 m	Unregulated charities	
70 n	Regulated charities	
70 o	Red light business / Adult entertainment	
70 p	Non-Government Organisations	
70 q	Virtual currencies	
70 r	Marijuana	
70 s	Embassies/Consulates	
70 t	Gambling	
70 u	Payment Service Provider	
70 v	Other (specify)	
71	If restricted, provide details of the restriction	
72	Does the Entity perform an additional control or quality review on clients subject to EDD?	
73	Confirm that all responses provided in the above Section KYC, CDD and EDD are representative of all the LE's branches	
73 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
73 b	If appropriate, provide any additional information / context to the answers in this section.	

8. MONITORING & REPORTING		
74	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
75	What is the method used by the Entity to monitor transactions for suspicious activities?	
76	If manual or combination selected, specify what type of transactions are monitored manually	
77	Does the Entity have regulatory requirements to report suspicious transactions?	
77 a	If Y, does the Entity have policies, procedures and processes to comply with suspicious transaction reporting requirements?	
78	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	
79	Confirm that all responses provided in the above Section MONITORING & REPORTING are representative of all the LE's branches	
79 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
79 b	If appropriate, provide any additional information / context to the answers in this section.	

9. PAYMENT TRANSPARENCY		
80	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	
81	Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:	
81 a	FATF Recommendation 16	
81 b	Local Regulations	
81 b1	Specify the regulation	
81 c	If N, explain	
82	Does the Entity have processes in place to respond to Request For Information (RFIs) from other entities in a timely manner?	
83	Does the Entity have controls to support the inclusion of required and accurate originator information in international payment messages?	
84	Does the Entity have controls to support the inclusion of required beneficiary information international payment messages?	
85	Confirm that all responses provided in the above Section PAYMENT TRANSPARENCY are representative of all the LE's branches	
85 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
85 b	If appropriate, provide any additional information / context to the answers in this section.	

10. SANCTIONS		
86	Does the Entity have a Sanctions Policy approved by management regarding compliance with sanctions law applicable to the Entity, including with respect its business conducted with, or through accounts held at foreign financial institutions?	
87	Does the Entity have policies, procedures, or other controls reasonably designed to prevent the use of another entity's accounts or services in a manner causing the other entity to violate sanctions prohibitions applicable to the other entity (including prohibitions within the other entity's local jurisdiction)?	
88	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and/or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and/or masking, of sanctions relevant information in cross border transactions?	
89	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?	
90	What is the method used by the Entity?	
91	Does the Entity screen all sanctions relevant data, including at a minimum, entity and location information, contained in cross border transactions against Sanctions Lists?	
92	What is the method used by the Entity?	
93	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	
93 a	Consolidated United Nations Security Council Sanctions List (UN)	
93 b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	
93 c	Office of Financial Sanctions Implementation HMT (OFSI)	
93 d	European Union Consolidated List (EU)	
93 e	Lists maintained by other G7 member countries	
93 f	Other (specify)	
94	Question removed	
95	When regulatory authorities make updates to their Sanctions list, how many business days before the entity updates their active manual and/ or automated screening systems against:	
95 a	Customer Data	
95 b	Transactions	

96	Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries/regions against which UN, OFAC, OFSI, EU and G7 member countries have enacted comprehensive jurisdiction-based Sanctions?	
97	Confirm that all responses provided in the above Section SANCTIONS are representative of all the LE's branches	
97 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
97 b	If appropriate, provide any additional information / context to the answers in this section.	

11. TRAINING & EDUCATION		
98	Does the Entity provide mandatory training, which includes :	
98 a	Identification and reporting of transactions to government authorities	
98 b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	
98 c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	
98 d	New issues that occur in the market, e.g., significant regulatory actions or new regulations	
98 e	Conduct and Culture	
99	Is the above mandatory training provided to :	
99 a	Board and Senior Committee Management	
99 b	1st Line of Defence	
99 c	2nd Line of Defence	
99 d	3rd Line of Defence	
99 e	3rd parties to which specific FCC activities have been outsourced	
99 f	Non-employed workers (contractors/consultants)	
100	Does the Entity provide AML, CTF & Sanctions training that is targeted to specific roles, responsibilities and high risk products, services and activities?	
101	Does the Entity provide customised training for AML, CTF and Sanctions staff?	
102	Confirm that all responses provided in the above Section TRAINING & EDUCATION are representative of all the LE's branches	
102 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
102 b	If appropriate, provide any additional information / context to the answers in this section.	

