CHRYSCAPITAL

Anti-Money Laundering and Combatting Financing of Terrorism Compliance Policy

Release date	10 November 2020
Distribution	All Employees and Partners

Amendment Sheet			
Sr. No.	Date	Revision Status	Reason for Amendment
1.	10 November 2020	Initial Release	NA
2.	11 November 2021	First Amendment	Updates with (1) recommendations of FSC (2) internal enhancements like training (3) revised FSC AML Handbook released in March 2021 (4) internal legal review
3.	3 March 2023	Second Amendment	i) Updates for structured training for directors and sample Internal Disclosure Form. ii) Updates for World Check One Ongoing screening, Sanctions Memo and employee ongoing screening is on UN Sanction lists only. iii) Updates with respect to (i) revised FSC AML Handbook released in September 2022 (ii) recommendations of FSC (during inspections) and other general updates.
4.	December 2024	Third Amendment	Re-assessment of AML/CFT Framework and other general updates which include: Updates with respect to digital signature Section 2 – Regulations and Guidance: Remove link to POCA and add link to FCC Act 2023
5.	November 2025	Fourth Amendment	Following updates made: i) Inclusion of offences under FCC Act in Section 1 ii) Inclusion of NRA 2025 in Section 1 iii) Changes in the requirements for Introducer Certificate Testing and Omnibus Account Testing Changes in the Transaction Monitoring process.

CHAPTER 1: REGULATORY REQUIREMENTS

Scope and Background

The Group as part of its Financial Services Commission ("FSC") licensing conditions is required to adopt, enforce, and re-assess on an annual basis its AML/CFT framework. The aim of this AML/CFT framework is for the Group to comply with its licensing conditions in meeting its statutory requirements in relation

to the identification and combatting laundering of criminal proceeds, the financing of terrorism and the financing of proliferation of weapons of mass destruction (henceforth referred to collectively as "ML and TF").

As per the Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020 ("FSC Handbook 2020") in order to combat ML, the FSC finds it vital that all Financial Institutions ("FIs"), as defined by The Financial Intelligence and Anti- Money Laundering Act 2002 (as amended from time to time) ("FIAMLA 2002"), in Mauritius to exercise appropriate care and diligence to ensure that neither it nor any services offered by it are used by anyone who is a criminal or whose intentions are to launder the proceeds of crime or to engage in terrorist financing. The implementation of, and adherence to, effective Customer Due Diligence ("CDD") and vigilance procedures play a central role in the prevention of ML and TF by its Licensees .

Apex Financial Services (Mauritius) Ltd ("AFSML") (previously known as SANNE Mauritius) is a management company licensed by the FSC and is also required to abide by the relevant laws and regulations. AFSML has an AML/CFT manual in place incorporating the requirements prescribed by the AML/CFT laws.

AFSML and the CC Entities/ the Group under its management were previously abiding by the Code on the Prevention of ML & TF 2012 (as amended from time to time) ("FSC Code 2012") which has been repealed as of 6 November 2020.

However, as per a communique issued by the FSC on 6 Nov 2020, the revocation of the FSC Code 2012 shall not affect any obligations or liability incurred under it, including any previous operations or anything duly done or suffered, as well as any regulatory action already taken as a result of non-compliance with the repealed FSC Code 2012, and any investigation carried out under it.

Being the Management Company of the Group, this AML/CFT framework emanates from AFSML AML/CFT Manual. Chapter 1 has been mostly derived and quoted from FSC Handbook 2020 while Chapter 2 is more specific to the Group's controls and processes approved by its respective Boards.

I. Regulations and Guidance:

The Group is considered a 'FI' under the FIAMLA 2002 and have statutory obligations to comply with the different legislations mentioned below.

1. Mauritian Legislation

Acts (links of the different Acts referred to above):

Financial Intelligence and Anti-Money Laundering Act 2002 ("FIAMLA 2002")

- https://www.fscmauritius.org/media/3652/finan cial-intelligence-and-anti-money-laundering-act-2002.pdf

Financial Intelligence and Anti Money Laundering Regulations 2018 ("FIAML Regulations 2018")

- https://www.fscmauritius.org/media/81433/financial-intelligence-and-anti-money-laundering-regulations-2018.pdf

Financial Intelligence and Anti Money Laundering (Registration by Reporting Person) Regulations 2019 ("FIAML Regulations 2019")

- Reference can be done to the circular issued by FSC on same: https://www.fscmauritius.org/media/85176/fsc-communique-registration-of-reporting-persons.pdf

FIAMLA (Amendment of Schedule) Regulations 2022

- https://www.fiumauritius.org/fiu/wp-content/uploads/2022/08/185-The-Financial-Intelligence-and-AntiMoney-Laundering-Act-Amend-of-Schedule-Reg-2022.pdf

Handbook:

Anti-Money Laundering and Combatting the Financing of Terrorism Handbook 2020 ("FSC Handbook 2020")

- https://www.fscmauritius.org/media/131386/updated-aml-cft-handbook.pdf

Other relevant Acts:

The Financial Crimes Commission Act 2023
Prevention of Terrorism Act 2002

- https://www.fscmauritius.org/media/1140/prevention_of_terrorism_act2002.pdf

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

- https://www.fscmauritius.org/media/77953/the-united-nations-financial-prohibitions_-arms-embargo-_-travel-ban-sanctions-act-2019.pdf

AML and CFT (Miscellaneous Provisions) Act 2019

- https://www.fscmauritius.org/media/78008/9_the-anti-money-laundering-and-combatting-the-financing-of-terrorism-and-proliferation-miscellaneous-provisions-act-2019.pdf

AML and CFT (Miscellaneous Provisions) Act 2020

- https://www.fscmauritius.org/media/84981/the-anti-money-laundering-and-combatting-the-financing-of-terrorism-and-proliferation-miscellaneous-provisions-act-2020.pdf

The Financial Services Act 2007 ("FSA 2007")

- https://www.fscmauritius.org/media/84940/financial-services-act-2007pdf.pdf

Other Guidelines:

Guidelines on the Implementation of Targeted Financial Sanctions (TFS) under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 ("Sanctions Guidelines 2020")

- https://www.fscmauritius.org/en/being-supervised/amlcft/guidelines-on-the-implementation-of-targeted-financial-sanctions-tfs-under-the-united-nations-financial-prohibitions-arms-embargo-and-travel-ban-sanctions-act-2019

Guidelines on Fitness and Propriety

- https://www.fscmauritius.org/media/85115/circular-letter.pdf
- https://www.fscmauritius.org/media/85113/guide-to-fitness-propriety-with-pq.pdf

The above-mentioned Acts/Guidelines/Regulations are not intended to be exhaustive.

Section 17A of the FIAMLA 2002 states that:

1. Every reporting person shall:
   a) Establish policies, controls, and procedures to mitigate and effectively manage the risks of money laundering and terrorism financing identified in any risk assessment undertaken by the reporting person under Section 17 of FIAMLA 2002;
   b) Monitor the implementation of, regularly review, update and, where necessary, enhance the policies, controls and procedures established under paragraph (a);
   c) Maintain a record in writing of –
      i) The policies, controls and procedures established under paragraph (a)
      ii) Any changes to those policies, controls and procedures made as a result of the review and update required under paragraph (b); and
      iii) The steps taken to communicate those policies, controls and procedures, or any changes to them, internally.
2. The policies, controls and procedures adopted under paragraph (1) shall be proportionate to the size and nature of the business of a reporting person, as the case may be, and approved by its senior management.

The Group being a reporting person must be in compliance with Section 17A of the FIAMLA 2002 and the AML/CFT Framework has been drafted in line with Section 17A of the FIAMLA 2002.

The FIAMLA and FIAML Regulations 2018 state offences related to money laundering and terrorist financing (as explained above). Some of these offences, as applicable to financial institutions, are listed below for ease of reference:

A. Section 3 of the FIAMLA states that:

1. Any person who
   a) engages in a transaction that involves property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime; or
   b) receives, is in possession of, conceals, disguises, transfers, converts, disposes of, removes from, or brings into Mauritius any property which is, or in whole or in part directly or indirectly represents, the proceeds of any crime, where he suspects or has reasonable grounds for suspecting that the property is derived or realized, in whole or in part, directly or indirectly from any crime, shall commit an offence.
2. A reporting person who fails to take such measures as reasonably necessary to ensure that neither he, nor any service offered by him, 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.

B. Section 4 of the FIAMLA states:

Without prejudice to section 109 of the Criminal Code (Supplementary) Act, any person who agrees with one or more other persons to commit an offence specified in section 3(1) and (2) shall commit an offence.

C. Section 5 of the FIAMLA states:

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

D. Section 8 of the FIAMLA states:

1. Any person who –
   a) commits an offence under this Part; or
   b) disposes or otherwise deals with property subject to a forfeiture order under subsection (2), shall, on conviction, be liable to a fine not exceeding 10 million rupees and to penal servitude for a term not exceeding 20 years.
2. Any property belonging to or in the possession or under the control of any person who is convicted of an offence under this Part shall be deemed, unless the contrary is proved, to be derived from a crime and the Court may, in addition to any penalty imposed, order that the property be forfeited.
3. Sections 150, 151 and Part X of the Criminal Procedure Act and the Probation of Offenders Act shall not apply to a conviction under this Part.

E. Section 16(1) of FIAMLA states:

Any reporting person and its officers shall not disclose to any person that a suspicious transaction report is being or has been filed, or that related information is being or has been requested by, furnished, or submitted to FIU.

F. Section 16(3a) of FIAMLA states:

Any person who fails to comply with subsection (1) shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

G. Section 17(c)(6) of FIAMLA states:

Customer due diligence requirements

Any person who knowingly provides any false or misleading information to a reporting person in connection with CDD requirements under the FIAMLA or any guidelines issued under this Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding 500, 000 rupees and to imprisonment for a term not exceeding 5 years.

