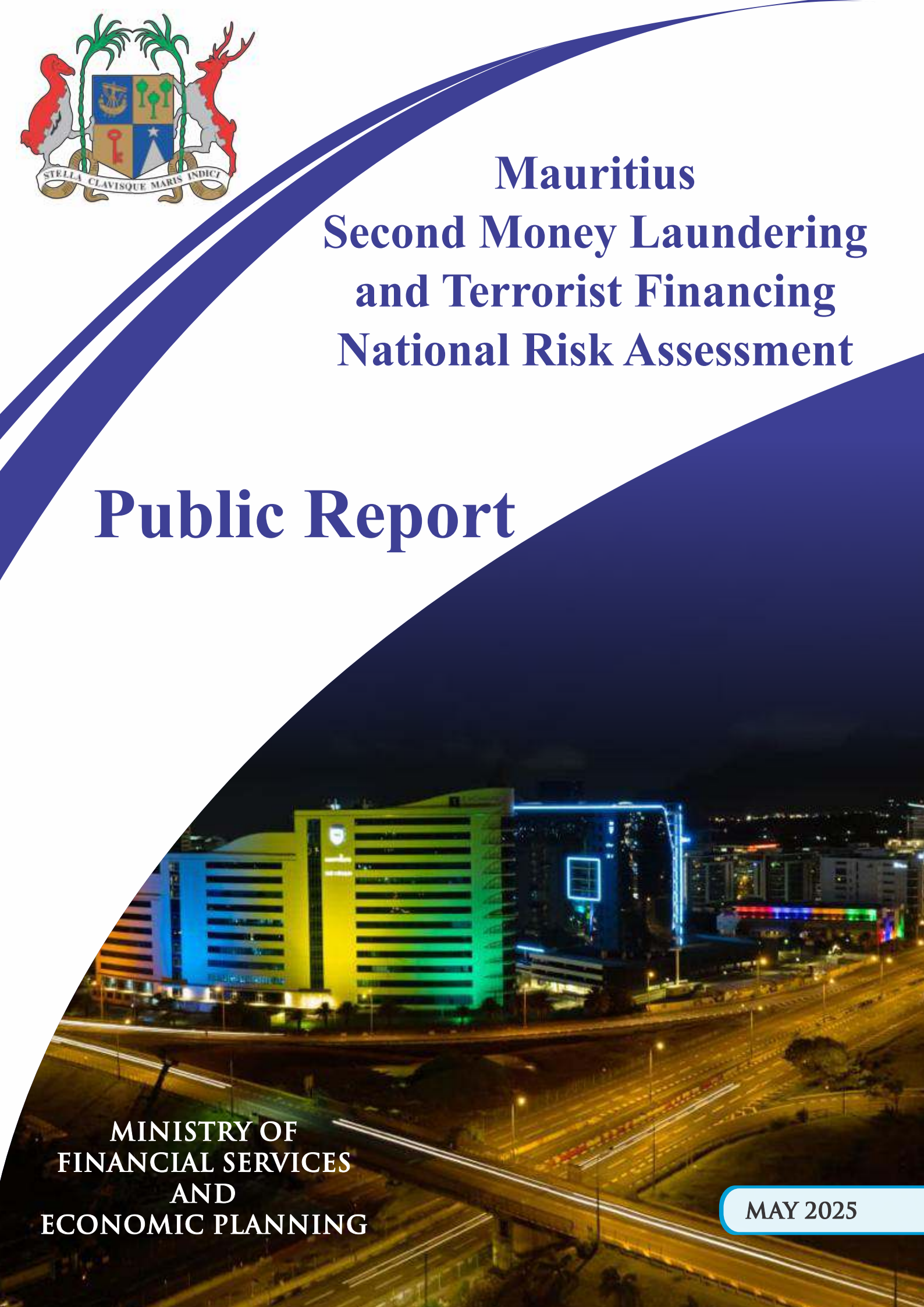
Mauritius
Second Money Laundering and Terrorist Financing National Risk Assessment

Public Report



MINISTRY OF
FINANCIAL SERVICES
AND
ECONOMIC PLANNING

MAY 2025

Mauritius
Second Money Laundering and Terrorist Financing National Risk Assessment

Public Report

Ministry of Financial Services
and
Economic Planning

May 2025

TABLE OF CONTENTS

FOREWORD BY THE MINISTER OF FINANCIAL SERVICES AND ECONOMIC PLANNING

Safeguarding the integrity and stability of our financial system and institutions is not a destination but a continuous journey, where all stakeholders have to regularly identify, understand and mitigate potential risks. The National Risk Assessment (NRA) serves as a crucial tool for analysing threats and vulnerabilities, enabling us to better protect our economy from illicit activities and strengthen the resilience of our financial services sector.