12. QUALITY ASSURANCE /COMPLIANCE TESTING		
103	Are the Entity's KYC processes and documents subject to quality assurance testing?	
104	Does the Entity have a program wide risk based Compliance Testing process (separate to the independent Audit function)?	
105	Confirm that all responses provided in the above Section QUALITY ASSURANCE / COMPLIANCE TESTING are representative of all the LE's branches	
105 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
105 b	If appropriate, provide any additional information / context to the answers in this section.	

13. AUDIT		
106	In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	
107	How often is the Entity audited on its AML, CTF & Sanctions programme by the following:	
107 a	Internal Audit Department	
107 b	External Third Party	
108	Does the internal audit function or other independent third party cover the following areas:	
108 a	AML, CTF & Sanctions policy and procedures	
108 b	KYC / CDD / EDD and underlying methodologies	
108 c	Transaction Monitoring	
108 d	Transaction Screening including for sanctions	
108 e	Name Screening & List Management	
108 f	Training & Education	
108 g	Technology	
108 h	Governance	
108 i	Reporting/Metrics & Management Information	
108 j	Suspicious Activity Filing	
108 k	Enterprise Wide Risk Assessment	
108 l	Other (specify)	
109	Are adverse findings from internal & external audit tracked to completion and assessed for adequacy and completeness?	
110	Confirm that all responses provided in the above section, AUDIT are representative of all the LE's branches	
110 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
110 b	If appropriate, provide any additional information / context to the answers in this section.	

Declaration Statement

Wolfsberg Group Correspondent Banking Due Diligence Questionnaire 2020 (CBDDQ V1.3)
Declaration Statement (To be signed by Global Head of Correspondent Banking or equivalent position holder AND Group Money Laundering Prevention Officer, Global Head of Anti- Money Laundering, Chief Compliance Officer, Global Head of Financial Crimes Compliance OR equivalent)

(Financial Institution name) is fully committed to the fight against financial crime and makes every effort to remain in full compliance with all applicable financial crime laws, regulations and standards in all of the jurisdictions in which it does business and holds accounts.

The Financial Institution understands the critical importance of having effective and sustainable controls to combat financial crime in order to protect its reputation and to meet its legal and regulatory obligations.

The Financial Institution recognises the importance of transparency regarding parties to transactions in international payments and has adopted/is committed to adopting these standards.

The Financial Institution further certifies it complies with / is working to comply with the Wolfsberg Correspondent Banking Principles and the Wolfsberg Trade Finance Principles. The information provided in this Wolfsberg CBDDQ will be kept current and will be updated no less frequently than on an annual basis.

I, _____ (Global Head of Correspondent Banking or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of the Financial Institution.

The Financial Institution commits to file accurate supplemental information on a timely basis.

I,_____ (MLRO or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of the Financial Institution.

I,_____ (MLRO or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of the Financial Institution.

_____ (Signature & Date)

_____ (Signature & Date)

Annexure 3

[IQ EQ Fund Services (Mauritius) Ltd / IQ EQ Corporate Services (Mauritius) Ltd / IQ EQ Trustees (Mauritius) Ltd/IQ EQ Global Administrators (Mauritius) Ltd][36] (the "Administrator")
33 Edith Cavell Street
Port-Louis
Mauritius

Dear Sir or Madam,

Re: [*Name[37] of Introduced Party*], the "Introduced Party" of [*Address[38] of Introduced Party*] in relation to [*Name of Serviced Entity*], the Serviced Entity as [*Capacity of the Introduced Party*]