H. Section 19 of FIAMLA states:

Offences relating to obligation to report and keep records and to disclosure of Information prejudicial to a request

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

a) fails to comply with section 17, 17A, 17B. 17C, 17D, 17E, 17F or 17G;

b) destroys or removes any record, register or document which is required under this Act or any regulations; or

c) facilitates or permits the performance under a false identity of any transaction falling within this Part,

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

2. Any person who –

a) falsifies, conceals, destroys, or otherwise disposes of or causes or permits the falsification, concealment, destruction or disposal of any information, document or material which is or is likely to be relevant to a request to under the Mutual Assistance in Criminal and Related Matters Act 2003; or

b) knowing or suspecting that an investigation into a money laundering offence has been or is about to be conducted, divulges that fact or other information to another person whereby the making or execution of a request to under the Mutual Assistance in Criminal and Related Matters Act 2003 is likely to be prejudiced, shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

I. Section 19e of the FIAMLA provides that:

Duty to provide information for purpose of conducting risk assessment

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

J. FIAML Regulations 2018

Regulation 33 of FIAML Regulations 2018 states that any person who contravenes regulations under FIAML Regulations 2018 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.

Failure to comply with the FIAMLA 2002 and FIAML Regulations 2018 may result in regulatory action.

The FSC has also published the Financial Services (Framework for the Imposition of Administrative Penalties) Rules 2022 which has come into operation on 1 October 2022.

In addition, the FSC issued the Enforcement Manual on 12 June 2020 which sets out the overall approach of the FSC to the exercise of its enforcement powers where relevant laws/guidelines have been breached.

Furthermore, Mauritius went through its first National Money Laundering and Counter Terrorism Financing Risk Assessment ("NRA") in 2019. The aim of this assessment was to provide Mauritius with an effective pathway to implementing a risk-based AML/CFT regime, through the efficient allocation of resources and the adoption of measures to prevent and mitigate ML and TF.

International Guidelines

Mauritius fully supports international initiatives to prevent ML and to combat TF. All relevant international standards, FSAP Recommendations and national commitments are taken into account which include (i) the Financial Action Task Force's (FATF) Recommendations (ii) the Basel Committee's Paper on Customer Due Diligence; (iii) IOSCO's Principles on Client Identification and Beneficial Ownership for the Securities Industry; (iv) IAIS' Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities; (v) the recommendations made by IMF/World Bank Assessors in FSAP 2007 on how certain aspects of the system could be strengthened; and

(vi) aligning with other Codes issued to FIs i.e. guidance notes issued by Bank of Mauritius to ensure one form of language for enforceable measures and for guidance.

[10]As per the Financial Intelligence and Anti- Money Laundering Act 2002 (as amended from time to time) ("FIAMLA 2002"), Financial Institution means – (a) an institution or a person, as the case may be, licensed, registered or authorized under – (i) section 14, 77, 77A or 79A of the Financial Services Act; (ii) the Insurance Act, other than an insurance salesperson; (iii) the Securities Act other than an entity registered with that Act as a reporting issuer and which does not conduct any financial activities; (iv) the Captive Insurance Act; or (v) the Trusts Act as a qualifies trustee; (vi) section 12 of the Private Pension Schemes Act; (vii) the Virtual Asset and Initial Token Offering Services Act 2021 or (b) a credit union

[11]Can also be termed as Financial Institution

[12]https://www.fscmauritius.org/media/131404/fs-framework-for-the-imposition-of-admin-penalties-rules-2022.pdf

[13]https://www.fscmauritius.org/media/84954/enforcement-manual.pdf

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

[15]https://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf

II. Overview of ML, TF, and Proliferation Offences:

ML and TF Risk Analysis

ML is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. The goal of a money launderer is to disguise the origin and ownership of the money so that it appears to have come from a legitimate source. Traditionally, ML will often involve a complex series of transactions, represented in three separate phases which are placement, layering and integration. Reference can be made to FSC Handbook 2020 for more details on these three phases. However, the FSC Handbook 2020 also suggests that rather than getting caught up in trying to establish whether an activity relates to a particular phase of the traditional model, the financial institutions should ask themselves – "do I know, suspect, or have reasonable ground to suspect that the assets in question are derived from criminal activities?" The assets do not have to be linked or suspected to be linked to a specific act of ML.

TF is the financial support, in any form, of terrorism or those who encourage, plan, or engage in terrorism. TF often involves a complex series of transactions, generally considered as representing three separate phases which are collection, transmission, and use. Reference can be made to FSC Handbook 2020 for more details.

Proliferation of weapons of mass destruction ("WMDs") can be in many forms, but ultimately involves the transfer or export of technology, goods, software, services, or expertise that can be used in programmes involving nuclear, biological, or chemical weapons, and their delivery systems (such as long-range missiles). Unscrupulous persons may also take advantage of the potential profits to be made by facilitating the movements of sensitive materials, goods, technology, and expertise, providing seemingly legitimate front organizations, or acting as representatives or middlemen.

As listed above, the FIAMLA 2002 and FIAML Regulations 2018 state offences related to ML and TF which cover (a) persons or FIs engaging in transactions involving proceeds of crime (b) cash transactions above prescribed threshold (c) failure to report suspicious transactions (d) any person providing false CDD (e) failure to keep and provide information to local authorities, etc.

III. Corporate Governance:

1. Board and Senior Management

They have a responsibility to ensure that a FI's systems and controls are appropriately designed and implemented and are effectively operated to reduce the risk of the business being used in connection with ML/TF. They must establish documented systems and controls which, inter alia, undertake risk assessments of its business and its customers , determine the true identity of customers and any beneficial owners and controllers, apply increased vigilance to transaction and relationships posing higher risks of ML/TF, etc.

The Board must take ownership of, and responsibility for, the business risk assessments and ensure that they remain up to date and relevant. On the basis of its business risk assessment, the Board must establish a formal strategy to counter money laundering and financing of terrorism, including provision as to the extent and frequency of compliance reviews.

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 FI occur.

Any appointment of an officer or admission of a shareholder by the FI should be made in line with the Guidelines on Fitness and Propriety issued by the FSC, wherever applicable.

[16]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) a signatory to a transaction or account (b) any person to whom an account or rights or obligations under a transaction have been assigned or transferred; (c) any person who is authorized to conduct a transaction or control an account; (d) any person who attempts to take any action referred to above; (e) an applicant for business.

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

2. Appointment of Compliance Officer ("CO")

In line with Regulation 22 (1) (a) of FIAML Regulations 2018, a FI needs to designate a CO, who must be a natural person, at senior management level and the latter must be an approved officer by the FSC under Section 24 of the FSA 2007.

The CO must have the appropriate qualification knowledge, skill and experience in accordance with the Competency Standards issued by the FSC in October 2014 and updated as at 9 June 2022: https://www.fscmauritius.org/media/127924/amendments-to-competency-standards-with-respect-to-money-laundering-reporting-officer-and-compliance-officer-june-2022.pdf.

The CO will be responsible for the implementation and ongoing compliance of the FI with internal programs, controls, and procedures with the requirements of the FIAMLA 2002 and FIAML Regulations 2018.

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

a) Ensuring continued compliance with the requirements of the FIAMLA 2002 and FIAML Regulations 2018 subject to the ongoing oversight of the Board of the FI and senior management;

b) Undertaking day-to-day oversight of the program for combatting ML and TF;

c) Regularreporting, includingreportingofnon-compliance, tothe Boardandseniormanagement; and

d) Contributing to designing, implementing, and maintaining internal Policy Handbooks, policies, procedures, and systems for combatting ML and TF.

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

3. Appointment of Money Laundering Reporting Officer ("MLRO")

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

As per the FSC Handbook 2020, the MLRO should be a natural person and an approved officer by the FSC under Section 24 of the FSA 2007. The MLRO must have the appropriate knowledge, skill, and experience in accordance with the Competency Standards issued by the FSC in October 2014 and updated as of 9 June 2022 as mentioned in above link.

The MLRO is the person who is nominated to ultimately receive internal disclosures and who considers any report to determine whether an external disclosure is required to be done to the Financial Intelligence Unit ("FIU"). In the absence of the MLRO, the FSC requires the appointment of a Deputy MLRO who should be of similar status, qualification, and experience to the MLRO.

The MLRO should be the main point of contact with the FIU in the handling of disclosures.

In the absence of the MLRO, the Deputy MLRO ("DMLRO") is expected to fulfil similar duties, as provided, and explained above.

The filing of the STR with the FIU should be done within 5 working days of the date the suspicious transaction has been found.

4. Non-compliance or Non-adherence to Procedures as set out in this AML/CFT Framework

Non-compliance or non-adherence to procedures as laid down in this AML/CFT Framework and AFSML's AML/CFT Manual (where appropriate) by any officer of the Group or AFSML officer might lead to disciplinary action and breaches will be actively monitored by the CO or any other relevant authority put in place by the Board.

[18]For the avoidance of doubt, the same individual can be appointed to the positions of MLRO and CO, provided the Financial Institution considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively

[19]As defined in the FIAML Regulations 2018

IV. Risk Based Approach:

1. Business Risk Assessment ("BRA")

A FI must, under Section 17(1) of the FIAMLA 2002 identify, assess, understand, and monitor its own ML and TF risks. The BRAs are designed to assist the FI in making such an assessment and provide a method by which the FI can identify the extent to which its business and its products and services are exposed to ML and TF.

While performing business, Management, Compliance and Risk Management should all work together in performing the BRA. Primarily, responsibility for the quality and execution of the risk analysis lies with the first line of defense. The role of Compliance is process monitoring, facilitating, and testing. Other functions or departments such as Audit can also provide the necessary input. The ultimate responsibility for the BRA lies with the Board of directors of the Group.