I have the pleasure to present the NRA Report on Mauritius money laundering risks and the terrorist financing risks. It is Mauritius second risk assessment and is a follow up on the last NRA carried out in 2019. This NRA updates our understanding of risks and has been undertaken in consultation with stakeholders in the public and private sectors.

The successful exit of Mauritius from the Financial Action Task Force (FATF)'s *List of Jurisdictions Under Increased Monitoring* (commonly referred to as 'Grey List') coupled with the subsequent recognition as one of the top-tier jurisdictions rated '*Compliant'* or '*Largely Compliant'* to all of the 40 FATF Recommendations constitute landmark accomplishments for the country. Mauritius has maintained its momentum in the fight against money laundering and terrorism financing, continually taking steps proactively to assess and enhance its Anti-Money Laundering and Combatting the Financing of Terrorism and Combatting the Financing of Proliferation framework.

These updated findings and recent developments in the second NRA exercise provide a greater opportunity to respond effectively to the fight against money laundering and terrorist financing. While recognising that risks are constantly evolving, it is the responsibility of one and all to stay alert in the face of emerging threats and vulnerabilities. This will better equip us in the formulation of appropriate policies and strategies to address risks and allocate resources efficiently in combatting financial crimes.

I would like to commend the dedication and commitment demonstrated as well as the relentless efforts put in by all those involved in ensuring the successful completion of this exercise. Through synergistic collaboration, the public and the private sectors can pursue their coordinated efforts to strengthen the reputation of Mauritius as an International Financial Centre of excellence, and enhance the resilience and sustainability of our economy.

Honourable Dr. Mrs. Jyoti Jeetun
Minister of Financial Services and Economic Planning
May 2025

ACRONYMS

AC	Authorised Company
A.C.T	AML/CFT Coordination Task Force
ADSU	Anti Drug and Smuggling Unit
AGO	Attorney General's Office
AML	Anti-Money Laundering
AML/CFT/CPF	Anti-Money Laundering/Countering the Financing of Terrorism/ Countering Proliferation Financing (also used for Combatting the financing of terrorism and Combatting the financing of proliferation of weapons of mass destruction)
AU	African Union
ARID	Asset Recovery Investigation Division
ARINSA	Asset Recovery Inter-Agency Network for Southern Africa
BEPS	Base Erosion and Profit Shifting
BO	Beneficial Owner
BoM	Bank of Mauritius
CDD	Customer Due Diligence
CEF	Closed-End Funds
CFT	Countering the Financing of Terrorism (also used for Combatting the financing of terrorism)
CIS	Collective Investment Scheme
CSFTA	Convention for the Suppression of the Financing of Terrorism Act 2003
COMESA	Common Market for Eastern and Southern Africa
CPF	Countering Proliferation Financing (also used for Combatting the financing of proliferation of weapons of mass destruction)
CSP	Company Service Provider
CCU	Cooperative Credit Union
DNFBPs	Designated Non-Financial Businesses and Professions
DPMS	Dealers in Precious Metals and Stones
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EOIR	Exchange of Information on Request
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FCC	Financial Crimes Commission
FCC Act	Financial Crimes Commission Act 2023
FCD	Financial Crimes Division
FIAMLA	Financial Intelligence and Anti-Money Laundering Act
FIAMLR	Financial Intelligence and Anti-Money Laundering Regulations
FI	Financial Institution
FIU	Financial Intelligence Unit
FSA	Financial Services Act
FSC	Financial Services Commission