I/We hereby certify that in accordance with the provisions[39] of the Financial Intelligence and Anti-Money Laundering Act 2002[40] ("FIAMLA"), the Financial Intelligence and Anti-Money Laundering Regulations 2018 ("FIAML Regulations 2018"), the Financial Services Act 2007 and the Anti-Money Laundering and Combatting of the Financing of Terrorism Handbook ("FSC AML/CFT Handbook") issued by the Financial Services Commission, as amended from time to time, and/ or equivalent legislations and regulations [*please state relevant AML/CFT legislations and regulations in your jurisdiction*] that:

(i) I/We have identified and verified the Introduced Party and confirm that documentary evidence[41] has been obtained (as applicable):
- The above-named Introduced Party;
- Each beneficial owner and controller of the above-named client;
- Each third party for whom the above-named client is acting (and each beneficial owner and controller of that third party); and
- Each person purporting to act on behalf of the above-named client;

(ii) I/We confirm that I/we have not relied upon any other party to apply verification measures in relation to the Introduced Party, nor have we applied simplified or reduced identification measures (unless permitted under local regulation to do so);

(iii) The purpose and intended nature of the business relationship[42] is:

(iv) Original or certified copies of Customer Due Diligence documentation will be made available to the Administrator**, upon request without any delay[43]**;

(v) The ultimate beneficial owner(s) of the Introduced Party is/are:

---

[36] Please amend as appropriate.

[37] The name should be as per passport or document issued by a government/regulatory body.

[38] Current residential address and permanent residential address for a natural person or registered/business address for a legal person/arrangement.

[39] Regulations 3 and 21 of the FIAML Regulations 2018

[40] Section 17C of the FIAMLA

[41] The Customer Due Diligence information relating to the above mentioned parties, together with a structure chart, would have been provided to the Administrator at the time of on-boarding and upon changes.

[42] This is with respect to the relationship between the introduced party and the introducer.

[43] Upon request without delay will be maximum two working days.

Full Name	Address

(vi) I/We will inform the Administrator of any change in the structure provided and provide the updated structure chart including details on all principals[44] involved and up to the ultimate beneficial owner(s) (natural person) immediately;

(vii) The Introduced Party is applying on his/her own behalf and not as nominee, trustee or in a fiduciary capacity for any other person;

(viii) I/We am/are unaware of any activities of the Introduced Party that cause me/us to suspect either that the Introduced Party is engaged in money laundering or any other form of criminal conduct;

(ix) (a) I/We further undertake to keep the due diligence documents for the duration of the relationship and for a period of at least seven years thereafter; *(To delete clause if not applicable)*

OR

(b) The record keeping requirement in our jurisdiction is [*insert your legal record keeping period requirement]*. I/We undertake to provide the due diligence documents to you after termination of the relationship and within a period of two working days;

(x) I/We undertake to advise you promptly in case I/we cease to have a business relationship with the Introduced Party and/or unable to comply with the above undertakings or no more hold a regulated status;

(xi) I/We will provide the Administrator with the relevant documentation, including our AML/ CFT policies and procedures[45] or alternatively complete and sign off on the Wolfsberg [FCC/CBDD[46]] Questionnaire provided to me/us.

I/We hereby undertake to provide the aforementioned due diligence documentation to the Administrator as and when required to enable it to discharge its duties under Mauritian Law **upon request without delay[47]**.

I/We agree to indemnify and hold you harmless from and against any loss, liability, claim, damage or expense suffered or incurred by you or any of your affiliates as a result of your acting in reliance on this declaration but only to the extent that we have acted or omitted to act out of negligence, bad faith or willful default.

We understand that the Administrator agrees to expedite the proposed transaction based on the above undertaking and information and that testing of this arrangement will be done within one year of the execution of this document and thereafter on a regular basis. [*We further understand that the Administrator is required to table a report to the Serviced Entity*

[44] Principals will include the directors and shareholders..