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

It is important to note that risks to FIs may change as a result of both internal and external factors. The FI's activities may for instance be expanded or changed, specific trends may emerge in the financial and economic world or laws and regulations may be amended.

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

Section 17(2) of the FIAMLA 2002 requires businesses to assess 6 key areas when undertaking the BRA amongst other risk factors:

a) The nature, scale, and complexity of the FI's activities. For instance, an assessment needs to be done whether large volume and more complex transactions may pose higher risk of ML than less complex and voluminous transactions;

b) The products and services provided by the FI. For instance, where payments are allowed to any unknown or un-associated third parties, this can be a higher risk or non – face- to – face or use of introducers can increase the risk;

c) The persons to whom and the manner in which the products and services are provided. For instance, the involvement of Politically Exposed Persons ("PEPs"), high net worth individuals, persons from higher risk jurisdictions, etc. will entail more risk;

d) The nature, scale, complexity, and location of the customer's activities. For instance, country or territory subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the UN or the EU, will pose higher risk;

e) Reliance on third parties for elements of the customer due diligence process. For instance, the extent and type of any reliance placed or to be placed on third parties will affect risk; and

f) Technological developments which will include an assessment of operational, reputational, and legal risks. For instance, the potential loss that could be incurred due to significant deficiencies in system reliability or integrity.

As per Section 17(2) (b) of the FIAMLA 2002, FIs shall take into account the findings of the NRA and any guidance issued in their BRA. As per the latest NRA report, the ML threat of the Securities Sector has been assessed as Medium-High. The main activities which are more vulnerable to ML are Collective Investment Schemes, Closed-End Funds, and Investment Advisers, primarily because of their size, complex structures, high value of assets and use of sophisticated products. The overall TF risk in Mauritius is Medium given the TF threat is rated Medium- Low and TF vulnerability is rating Medium-High.

The above risk factors are part of a non-exhaustive list, and it is for the FI 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 BRA, the FI has to demonstrate how effective and robust its BRA is in line with its inherent risks and vulnerabilities and the Commission will assess to what extent the BRA conducted reflect residual risks faced by the FI.

Reference can be done to the FSC Handbook 2020 for more detailed explanation on the different relevant risk factors to be considered when conducting a BRA.

2. Customer Risk Assessment ("CRA")

The CRA, that is assessing the risk of ML/TF posed by a customer, must be undertaken prior to the establishment by a FI of a business relationship or carrying out an occasional transaction, with or for, that customer. This risk assessment must be documented in order to be able to demonstrate its basis. It should be a living document that is revisited and reviewed, as and when more information about the customer and relationship is obtained.

As per the FSC Handbook 2020, the customers may be risk rated on the following:

a) Customer Risk

b) Countries and Terrorist Risk

c) Products, Services and Transaction Risk

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

Regarding frequency of the reviews, it is recommended as per the Handbook that CRAs should be reviewed:

a) At least annually for higher risk customers or whenever a transaction with a high-risk country or high-risk customer occurs;

b) At least every 3 years for standard risk customers subject to sector specific guidance; and

c) At the point of a material change in the customer's circumstances, for example establishing connections with a higher risk jurisdiction or engaging in a higher risk business.

The above are only examples of suggested review frequency, a FI may decide to different frequency level should their business and client risk assessments merit same, as long as this can be justified and is properly documented.

V. Customer Due Diligence ("CDD"):

FIs must identify their customers, and where applicable, their beneficial owners and then verify their identities, which is essential to the prevention of ML and combatting the TF.

Section 17C of FIAMLA 2002 has elaborated circumstances where CDD are required.

CDD information is also a vital tool for the MLRO and employees when examining unusual or higher risk activity or transactions, in order to determine whether a STR will be appropriate. If a FI forms a suspicion that one or more actual or proposed transactions relates to ML or TF, it should take into account the risk of tipping off when performing the CDD process. If the FI reasonably believes that performing the CDD process will tip off the customer or potential customer, it should stop the CDD process and will need to file a STR in such circumstances. Tipping off is an offence.

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

1) The identity of the third party (and any beneficial owners or associated persons as required);
2) The proofs of identity required under Regulation 3 of the FIAML Regulations 2018; and
3) The relationship between the third party and the applicant for business.

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

1. Identification and Verification

Regulation 3(1) of the FIAML Regulations 2018 imposes an obligation for a FI to identify its customer whether permanent or occasional and verify the identity of its customer.

The FSC Handbook 2020 and FIAML Regulations 2018 has provided guidance on Data/CDD to be collected on natural persons, legal persons , legal arrangements and individuals acting on behalf of applicants for business and customers.

It is important to note that for customers that are legal persons or legal arrangements, FI should identify and verify the identity of beneficial owners by obtaining information on:

a) The identity of all the natural persons who ultimately have a controlling ownership interest in the legal person;

b) Where there is doubt under subparagraph (a) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising effective control of the legal person; and

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

[20]As per the FIAML Regulations 2018, the applicant for business means a person who seeks to establish a business relationship or carries out an occasional transaction with a reporting person.

[21]As per FIAMLA 2002 legal person means any entity other than a natural person; and includes a company, a foundation, an association a limited liability partnership or such other entity as may be prescribed;

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

2. Source of Funds/Source of Wealth

FIs must keep and maintain customer relationship information with respect to all its customers and this would include scrutinizing the source of funds and the source of wealth , as required. A FI is required to hold sufficient information to establish the source of wealth and this information must be obtained for all higher risk customers (including higher risk PEPs) and all other relationships where the type of product or service being offered makes it appropriate to do so because of its risk profile.

3. Certification

As per the AML/CFT Handbook 2020 updated as of 21 September 2022, copies of the verification of identity documentation can be certified by a suitable person, such as a lawyer, notary, actuary, an accountant, or any other person holding a recognized professional qualification, director, or secretary of a regulated financial institution in Mauritius or meets the FATF's standards, a member of the judiciary or a senior civil servant.

The certifier should sign copy of the document and clearly indicate the date of certification, his or her name, address and position or capacity on it together with contact details to facilitate tracing of the certifier and, where available, any registration number with any professional body.

4. Timing of verification of identity

The FI must take all reasonable measures to complete all CDD measures for all clients prior to the establishment of a new customer relationship and prior to providing any financial service. Where it is necessary to provide financial services to a client prior to completion of CDD measures, the decision to do so must be appropriately authorized by senior management and the reasons recorded in writing.

VI. Enhanced Due Diligence ("EDD"):

As per Regulation 12(1) of the FIAML Regulations 2018, a FI shall perform EDD:

1. Where a higher risk of money laundering or terrorist financing has been identified;
2. Where through supervisory guidance a high risk of money laundering or terrorist financing has been identified;
3. Where a customer or an applicant for business is from a high risk third country;

4. In relation to correspondent banking relationships;
5. Where the customer or the applicant for business is a political exposed person;
6. 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;
7. In the event of any unusual or suspicious activity.

The EDD measures that may apply for higher risk relationships as per the FSC Handbook 2020 should include:

1. Requesting additional information on the customer and updating on a frequent basis the customer or the beneficial owner;
2. Obtaining additional information on the intended nature of the business relationship and the source of fund/wealth;
3. Obtaining information on the intended or performed transactions;
4. Obtaining the approval of senior management to commence or continue the business relationship;
5. Conducting close monitoring of the business relationship;
6. Any other measures a FI may undertake with relation to a high-risk relationship.

The FI must also apply enhanced due diligence measures in all high-risk business relationships, customers, and transactions and in particular when dealing with (i) Political Exposed Persons ("PEPs"), (ii) Connected persons that are PEPs and (iii) in non- face to face relationships or occasional transactions that pose higher risk. In addition to above, there are other instances (not exhaustive list) where EDD can be applied which are (i) in event if any unusual or suspicious activity and (ii) adverse media alerts found during screening.

The FI must develop a clear policy on the acceptance of business relationships with such persons; obtain the approval of senior management prior to establishing relationships, 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 apply enhanced due diligence measures to establish the source of funds and source of wealth of such persons.

In case where a FI is unable to perform the required EDD, the latter shall terminate the business relationship and file a STR under section 14 of the FIAMLA 2002.

[23]As per FSC Handbook 2020, senior management includes an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.

[24]Source of wealth is usually requested where there is a requirement to conduct Enhanced Due Diligence

[25]For instance, NRA Report and FSC Guidelines

VII. Simplified Due Diligence:

Simplified CDD measures can be implemented in cases where lower risks have been identified and this corresponds to the situations outlined in Regulation 11 of the FIAML regulations and where the CDD measures are commensurate with the lower risk factors, or any guidance issued. Low risks factors

identified should be in accordance with the National Risk Assessment or any risk assessment recently issued by the regulators.

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

VIII. Third Party Reliance:

A FI 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 FI must ensure that the identification information sought from the third party is adequate and accurate. The CDD information has to be submitted immediately in line with section 17D of the FIAMLA 2002 upon onboarding although the documents can be provided upon request at a later date. Where such reliance is permitted, the ultimate responsibility for CDD measures will remain with the FIs relying on the third party.

In a third-party reliance scenario, the third party should be regulated, supervised, and monitored and subject to CDD in line with section 17C of the FIAMLA 2002 and record keeping requirements pursuant to section 17F of the FIAMLA 2002 and Regulation 21 of the FIAML Regulations 2018 which provides for third party reliance. As per FIAML Regulations 2018, a reporting person shall not rely on a third party based in a high-risk country.

The FSC Handbook clearly mentions what kind of arrangements the FI should have with the third party in order to meet FSC's expectations.

Third parties may not be relied upon to carry out the ongoing monitoring of dealings with a customer, including identifying the source of wealth or source of funds. Reliance shall not be placed on third parties to verify that any person purporting to act on behalf of a customer is so authorized, and to identify and verify the identity of that person.

The FSC recommends that regular assurance testing is carried out in respect of the third-party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient.

Introducers are a form of Third-Party Reliance. The FSC Handbook further elaborates that FI's board of directors or equivalent senior management must ensure that periodic testing of the arrangements listed in the FSC Handbook 2020 on introduced business be conducted by the FI.

IX. Monitoring Transactions and Activity:

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

The type of monitoring applied by the FI will depend on a number of factors and should be developed with reference to the FI's BRAs and risk appetite. Particular attention should be paid to high-risk relationships (for example, those involving PEPs), high risk countries and territories and high-risk transactions.

In accordance with Regulation 3(1) (e) of the FIAML Regulations 2018, FIs should conduct ongoing monitoring of a business relationship, including:

1. Scrutiny of transactions undertaken throughout the course of the relationship, including, where necessary, the source of funds, to ensure that the transactions are consistent with his knowledge of the customer and the business and risk profile of the customer;
2. Ensuring that documents data or information collected under the CDD process are kept up to date and relevant by undertaking reviews of existing records, in particular for higher risk categories of customers.

1. PEPs[26]

In accordance with Regulation 15(1) (b) of FIAML Regulations 2018, where a customer or beneficial owner is or becomes a foreign PEP during the course of an existing business relationship which is deemed high risk, as part of the EDD measures subsequently applied, the FI shall obtain senior management approval to continue that relationship. The same requirement applies in cases when there is higher risk business relationship with a domestic PEP or an international organization PEP as well as family members and close associates (as provided in Regulation 15(5)) of the above-mentioned types of PEPs.

[26](i)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.

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

(iii) International organization PEP means a person who is or has been entrusted with a prominent function by an international organization 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.

[27]As per FIAML Regulations 2018 family members (a) means an individual who is related to a PEP either directly through consanguinity, or through marriage or similar civil forms of partnership; and (b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee

[28]As per FIAML Regulations 2018 close associates (a) means an individual who is closely connected to a PEP, either socially or professionally; and (b) includes any other person as may be specified by a supervisory authority or regulatory body after consultation with the National Committee

2. High Risk Transactions or Activity

When conducting ongoing monitoring, red flags (which have been elaborated in the FSC Handbook 2020) may indicate high risk transactions or activity within a business relationship.

3. Ongoing CDD

The extent of the FI's ongoing CDD measures must be determined on a risk-sensitive basis. However, the FI must be aware that as a business relationship develops, the risks of ML and TF may change.

4. Customer Screening

When conducting searches against the name of an individual or entity, FIs should consider "negative

press" in addition to whether the individual or entity is named on a sanctions or PEP list.

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

The FSC Handbook clearly explains what kind of documentation the FI must have in place when a screening is done.

5. Sanctions

In addition to above, FIs need comply with some specific local obligations under the Sanctions Act 2019 and Sanctions Guidelines 2020. The Sanctions Act 2019 enables the Government of Mauritius to implement targeted sanctions, including financial sanctions, arms embargo and travel ban, and other measures imposed by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations, with a view to addressing threats to international peace and security, including terrorism, the TF and the WMDs. The Sanctions Act 2019 imposes three main targeted sanctions, namely financial prohibitions, arms embargo, and travel ban, against parties listed by or under the authority of the UNSC.

As per the notice issued by the National Sanctions Secretariat ("NSSEC"), the FI must immediately (i.e., without delay and not later than 24 hours) verify whether the details of the Listed Party match with the particulars of any of its customer. If there is a positive match, the FI must identify whether the customer owns any funds or other assets with it, including the funds or assets mentioned above. The FI is required to make a report to the National Sanctions Secretariat and the FSC where funds or other assets have been identified by it.

An internal report must also be made to the MLRO. The MLRO should then file a STR to FIU with any information relating to a Listed Party which is known to it.

Reference can be made to the FSC Handbook 2020 for more details on Monitoring Transactions and Activity.

6. Oversight of Monitoring Process by CO

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

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

If during any monitoring exercise, it is found that the FI is exposed to a risk which it cannot control, the matter shall be brought to the attention of the Board who would take the necessary action in order to protect the business.

Reference can be made to the FSC Handbook 2020 for more details on Monitoring Transactions and Activity.

X. Reporting Suspicious Transactions:

1. Suspicious Transaction Reporting Procedures

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

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

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

It is the responsibility of the MLRO (or if appropriate, the DMLRO) to consider all internal disclosures he/she receives in the light of full access to all relevant documentation.

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

Regulation 29(2) of the FIAML Regulations 2018 and Section 14 of the FIAMLA 2002 states that every reporting person shall, as soon as he becomes aware of a suspicious transaction, needs to make a report to FIU of such transaction not later than 5 working days after the suspicion arose.

In addition, as per Section 14C of FIAMLA 2002, every reporting person shall, within such time and in such form and manner as may be prescribed, register with FIU.

2. Tipping Off

Section 16(1) of the FIAMLA 2002 states that no person (the reporting person and any a director, employee, agent, or other legal representative) directly or indirectly involved in the reporting of a suspicious transaction shall inform any person involved in the transaction or an unauthorized third party that the transaction has been reported or that information has been supplied to the FIU pursuant to a request made under section 13(2) or (3) of the FIAMLA 2002. If the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead the FI should immediately file an STR with the FIU.

Should an employee of the Group be found to be engaged in tipping off, disciplinary action as mentioned in Chapter 1 under Non-compliance or Non-adherence to Procedures as set out in this AML/CFT Framework may be considered by the Board of the Group.

Additionally, Section 16 (3A) of the FIAMLA provides for the offence of tipping off.

3. Offence

As per Section 14 of the FIAMLA 2002, where a FI:

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.

More details on reporting procedures on a suspicious transaction is provided in the FSC Handbook 2020.

XI. Record Keeping:

FIs are expected to have appropriate and effective policies, procedures, and controls in place to ensure that records including transactions are maintained during and after the course of the business relationship, either in the form of original documents or copies for a period of 7 years as required by the legislations.

Reference to FSC Handbook 2020 can be made for more details of record keeping requirements.

XII. Employee Screening and Training:

The FI is required, under Regulation 22(1)(b) of FIAML Regulations 2018, to implement programmes for screening procedures so that high standards are maintained when hiring employees. Furthermore, the FI should also carry out periodic ongoing screening of its employees against the UN's list of designated persons under terrorist and proliferation financing targeted financial sanctions.

Regulation 22(1)(c) of FIAML Regulations 2018 states that programmes against ML/TF should also be in place to include ongoing training programme for the directors, officers, and employees of the FI, to maintain awareness of the laws and regulations relating to ML/TF to:

1. Assist them in recognizing transactions and actions that may be linked to ML/TF; and
2. Instruct them in the procedures to be followed where any links have been identified under sub subparagraph (i).

1. The Board and Senior Management

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

The ongoing training provided by the FI shall cover:

a) The FIAMLA 2002, FIAML Regulations 2018, any AML/CFT Code issued by the FSC and this AML/CFT Framework;

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

c) The FI's policies, procedures, and controls for the purposes of foreseeing, preventing, and detecting ML and TF.

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

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

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

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

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

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

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

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

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

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

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

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

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

Following on-site inspection of FIs, the FSC has also been requesting for evidence of structured training by the directors of the FI. It is therefore important to maintain a register of trainings dispensed.

2. MLRO and DMLRO

Ongoing professional development, including participating in professional associations and conferences, is vital for MLROs/ DMLROs. In addition, MLROs and DMLROs should receive in depth training on all aspects of the prevention and detection of ML/TF as specified under 12.8.2 in the FSC Handbook 2020.

As per the Competency Standards issued by the FSC, MLROs/DMLROs should have a minimum of 10 hours CPD annually.

3. CO

The CO is responsible for ensuring continued compliance with the requirements of the FIAMLA 2002 and FIAML Regulations 2018 subject to ongoing oversight of the Board of the FI and senior management. The CO shall have an overall oversight of the program for combating ML/TF amongst others (Regulation 22 (3) of FIAML Regulations 2018).

The CO should receive in depth training on all aspects of the prevention and detection of ML/TF, including, but not limited to, addressing the monitoring, and testing of compliance systems and controls (including details of the FI's policies and procedures) in place to prevent and detect ML and TF. Effective June 2022, the CO is also required to meet the CPD requirements of at least 10 hours annually further to the updated Competency Standards issued by the FSC.

Reference to FSC Handbook 2020 can be made for more details on employee screening and training.

XIII. Independent Audit:

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

1. Scope of Independent Audit

In line with international best practices, the independent audit exercise should be risk-based, and the scope of the independent audit exercise is mainly a verification of the AML/CFT risk faced by the FI.

Every independent audit should mandatorily test compliance in the non-exhaustive list provided in the FSC Handbook 2020 which includes AML/CFT policies and procedures, internal risk assessments, MLRO function and effectiveness and other areas. Reference can be made to Section 13.2 of the FSC Handbook 2020 for more details.

2. Choosing the Audit Professional

Regulation 22 (1) (d) of the FIAML Regulations 2018 requires the audit process to be carried out independently. The audit function should therefore be independent of and separate from the operational and executive team dealing with the AML/CFT processes of the FI. The audit professional should also have the necessary skills, qualifications, experience, understanding of local AML/CFT regulations and sufficient knowledge of the industry.

3. Assessing the Independence of the Audit Professional

The FI 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 independent service providers/consultants.

When sourcing an external audit professional to conduct the audit, the FI should conduct some level of due diligence as listed in Section 13.3 of the FSC Handbook 2020 to confirm the proposed or selected professional candidate has the requisite competence.

4. Frequency of Independent Audit

The frequency of the Independent Audit should be commensurate with the FI's size, nature, context, complexity, and internal risk assessment. Hence, the greater the AML risk, the greater should be the frequency of audit.