[45] The AML/CFT policies & procedures should cover Politically Exposed Persons, Targeted Financial Sanctions, Customer Due Diligence, Enhanced Due Diligence, Transaction Monitoring, Suspicious Transactions Reporting and Anti-Bribery & Corruption.

[46] The Wolfsberg CBDD Questionnaire will need to be completed by any financial institution which is involved inpooling of funds or provides omnibus accounts.

[47] Refer to footer 43.

detailing the outcome of the testing exercise in line with Section 8 of the FSC AML/CFT Handbook[48]].

Yours faithfully,
[Signature]

Full name of Third Party:	
Full Address of Third Party:	
Name of Regulator:	
Country of Regulator:	
Registration Number:	
Full name of declarant:	
Designation of declarant:	
Date:	

[48] Applicable for reporting entities only (for e.g, funds) – Hence, this section need to be removed if not applicable.

Annexure 4

INTERNAL STR FORM

Part 1 Report Type and Reporting Person

1.1	Name of Reporting Person	
1.2	Team/Department	
1.3	Reporting Date	
1.4	Name of Reporting Officer	
1.5	Designation of Reporting Officer	

1.6 Reason for Suspicion

1.7 Action taken

1.8 Indicators

Refer to Data Sheet (below) for list of Indicators

Part 2 Transaction

2.1	Transmode Code	
2.2	Local Amount	
2.3	Date	
2.4	Description	
2.5	Comments	
2.6	Location	

2.7 Transaction Type

Transaction Type	
Multiparty	

Involved Party No.1	
Role	
Country	
Funds Code	
Comments	

Foreign Currency

Currency (eg USD, EUR, etc)	
Exchange Rate (as at date of transaction)	
Amount	

The Party is	My Client/ Not My client
Party Type	Person/ Account/ Entity

Part 3 Person:

The Party is	My Client/ Not My client
Party Type	Person/ Account/ Entity
Person	
Title	
First Name*	
Middle Name	
Last Name*	
Gender*	
Birth Date*	
Maiden Name	
Alias	
NIC	
ID Number	
Nationality 1*	
Nationality 2	
Nationality 3	
Residence*	
Tax number	
Source of wealth	
Passport	Yes/No
Deceased	Yes/No
Phone	
Contact Type*	
Comm. Type*	
Number*	
Comments	
Address	
Type*	
Address*	
City*	
Country*	
Comments	
Identification	
Type*	
Number*	
Issue Date	
Expiry Date	
Issued by	
Issued Country*	
Comments	
Email Address*	

Part 4 Account:

Account*	
Institution Name*	
Name*	
Branch	
Non Banking Institution?	Yes/ No
CODE or SWIFT?	Institution Code/ Swift
Account Type*	
Status Code	
Currency Code	
Beneficiary	
IBAN	
Client Number	
Opened*	
Closed	
Balance*	
Date of Balance*	
Signatories*	

Part 5 Entity:

Name*	
Business*	
Incorporation Legal Form	
Incorporation Number*	
Incorporation Date	
Incorporation State	
Incorporation Country Code	
Tax Number	
Comments	
Business Closed?	Yes/No

DATA SHEET

Code	Indicators
BRI	Business Relationship with Suspect is an Insider no longer affiliated with Reporting Institution
BRIS	Business Relationship with Suspect is an Insider still affiliated with Reporting Institution
CBRWF	False declaration or failure to declare
IDA	Automated rules based account monitoring
IDB	In-branch/ Teller identified
IDC	Manual account monitoring
IDD	Manually Identified
LOFAC	Appear on OFAC or other list
MIS	The transaction has a material impact on the financial soundness of the reporting institution
OA	Corruption
OB	Narcotic Drugs and Psychotropic substances
OC	Fraud
OD	Money laundering
OE	Participation in organised criminal group/ racketeering
OF	Proliferation
OG	Tax evasion/ Smuggling/ Tax Crimes
OH	Terrorism/ terrorist financing
OI	Trafficking in human beings and migrant smuggling
OJ	Sexual Exploitation including sexual exploitation of children
OK	Illicit arms trafficking
OL	Illicit trafficking in stolen and other goods
OM	Counterfeiting currencies
ON	Counterfeiting and piracy of products/ IPR breaches
OO	Environmental Crime
OP	murder and grievous bodily injury
OQ	Kidnapping, illegal restraint, hostage taking
OR	Robbery or theft
OS	Extortion
OT	Forgery
	Other
OU	Piracy
OV	Insider Trading/ market manipulation
OX	Illegal exchange of FX/ Illegal Money Value Transfer Services
PEPI	Involves international PEPs
PEPL	Involves local PEPs
RADVC	Adverse reports that have appeared on commercial, e.g., World Check
RADVI	Adverse reports that have appeared on international press (including internet)
RADVL	Adverse reports that have appeared on local press
TA	Activity does not match client profile
TB	Purchase of securities or high value goods

TC	Smurfing
TD	Structuring
TE	Trade based money laundering
TF	Use of casinos and gaming activities
TG	Use of nominees and trusts
TH	Use of Hawala or alternate money remittance
TI	Use of offshore financial services
TJ	Use of shell companies
TK	Use of family members and third parties
TL	Use of gatekeepers
TM	Use of new payment technologies/ methods
TN	Denomination Conversion
TR	Suspicious behaviours/ Reluctance to provide details and documents

Account Status Code
Active
Closed by customer
Closed by reporting entity
Closed due to inactivity
Dormant
Inactive
Inactive (no transactions within 1 year)
New account
No account associated, other relationship with customer
UNKNOWN

Address
Business
Operational
Private
Registered
UNKNOWN

Transmode Code
ATM
Card Purchase (Credit/Debit)
Courier
Currency exchange
Denomination Exchange
Deposit
Electronic transaction
In-branch/Office
Inquiry
Insurance (Purchase/ Redeem/ Claim)
Inter bank transfer (domestic bank to domestic bank via SWIFT/MACSS)
Lease

Loan Disbursed
Loan Repaid/ Waived
Mail deposit
Other
Proposed transactions
Purchase
Purchase of negotiable instrument
Refund
Sale
Sale of negotiable instrument
Transfer (to other party)
Transfer (to self, other account)
Transport across border (BCR)
Unknown
Void/ Cancellation
Wire Transfer
Withdrawal

Funds Code
Bank draft
Bearer bond
Bill of exchange
Card (Credit/ Debit)
Cash
Cash (different currency than the from/to side
Cash (different denomination from the from/ to side)
Casino chips
Certificate of deposit
Cheque
Counterfeit
Credit
Currency exchange
Deposit
E-currency (funds held in digital currency, bullions, etc)
Electronic funds transfer
Electronically held funds
From Account
Hotel Transaction
Insurance Policy (Life/ General)
Loan
Money order
NGOs, Charity
Other
Other negotiable instrument
Promissory note
Real Estate

Securities/ Shares/ Stock
Transfer self
Traveller's cheques
UNKNOWN

Incorporation Legal Form
Company
Corporation
Foundation
Funds
General Partnership
Global Business Category 1
Global Business Category 2
Incorporated
International Business Company
Limited Liability Partnership
Limited Partnership
Look through Company
Other
Partnership
Private Limited
Proprietary Limited Company
Protected Cell Company
Public Limited
Societe Civile
Societe Commerciale
Sole Proprietorship
Trusts
Unknown
Unlimited

Role
Instructed
Introducer
Issued Shares/Stock
Leased (from)
Leased (to)
Loan holder
Office Bearer
Other
Outgoing
Partner
Payee/ receiver
Payer / Sender
Proposed

Prospective Client
Provided Item for hire
Provided service
Received service
Registered owner (current)
Registered owner (previous)
Rentee
Rentor
Seller
Settlor
Sold on behalf of
Source party
Suspected beneficiary or on whose behalf
Trustee
Unknown

Account Type
Arrangement
Business
Credit
Current
Foreign currency account
Mortgage
Other
Personal account
Safe deposit box
Savings
Term Deposit
Trading Account
Trust Account
UNKNOWN