5. Key Components of the AML/CFT Programme

The audit exercise of the FI will involve review and assessment of the framework, together with sample testing of policies and procedures. Reference can be made to be Section 13.5 of the FC Handbook 2020 which includes comprehensive details of the AML/CFT programme and the audit exercise.

6. Audit Outcome, Report, and Recommendations

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

CHAPTER 2: DECISIONS TAKEN/TO BE TAKEN BY THE BOARD

Background:

Name of Company	Details
ChrysCapital Management Company V, LLC	The Company was incorporated on 27 June 2007 and is authorized to operate as a CIS Manager on 5 February 2009. The Company was set up to manage, operate and make all investment decisions of ChrysCapital V, LLC ("the Fund") under the supervision of the Fund's board of directors. ChrysCapital V, LLC has been liquidated in 2019.
Corpus Management Company VI, LLC	The Company was incorporated on 29 February 2012 and is authorized to operate as a CIS Manager on 1 March 2012. The principal activity of the Company is to act as CIS Manager to ChrysCapital VI, LLC a Closed-ended fund, and Lavender Investments Limited, a wholly owned subsidiary of ChrysCapital VI, LLC and also a CIS Expert Fund , both incorporated in Mauritius. Lavender Investments Limited has been liquidated in 2023.
Corpus Management Company VII, LLC	The Company was incorporated on 9 December 2015 and was authorized to operate as a CIS Manager on 14 December 2015. The principal activity of the Company is to act as CIS Manager to ChrysCapital VII, LLC a Closed-ended fund, Auburn Limited, a wholly owned subsidiary of ChrysCapital VII, LLC and also a CIS Expert Fund and CC VII Holdings, LLC (the blocker entity), a Global Business Company. All of the entities are incorporated in Mauritius.
Corpus Management Company VIII, LLC	The Company was incorporated on 2 October 2018 and is authorized to operate as a CIS Manager on the same date. The principal activity of the Company is to act as CIS Manager to ChrysCapital VIII, LLC a Closed-ended fund, Emerald Investments Limited, a wholly owned subsidiary of ChrysCapital VIII, LLC and also a CIS Expert Fund and CC VIII Holdings LLC, a blocker entity holding a Global Business Licence and all incorporated in Mauritius.
Corpus Management Company IX, LLC	The Company was incorporated on 15 November 2021 and was authorized to operate as a CIS Manager on the same date. The principal activity of the Company is to act as CIS Manager to ChrysCapital IX, LLC a Closed-ended fund, Geranium Investments Limited, a wholly owned subsidiary of ChrysCapital IX, LLC and also a CIS Expert Fund, both incorporated in Mauritius, CC IX Holdings, LLC (the blocker entity) and Graphite Investments Limited, both Global Business Companies as well as Defati Investments Holding B.V. and PEF 2022-2023 PASS, C.V.
Corpus Management Company X, LLC	The Company was incorporated on 17 June 2024 and is authorized to operate as a CIS Manager on the same date. The principal activity of the Company is to act as CIS Manager to ChrysCapital X, LLC a Closed-ended fund, Mauve Investments Limited, a wholly owned subsidiary of ChrysCapital X, LLC and also a CIS Expert Fund, both incorporated in Mauritius and ChrysCapital X Holdings, LLC (the blocker entity), a Global Business Company.
ChrysCapital VI, LLC	The Fund was incorporated on 29 February 2012 andis authorized to operate as a Closed End Fund on 1 March 2012. The Company's objective is to make equity and equity related investments to realize superior returns through long term capital appreciation in a diversified portfolio of companies. The Company had investments in listed and unlisted companies in India and USA through its subsidiaries.

ChrysCapital VII, LLC	The Fund was incorporated on 9 December 2015 and was authorized to operate as a Closed End Fund on 14 December 2015 The Fund's objective is to focus on equity and equity-related growth/expansion capital or buyout investments in companies with existing or expected operations or ties to the Indian subcontinent. The Fund intends to capitalize on the long-term growth prospects and the competitive advantages of India with the objective of delivering superior returns to the investors.
ChrysCapital VIII, LLC	The Fund was incorporated on 1 October 2018 and is authorized to operate as a Closed End Fund on 2 October 2018 The Company's objective is to focus on equity and equity related growth/expansion capital or buyout investments in companies with existing or expected operations or ties to the Indian subcontinent. The Company capitalizes on the long-term growth prospects and the competitive advantages of India to deliver superior returns to investors. The Company holds investments in both listed and unlisted companies in India through its subsidiaries.
ChrysCapital IX, LLC	The Fund was incorporated on 15 November 2021 and is authorized to operate as a Closed End Fund on the same date. The Fund's objective is to achieve substantial long-term capital appreciation and gain competitive advantages, primarily through investments in companies operating in various sectors in the Indian subcontinent. The Fund intends primarily to target companies in sectors that are fast growing and that are positioned to benefit from the secular growth and cost advantages of the Indian subcontinent. The Fund may also evaluate buyouts and platform investments in certain situations. The Fund intends to build a portfolio of investments in five target sectors namely business services, financial services, healthcare, manufacturing and consumer goods and services.
ChrysCapital X, LLC	The Fund was incorporated on 17 June 2024 and is authorized to operate as a Closed End Fund on the same date. The Fund's objective is to achieve substantial long-term capital appreciation and gain competitive advantages, primarily through investments in companies operating in various sectors in the Indian subcontinent. The Fund intends primarily to target companies in sectors that are fast growing and that are positioned to benefit from the secular growth and cost advantages of the Indian subcontinent. The Fund may also evaluate buyouts and platform investments in certain situations. The Fund intends to build a portfolio of investments in five target sectors namely business services, financial services, healthcare, manufacturing and consumer goods and services.
Mauve Investments Limited	The Fund was incorporated on 17 June 2024 and received its authorization to operate as a Collective Investment Scheme and an Expert Fund on 18 June 2024. The Fund's primary objective is to invest in shares of companies publicly listed on the Indian stock exchanges which are regulated by SEBI, with a view to delivering superior return to investors.
Emerald Investments Limited	The Fund was incorporated on 17 December 2018 and received its authorization to operate as a Collective Investment Scheme and an Expert Fund on 24 December 2018. The Fund's primary objective is to make equity and equity related investments to realize superior returns through long-term capital appreciation in a diversified portfolio of companies.

Geranium Investments Limited	The Fund was incorporated on 15 November 2021 and received its authorization to operate as a Collective Investment Scheme and an Expert Fund on the same date. The Fund's would invest in businesses that aim to leverage the attractive dynamics of India. It would focus on listed equity and equity-related growth/expansion capital in listed companies with significant operations in, or potentially significant ties to, the Indian subcontinent.
ClearEdge LLC	The Company was incorporated in Mauritius on 28 July 2020 to fully invest in Celeste Investments Limited (the "FPI Entity") which has been incorporated in Mauritius. The FPI Entity will subsequently invest in listed securities in India.
ClearEdge Asset Management Company LLC	The Company was incorporated on 28 July 2020 and acts as CIS Manager to ClearEdge LLC, Celeste Investments Limited and CE Holdings LLC primarily but also to other entities, in Mauritius and outside Mauritius, as may be requested from time to time. The CIS Maanger's objective is also to invest in participating shares Series E of Clearedge LLc and pay advisory fees to sub-advisor ChrysCapital Associates LLP in India.

Adoption/Re-assessment:

The Group had previously adopted a combined AML/CFT Framework on 10 November 2020 except for Corpus Management Company IX, LLC and ChrysCapital IX, LLC which as adopted on 23 November 2021 and Geranium Investments Limited which as adopted on 2 December 2021 and last reassessed on 12 January 2023. A revised framework was then adopted by the whole Group on 3 March 2023.

ChrysCapital VII, LLC and Corpus Management Company VII, LLC had adopted their AML/CFT Framework on 20 October 2021 which was last reassessed on 10 November 2022. A separate AML/CFT Framework for each FI entity within the Group was subsequently adopted in December 2024 and last amendment to the AML/CFT Frameworks were approved by the respective Boards on 10 November 2025 except for ChrysCapital Management Company V, LLC which was approved on 21 November 2025. Auburn Limited and ChrysCapital Management Company IV, LLC did not have their respective framework reassessed given that both were under winding up and have already surrendered their licence to the FSC.

As mentioned earlier, the AML/CFT framework will be assessed on an annual basis and as and when required when there are any changes in local regulations.

In addition to this, below are the specific actions already taken by the Board:

1. Appointment of MLRO/DMLRO*

The respective Boards have appointed a MLRO and a Deputy MLRO who are AFSML officers as well. Their appointments have also been communicated to the FSC and prior approval has been duly sought from the FSC, where required. The MLRO and DMLRO for each entity in the Group are as follows:

Name of BP	MLRO	Details
ChrysCapital Management Company V, LLC	Ms Shivanee Vythilingum Ram	Mr Dooshant Rai Ramroop
Corpus Management Company VI, LLC	Ms Viraksha Bholoo	Ms Nadia Oodally
Corpus Management Company VII, LLC	Ms Neeruj Ballgobin	Mr Dooshant Rai Ramroop
Corpus Management Company VIII, LLC	Ms Nadia Oodally	Mr Hashish Jeebun
Corpus Management Company IX, LLC	Mr Neeruj Ballgobin	Mr Abhishek Sagar Sumputh
Corpus Management Company X, LLC	Mr Neeruj Ballgobin	Ms Shivanee Vythilingum Ram
ChrysCapital VII, LLC	Mr Abhishek Sagar Sumputh	Ms Ashna Devi Bhunjun-Nursingdass
ChrysCapital VIII, LLC	Mr Abhishek Sagar Sumputh	Ms Nadia Oodally
ChrysCapital IX, LLC	Ms Shivanee Vythilingum Ram	Mr Abhishek Sagar Sumputh
ChrysCapital X, LLC	Ms Viraksha Bholoo	Ms Shivanee Vythilingum Ram
Mauve Investments Limited	Ms Shivanee Vythilingum Ram	Mr Abhishek Sagar Sumputh
Emerald Investments Limited	Ms Viraksha Bholoo	Ms Nadia Oodally
Geranium Investments Limited	Ms Shivanee Vythilingum Ram	Mr Abhishek Sagar Sumputh
ClearEdge LLC	Mr Abhishek Sagar Sumputh	Mr Neeruj Ballgobin
ClearEdge Asset Management Company LLC	Mr Abhishek Sagar Sumputh	Mr Neeruj Ballgobin

*In the event that there is any change in the above-mentioned officers, the approval of the FSC will have to be sought, as required by Mauritius laws, and will be followed by a notification to the Group. For avoidance of doubt, any change in these officers shall not require revising this AML/CFT Framework or Manual.

The MLRO shall provide to the Board a report annually or at any as such agreed frequency.

The report shall include details on Internal and External Suspicious Transaction Reporting (Only numbers are mentioned).

2. Appointment of CO

The respective Boards of the Group have appointed the above MLRO as CO also. Their respective appointments have also been communicated to FSC and prior approval has been duly sought from the FSC, where required. As part of the oversight monitoring function, the CO will need to be informed of any testing being conducted by the Group and report to the Board. This has been explained in Chapter 3 – Part 5.

The CO shall provide periodic reports to the Board. The CO report shall include the following matters:

a) Compliance status in respect of the requirements to the applicable AML/CFT laws and regulations.

b) Report any default or non-compliance on AML/CFT matters.

c) Oversight of the monitoring process of transactions and activity.

d) Adoption and any update of the AML/CFT framework/AML/CFT Policy Handbooke).

e) Independent audit status.

f) Findings of assurance testing carried out on any third-party reliance for CDD (e.g., Introducer certificates, Omnibus, etc.)

g) Training status for directors, officers, and employees of the Company in line with regulatory requirements.

h) Risk assessment status of the Group through BRA and CRA.

i) Testing/Verification carried out by the CO in line with the Compliance Oversight Framework adopted by the Group.

3. CDD

Each of the entity in the Group meets the definition of a FI and is responsible for conducting CDD on its clients/customers. For that purpose, the Group has delegated the conduct of CDD on its investors and other stakeholders to AFSML (Refer to Chapter 3 for more details)

However, the responsibility to verify source of funds/source of wealth and conduct ongoing monitoring remains on the Group. The Boards have therefore confirmed that all information on same is available on records.

Where the Group has delegated CDD to a third party (including AFSML), the Group shall have an oversight of delegated service. For that purpose, a periodic report of CDD status from delegate shall be tabled to the Board and CO.

a) Controlling ownership interest

The Board of the Group agrees that the percentage threshold of controlling ownership interest to be used on its customers (legal persons) for the identification of its beneficial owners be fixed at 20%.

b) Source of Funds

For all investors of the Group, there shall be a confirmation of source of funds in place and if not available, corroborative evidence shall be collected and documented to the satisfaction of the Board.

c) Investments

The Investment Funds or such other service providers appointed will ensure that legal, financial and compliance due diligence have been carried on the investee companies prior to approval of the investments by the Board or disbursement of funds to the investee companies.

Corpus Management Company VI, LLC, Corpus Management Company VII, LLC, Corpus

Management Company VIII, LLC, Corpus Management Company IX, LLC and Corpus Management Company X, LLC (the “Investment Managers”) hold Class B Ordinary shares in ChrysCapital VI, LLC, ChrysCapital VII, LLC, ChrysCapital VIII, LLC, ChrysCapital IX, LLC and ChrysCapital X, LLC respectively.

The Investment Managers make investment recommendations to the respective funds which they manage. The Board of the Investment Managers or such other service providers appointed will ensure that legal, financial and compliance due diligence have been carried

on the investee companies prior to approval and/or recommendation of the advices by the Board. These should be made available to the Group upon request by Board/Administrator/Regulator.

d) Divestments

The Investment Funds or such other service providers appointed shall ensure that due diligence has been carried on the buyers/vendors and the source of funds to pay the Group.

Prior to making any recommendation to the respective funds under management to divest from their investments, the Investment Managers shall ensure that due diligence has been carried on the purchasers and the source of funds prior to approval and/or recommendation by the Board of disposal of investments. These should be made available to the Group upon request by Board/Administrator/Regulator.

4. Enhanced Due Diligence

Enhanced due diligence shall be carried out on high-risk PEPs, connected persons to high-risk PEPs, occasional transaction and all high-risk relationships and prior approval of the Board is required before accepting such applicants for business.

a) Source of Wealth

In addition to source of funds, source of wealth will be requested in cases where enhanced due diligence is required for the high-risk relationships along with corroborative evidence.

5. Simplified CDD

Simplified CDD shall be carried out in cases where lower ML/TF risks have been identified in line with the applicable laws and regulations. In cases where simplified CDD carried out, the Group shall document that decision explaining the reasons of adopting simplified CDD and periodically review same, as required.

6. Third Party Reliance

As of the date the Framework is adopted, ChrysCapital VI, LLC and ChrysCapital VII, LLC have admitted 16 and 9 shareholders respectively through an eligible introducer. ChrysCapital VI, LLC and ChrysCapital VII, LLC have to conduct assurance testing on these third-party arrangements as per its regulatory requirements. To comply with same, ChrysCapital VI, LLC and ChrysCapital VII,

LLC have delegated AFSML to conduct assurance testing on the introducer.

The remaining entities of the Group have not admitted any shareholder through an introducer. No entity in the Group has admitted a shareholder through an omnibus account. In case appointed in the future, the Board will arrange to conduct the assurance testing as per the regulatory requirements.

7. Monitoring Transactions and Activity

a) Cash Transaction

The Group does not deal with any cash transaction. Any exception will be considered on a case-to-case basis.

b) Subscription Monies

All subscriptions monies should be received in the Group's designated bank account via banktransfer. No cash deposit is acceptable unless approved by the Board.

c) Distributions

All distributions have to be credited in the bank account of the shareholder/customer only and not to a third party unless approved by the Board.

In addition to above, the Group has delegated its transaction monitoring requirement to AFSML (Refer to Chapter 3 for more details).

Sanctions Screening

The Group has taken note of the regulatory requirement to screen its clients/customers against sanctions lists. To comply with same, the Group has delegated AFSML to conduct sanction screening (Refer to Chapter 3 for more details)

Any positive match will be reported as per local regulatory procedures.

Any positive match will be reported as per local regulatory procedures and in line with the Practice Note regarding Implementation of Targeted Sanctions which was adopted by the Group as per below:

Name of Company	Date COF approved by Board*
ChrysCapital Management Company IV, LLC	15 December 2022
ChrysCapital Management Company V, LLC	15 December 2022
Corpus Management Company VI, LLC	15 February 2023
Corpus Management Company VII, LLC	15 December 2022
Corpus Management Company VIII, LLC	14 November 2022
Corpus Management Company IX, LLC	10 November 2022
Corpus Management Company X, LLC	5 March 2025
ChrysCapital VI, LLC	15 February 2023
ChrysCapital VII, LLC	15 December 2022
ChrysCapital VIII, LLC	14 November 2022
ChrysCapital IX, LLC	10 November 2022
ChrysCapital X, LLC	5 March 2025
Mauve Investments Limited	11 March 2025
Auburn Limited	23 December 2022
Emerald Investments Limited	14 November 2022
Geranium Investments Limited	12 January 2023

Celeste Investments Limited	N/A – Winding up
ClearEdge LLC	21 November 2025
ClearEdge Asset Management Company LLC	2 October 2025

* These timelines are tentative in nature and may vary. Any changes in the above-mentioned timelines will be notified separately. The Policy will not be revised for changes related to timelines.

b) Transaction

The Group does not deal with any cash transaction. Any exception will be considered on a case-to-case basis.

c) Subscription Monies

All subscriptions monies should be received in the Group's designated bank account via bank transfer. No cash deposit is acceptable unless approved by the Board.

d) Distributions

All distributions have to be credited in the bank account of the shareholder/customer only and not to a third party unless approved by the Board.

In addition to above, the Group has delegated its transaction monitoring requirement to AFSML (Refer to Chapter 3 for more details).

Sanctions Screening

The Group has taken note of the regulatory requirement to screen its clients/customers against sanctions lists. To comply with same, the Group has delegated AFSML to conduct sanction screening (Refer to Chapter 3 for more details).

Any positive match will be reported as per local regulatory procedures.

Any positive match will be reported as per local regulatory procedures and in line with the Practice Note regarding Implementation of Targeted Sanctions which was adopted by the Group as per below:

Name of Company	Date sanctions screening PN adopted by Board*
ChrysCapital Management Company IV, LLC	15 December 2022
ChrysCapital Management Company V, LLC	15 December 2022
Corpus Management Company VI, LLC	15 February 2023
Corpus Management Company VII, LLC	15 December 2022
Corpus Management Company VIII, LLC	14 November 2022
Corpus Management Company IX, LLC	10 November 2022
Corpus Management Company X, LLC	5 March 2025
ChrysCapital VI, LLC	15 February 2023

ChrysCapital VII, LLC	15 December 2022
ChrysCapital VIII, LLC	14 November 2022
ChrysCapital IX, LLC	10 November 2022
ChrysCapital X, LLC	5 March 2025
Mauve Investments Limited	11 March 2025
Auburn Limited	23 December 2022
Emerald Investments Limited	14 November 2022
Geranium Investments Limited	12 January 2023
Celeste Investments Limited	N/A – Winding up
ClearEdge LLC	21 November 2025
ClearEdge Asset Management Company LLC	2 October 2025

* These timelines are tentative in nature and may vary. Any changes in the above-mentioned timelines will be notified separately. The Policy will not be revised for changes related to timelines.

d) Customer Screening

The Group has taken note of the regulatory requirement to conduct customer screening as well as consider any adverse media report. To comply with same, the Group has delegated AFSML to conduct customer screening (Refer to Chapter 3 for more details)

Any material adverse media report will be handled as per local regulatory procedures.

8. Reporting Suspicious Transactions

The respective MLRO of the Group shall be duly notified of any suspicious transaction identified. An internal disclosure form as per Annexure 1 needs to be filed to the MLRO. Should the MLRO find any reasonable grounds for the suspicion, she shall file the suspicious transaction report to the FIU within 5 working days. The Group shall ensure that all records on suspicious transactions are properly kept and maintained.

The Group has, through their respective MLRO, applied for electronic registration of the Group with the FIU. The respective DMLRO has also applied for registration on go AML.

Filing of a STR should be considered as a trigger event for a FI and the latter should conduct a re-assessment of the ML and TF risks of the customer once the STR has been filed.

9. Record Keeping

The Group shall and ensure other services providers keep the books and records as specified in the FSC Handbook 2020 for all its stakeholders and relevant transactions for a period of not less than 7 years after the business relationship has ended or after the transaction has completed. This also includes the training records of all the directors, officers, and employees.

10. Training

The Group shall ensure that its directors, officers, and employees receive the appropriate level of training on AML/CFT topics in line with Section 12.7 of the FSC Handbook 2020. The training can be in-house, sourced from third parties, structured or unstructured training, except for directors who need to follow structured AML/CFT training and the MLRO/CO who need to meet the Competency Standards issued by FSC in October 2014 and updated as of 31 December 2025.

a) Training Register

The Group shall have a training register in place which shall be tabled on an annual basis for the Board oversight, at the time the Compliance report from Administrator is tabled. The training registers for the Group had been tabled at the following Board meetings:

Name of Company	Date training register tabled to Board*
ChrysCapital Management Company V, LLC	21 November 2025
Corpus Management Company VI, LLC	10 November 2025
Corpus Management Company VII, LLC	15 December 2022
Corpus Management Company VIII, LLC	10 November 2025
Corpus Management Company IX, LLC	10 November 2022
Corpus Management Company X, LLC	10 November 2025
ChrysCapital VI, LLC	To remove as no aml obligation as already surrendered its licence.
ChrysCapital VII, LLC	10 November 2025
ChrysCapital VIII, LLC	10 November 2025
ChrysCapital IX, LLC	10 November 2025
ChrysCapital X, LLC	10 November 2025
Mauve Investments Limited	10 November 2025
Emerald Investments Limited	7 November 2025
Geranium Investments Limited	14 November 2025
Celeste Investments Limited	N/A – Winding up
ClearEdge LLC	27 June 2025
ClearEdge Asset Management Company LLC	27 June 2025

* These timelines are tentative in nature and may vary. Any changes in the above-mentioned timelines will be notified separately. The Policy will not be revised for changes related to timelines.

The Group shall ensure that the training register is up to date with all training records of its directors, officers, and employees.

b) Frequency of training

The Group shall provide/arrange for basic AML/CFT training to all directors, officers and employees including those with AML/CFT responsibilities at least every year or on a periodic basis. It may also be arranged when a legislative or regulatory change has been implemented or the FI risk assessment has been updated to ensure that directors, officers, and employees of the FI do not forget their responsibilities and are kept abreast with legislative and regulatory changes.

c) Measuring effectiveness

Given the size, nature and complexity of the Group business and adopting a risk-based approach, the Group resolves that to measure the effectiveness of the AML/CFT training as required under the FSC Handbook 2020, it would consider the assessment of the service provider appointed for the independent AML/CFT audit. The reports, findings and recommendations of the auditor would be considered on annual basis, so that further training needs may be identified, and adequate risk mitigation strategies and appropriate action can be taken.

The Board has confirmed that training on AML/CFT topics are being duly carried out and all training records have been properly kept and maintained. All training records have also been updated in the training register.

11. Risk Assessment

a) Business Risk Assessment ("BRA")

The Group shall adopt a process to identify and assess its exposure to ML and TF risks and conduct its re-assessment annually (or upon any trigger event) in accordance with the applicable laws and regulations. To comply with same, the Group has delegated AFSML to conduct its BRA and its re-assessment (Refer to Chapter 3 for more details)

b) Customer Risk Assessment ("CRA")

The Group shall adopt a process to estimate the risk of ML/TF of its customers and conduct its re-assessment in accordance with the applicable laws and regulations. To comply with same, the Group has delegated AFSML to conduct CRA on its customers and its re-assessment (Refer to Chapter 3 for more details).

After identification and assessment of the above risks, the Group needs to ensure that they are managed and mitigated through the establishment of appropriate and effective policies, procedures, and controls, with appropriate documentation to provide an audit trail. After initial CRA of customers, the Group will consider conducting re-assessment according to risk profile: (i) at least annually for high risk, (ii) at least every 3 years for standard risk and (iii) at least every 4 years for low risk.

12. Independent Audit

The Group has put in place an audit function to review and verify compliance with and effectiveness

of the AML/CFT measures taken in accordance with relevant laws and regulations. To meet the requirements of the independent audit function, the Group has contracted PricewaterhouseCoopers to conduct its AML/CFT independent audit to review and verify compliance with and effectiveness of the AML/CFT measures taken in accordance with relevant laws and regulations.

In line with the Group size, nature, context, complexity and following the BRA conducted, the Board of the respective entity has resolved to conduct its independent audit annually as per below:

Name of Company	BRA risk rating	Independent audit frequency*
ChrysCapital Management Company V, LLC	Low	Annually
Corpus Management Company VI, LLC	Low	Annually
Corpus Management Company VII, LLC	Low	Annually
Corpus Management Company VIII, LLC	Medium	Annually
Corpus Management Company IX, LLC	Medium	Annually
Corpus Management Company X, LLC	Medium	Annually
ChrysCapital VII, LLC	Medium	Annually
ChrysCapital VIII, LLC	Medium	Annually
ChrysCapital IX, LLC	Medium	Annually
ChrysCapital X, LLC	Medium	Annually
Mauve Investments Limited	Medium	Annually
Emerald Investments Limited	Low	Annually
Geranium Investments Limited	Low	Annually
ClearEdge LLC	Low	Annually
ClearEdge Asset Management Company LLC	Low	Annually

*In the event that there is any change in the above-mentioned independent audit frequencies, a notification will suffice as an alternative to revising this AML/CFT Framework/Manual.

13. Employee Screening

The Group currently has 4 employees. The Group has to conduct screening and carry out periodic ongoing screening of its employees against the UN Sanction Lists. To comply with same, the Group has delegated AFSML to conduct its employee screening as well as part of the CDD delegation (Refer to Chapter 3 for more details).

CHAPTER 3: PROCESSES DELEGATED TO APEX FINANCIAL SERVICES (MAURITIUS) LTD

I. CDD:

AFSML follows the local regulatory requirements with respect to CDD identification and verification as well as its ongoing monitoring, as per the FSC Handbook 2020. AFSML has a detailed consolidated CDD checklist in place which clearly provides what are the data verification and documents required for both natural and legal persons. This checklist is used by the On-Boarding & Structuring Unit ("OBS") at client on-boarding stage and by the Client Service Team on an ongoing basis. The Checklist also contains guidelines on Enhanced Due Diligence, Reduced Due Diligence, Eligible Introducers, Declaration on Source of Funds and Source of Wealth, etc.

Furthermore, each client entity administered by AFSML also has a CDD status checklist in place which reflect its CDD status such as passport expiry, screening and CDD documents in place. This CDD status checklist is kept updated by their file owners as and when required and used for ongoing monitoring. The CDD status checklist also captures whether standard, enhanced, or simplified CDD has been applied. The reason for carrying the applied CDD measures such as enhanced CDD or simplified CDD are also documented in the CDD status checklist.

As part of ongoing monitoring, CDD review are also being conducted by AFSML as part its compliance file review process.

II. Business Risk Assessment:

AFSML has designed a risk assessment tool which has been aligned with BRA requirements as per FSC Handbook 2020. This reporting tool is used to conduct BRA of client FIs of AFSML. The reporting tool consists of all the 6 key criteria required for BRA which will be risk-rated, together with consideration of any findings of the latest National Risk Assessment ("NRA") survey report. Re-assessment of the business risk will be done on an annual basis or upon any trigger event.

III. Customer Risk Assessment:

AFSML has designed a risk assessment tool for conducting CRA of customers of its client FIs, as per requirements of the FSC Handbook 2020. Customer Risk Re-assessment will be done in line with AFSML's Periodic Review Procedure which will be as follows: Customer Re-assessment of (i) High AML risk file to be done on an annual basis; (ii) Medium AML-risk files every 3 years and (iii) Low AML risk files every 4 years or at any other such frequency agreed by the Group.

IV. EDD:

AFSML have adequate measures in place to carry out EDD whenever there is a requirement to do so as listed out in the CDD checklist mentioned in (1) above. Evidence of any risk mitigation control and/or measures are documented and kept on file.

As mentioned earlier, in addition to source of funds, source of wealth is also requested along with corroborative evidence as part of EDD.

AFSML previously used KYC6 screening tool to carry out further checks on flagged stakeholders as part of EDD. This screening tool has been phased out with effect from 31 March 2021. Following the phasing out of KYC6, the Group Financial Crime Risk (Group FCR) has recommended to AFSML that EDD be carried out by doing basic screening including Google – Open-Source Screening and use of dedicated websites, which FI under its administration are also following. Effective November 2021, Media Check (through World Check license) is also being done.

V. Simplified CDD:

AFSML was previously applying Simplified CDD where the client was eligible for same based on FSC Code 2012 as per section 5.5.

Now in line with FIAML Regulations 2018, AFSML, is applying simplified CDD measures where lower risks have been identified that may also include the 4 instances from section 5.5 of previous FSC Code 2012 (used as per best industry practice) given no further guidance received on same.

VI. PEP:

PEPs who are considered as high-risk relationships are escalated to Business Risk Committee ("BRC") for onboarding/continuation approval where risk exposure is high. Other lower risk PEPs will be referred to Compliance/Client Services. A central PEP register which categorizes the PEPs into Domestic, Foreign and International Organizations is being maintained at AFSML. Any economic interest of PEPs is also captured in the PEP register to distinguish between PEP connection in public or private capacity. CS can also extract a specific PEP register for the client FI from the central PEP register.

VII. Third-Party Reliance:

AFSML maintains a centralized database of all introducers which is regularly updated by Client Services, i.e., within 7 days when a new introducer certificate received on a new shareholder onboarded.

As per guidance from FSC Handbook 2020 a risk profiling of each introducer is carried out to categorize them as Low Risk, Standard Risk, Potential Risk or High Risk. Depending on its risk assessment, the frequency and sample of testing will be finalized.

As part of AFSML testing methodology of introducer, the following documents are requested from the

latter within a set timeline:

1. Updated beneficial ownership details.
2. Copy of CDD documents and information on underlying shareholder and beneficial owners.

In case CDD information and documents were already requested and successfully obtained during a previous testing exercise, when doing testing again, the Introducer will only be requested to confirm whether there is any change in earlier submissions and if yes, to provide details of same.

This exercise is closely monitored, and any default findings are escalated to the Board of the FI and the CO of the FI.

a) CDD delegation to Third Party Service Providers

AFSML has put in place a process to conduct assurance testing on third party service provider ("TPSP") who have been entrusted by a licensee to conduct its CDD. As part of the testing, a checklist will be circulated to the TPSP where the latter will need to confirm compliance with regulatory requirements such as having a contractual agreement in place, its regulated status, performance of CDD measures in line with applicable laws and regulations, provide CDD docs on request and other requirements as listed in FSC Handbook 2020. Once the checklist is completed, AFSML will verify any gaps and same will be reported to the Board of the client FI.

VIII. Monitoring Transactions and Activity:

AFSML has a transaction monitoring tool called Bank Transfer Validation Form ("BATVAF") in place which is updated by the staff who handles the file of the client and reviewed by a senior, whenever a client entity performs a transaction, for example a payment to a service provider. The BATVAF is a questionnaire where responses are verified to ensure that the transaction is as per the Business plan which has been submitted to the FSC and accompanied by relevant supporting documents.

The BATVAF provides verification of the beneficiaries' countries for any sanction and was recently updated to capture verification being done against UN Sanctioned entities and individuals (requirement of the Sanctions Act 2019) with effect from 26 May 2021 (except those payees who were already on Console and were being screened through Finscan till December 2021).

For the Sanction Country verification, AFSML maintains a Sanction Country List which is updated on a monthly basis and accessible to all the staff. As for the UN Sanction List, same shall be refreshed and linked to BATVAF by Compliance Team as and when there are changes to the list upon notifications from the Financial Intelligence Unit.

The BATVAF also captures confirmation regarding verification of inward remittances. A practice note has also been put in place by First Line of Defense which emphasizes the existing controls at AFSML.

AFSML also ensures that there are at least one or two representatives from AFSML as the bank signatories to have an oversight of the transactions.

1. Customer Screening

AFSML uses World-Check One (an independent service provider forming part of Refinitiv) to assist in conducting screening on its Applicants for Business. AFSML has a dedicated team of World Check review team members that perform the screening as requested by client services. In case the report has been flagged, same is sent to the Compliance Unit for guidance.

Ongoing screening is being done on a daily basis on the platform of World Check One itself. AFSML has also a dedicated team, the Financial Crime Risk Alert Team, who closely monitor and attend to all flagged alerts from World Check One ongoing screening tool.

Any flagged report with a positive match is referred to the client engagement team handling the client file for appropriate action, including escalation to senior management and the Board of the FI, as required.

Sanction Screening

AFSML already has robust and reliable screening tools such as Worldcheck which screen all stakeholders against sanctions. For alerts from World Check One Ongoing screening tool, there is also an agreed internal turnaround time of 3 working days in place to action upon any possible sanction alert identified.

Currently all shareholders, beneficial owners, directors, and signatories of a client entity are on Console/Paxus and are subject to ongoing sanction screening via World Check One ongoing screening tool. For other related parties where inward or outward payment needs to be affected but they are not on Console, AFSML rely on the bank verification procedures for sanction screening.

Should there be a positive match identified on sanctions, AFSML will initiate the notifications to local authorities as required by AML guidelines and also apply any freezing order, as may be applicable. Reference should also be made to the Practice Note regarding Implementation of Targeted Sanctions which was adopted by the Group on the above-mentioned dates.

In cases, where a freezing order has been issued it is recommended that, that legal advice from local counsel be also sought. Similarly, any lapse of freezing order should be actioned upon in line with Section 34 of the Sanctions Act 2019.

IX. Record Keeping:

AFSML has adopted a Group Policy on Record Management which provide guidance on the management of records within the Apex Group by detailing the minimum standards on appropriate record keeping principles, which will ensure AFSML meets its obligations with respect to (i) The prevention of money laundering and sanctions and terrorist financing and compliance with other regulatory and legal requirements applicable to AFSML's business operation and (ii) the maintenance of Confidentiality, Security and Integrity of information within the organization.

AFSML has approved the retention period of 7 years for both digital and physical records in line with local AML/CFT requirements.

X. Employee Screening:

After initial screening on Worldcheck, ongoing screening is effected on a half-yearly basis against UN Sanction lists.

XI. Training:

1. AFSML OFFICERS:

a) AFSML is required to ensure that all relevant AFSML staff which includes MLRO/CO who are AFSML officers as well as AFSML directors on the Board of the FI, receive ongoing training with respect to AML/CFT topics as per its regulatory requirements. At least once annually, a classroom type training is held for all relevant staff on AML/CFT updates and then specialized training sessions are scheduled for focus groups.

b) In addition to above, an annual online training prepared internally by AFSML is also provided. Training to designated client MLROs and AFSML staff acting as officers for client FIs are also arranged.

c) All these training records are centrally kept and maintained at AFSML level for CPD purposes.

2. NON-AFSML OFFICERS/EMPLOYEES OF THE FI:

a) It is the responsibility of the FI to ensure that all its directors, employees and officers receive the appropriate level of AML/CFT training in line with applicable local laws and regulations and are suitably trained to fulfil their personal and corporate responsibilities. As per the FSC Handbook 2020, there is no single or definitive way to conduct training. It could be in-house, sourced from third parties, structured or unstructured training depending on the designation of the officer in relation to the Group. During outreach sessions on onsite inspections, the FSC has clarified that they expect evidence of structured training followed by directors of the FI, as part of training records.

b) AFSML being the management Company of the client FIs, has provided guidance to the directors, officers, or employees (non-AFSML officers mainly) on examples on what structured/unstructured training they could follow to be compliant with applicable laws and regulations for training. Structured training may include training courses, workshops, conferences, practical exams, etc. and unstructured training may include reading a technical article, AFSML highlights, videos, etc.

c) AFSML has also provided guidance on suggested evidence that the FI should keep in place as proof that the directors, officers, and employees have performed the structured/ unstructured training. For example, for structured training: attendance certificate or written email confirmation of attendance and for unstructured training: provide links or details of reading material, etc.

d) A separate training register is maintained for all non-AFSML directors, officers, and employees of each client FI under the administration of AFSML listing out all the above-mentioned details.

XII. Disciplinary Action:

All Directors and employees who are AFSML officers must:

1. Adhere to this AML/CFT Framework, supporting local requirements & procedures and AFSML Group Policies which are published on Knowledge Hub;
2. Follow the local STR internal reporting procedures in respect of any incident or suspicion;
3. Complete all Anti-Money Laundering and Combatting Terrorist Financing training as required by AFSML Group and/or local compliance team.

Breaches will be actively monitored by the CO, or any other relevant authority put in place by the Board.

AFSML Group has published the policy, namely, Ethics and Standards of Conduct Policy and a Model Citizen Slides, which set out the responsibilities, behaviors, and standards of conduct which all employees within the AFSML Group should adhere to.

Breach of any of the AFSML Group's or internal policies may lead to disciplinary action like:

1. Revocation of privileges.
2. Bonus Reduction.
3. Additional training requirements.

Other disciplinary actions in line with the provisions of local Employment laws or other such law which caters for specific breaches and as mentioned in each specific AFSML Group Policies.

Sample Internal Disclosure Form to MLRO

1. Reported To

Name of MLRO/DMLRO : _____

Email Address : _____

2. Reporting Employee

Name : _____

Telephone No

Email address of reporting employee

3. Client : _____

Client Name : _____

Address : _____

Contact Name : _____

Contact Telephone No

Date Client Relationship : _____

Commenced : _____

Client reference : _____

4. Information/Suspicion

Suspected Information/

Transaction : _____

Reasons for Suspicion : _____

_____

_____

Please attach copies of any relevant documentation to this report.

Reporter's Signature: _____ Date: _____

It is an offence to advise the customer/client or anyone else of your suspicion and report.

This report will be treated in the strictest confidence.

MLRO Use:

Date received: _____ Time received: _____

Ref: _____

CHRYSCAPITAL

Suite 604, 6th Floor, St James Court,
Port Louis 11328, Mauritius.

+230 5250 9398

www.chryscapital.com