GBCs	Global Business Companies
GDP	Gross Domestic Product
GRA	Gambling Regulatory Authority
GRA Act	Gambling Regulatory Authority Act 2007
HNWI	High Net Worth Individual
IAIS	International Association of Insurance Supervisors
ICAC	Independent Commission Against Corruption
ICC	Interagency Coordination Committee
ICRG	International Co-operation Review Group
IFC	International Financial Centre
IFSB	Islamic Financial Services Board
LLTI	Linked Long-Term Insurance
IRSA	Integrity Reporting Services Agency
ISIL	Islamic State of Iraq and the Levant
ISIS	Islamic State of Iraq and Syria
IO	Immediate Outcome
IOSCO	International Organization of Securities Commissions
ITOs	Initial Token Offerings
IITOs	Issuers of Initial Token Offerings
KYC	Know Your Customer
LEAs	Law Enforcement Authorities
MauCAS	Mauritius Central Automated Switch
MER	Mutual Evaluation Report
MIPA	Mauritius Institute of Professional Accountants
ML	Money Laundering
MLA	Mutual Legal Assistance
MLRO	Money Laundering Reporting Officer
MOC	Memorandum of Cooperation
MOU	Memorandum of Understanding
MPF	Mauritius Police Force
MRA	Mauritius Revenue Authority
MVTS	Money or Value Transfer Services
NBDTIs	Non-Bank Deposit Taking Institutions
NPOs	Non-Profit Organisations
NRA	National Risk Assessment
NRAWG	National Risk Assessment Working Group
ODPP	Office of the Director of Public Prosecutions
OECD	Organisation for Economic Co-operation and Development
OFI	Other Financial Institution
P2P	Peer-to-Peer
PEPs	Politically Exposed Persons
PIS	Payment Intermediary Services
PSP	Payment Service Providers
POCA	Prevention of Corruption Act
POTA	Prevention of Terrorism Act 2002

PF	Proliferation Financing
QTs	Qualified Trustees
ROC	Registrar of Companies
SADC	Southern African Development Community
STRs	Suspicious Transaction Reports
TCSPs	Trust and Company Service Providers
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UBOs	Ultimate Beneficial Owners
UN	United Nations
UNSA	United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolutions
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VAITOS Act	Virtual Asset and Initial Token Offering Services Act 2021

1. EXECUTIVE SUMMARY

This is the second Money Laundering and Terrorist Financing National Risk Assessment (NRA) of Mauritius, providing a critical opportunity to evaluate progress since 2019 and identify evolving risks and areas requiring further enhancement in combatting money laundering (ML) and terrorist financing (TF).

The fight against ML and TF is inherently global, and Mauritius remains exposed to international financial and security risks. The increasing use of Virtual Assets (VAs) presents additional complexities, particularly regarding privacy-focused cryptocurrencies, which challenge traditional Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) enforcement mechanisms. Given these global risks, Mauritius remains committed to reinforcing its resilience through continuous assessment and targeted reforms.

In fact, the efforts of Mauritius to safeguard its financial system against ML and TF remain ongoing. Following its 2018 Mutual Evaluation Report (MER) and subsequent placement on the Financial Action Task Force (FATF) Grey List, Mauritius took decisive corrective measures, leading to its delisting in 2021. Mauritius continued to enhance compliance with FATF standards, strengthening its regulatory framework and enforcement mechanisms to maintain its position as a well-regulated financial jurisdiction.

Mauritius adopted a strategic and coordinated approach to legislative and institutional reforms. Key initiatives included:

- Legislative Advancements: Enacting pivotal laws such as the Virtual Asset and Initial Token Offering Services Act 2021 (VAITOS Act) and the Financial Crimes Commission Act 2023 (FCC Act) to address emerging risks and streamline financial crime investigations.
- Institutional Enhancements: Establishing specialized arrangements such as the Inter-Ministerial Committee and Core Group for Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation, and Combatting Foreign Bribery (the Core Group) to ensure an effective implementation of the FATF Standards, enhancing the mandate of the National Committee for AML/CFT (the National Committee) for strategic oversight, and creating the Financial Crimes Division (FCD) at the level of the Supreme Court and Intermediate Court to expedite the processing of financial crime cases.
- Collaborative Frameworks: Strengthening interagency cooperation through the Memorandum of Cooperation (MOC), AML/CFT task forces, and enhanced information-sharing mechanisms.

Further, Mauritius conducted sector-specific risk assessments, including:

- The TF Risk Assessment for Non-Profit Organisations (NPOs) in 2020; and
- The ML/TF Risk Assessment of Virtual Assets (VAs) and Virtual Asset Service Providers (VASPs) in 2021, leading to the enactment of VAITOS Act to regulate VAs and VASPs.

Capacity building and international collaboration have been fundamental to the success of Mauritius. The country actively invested in technical assistance and training for Anti-Money Laundering/Countering the Financing of Terrorism/Countering Proliferation Financing (AML/CFT/CPF), while partnerships with global organizations bolstered investigative, supervisory, and enforcement capabilities. Additionally, Mauritius played a proactive role in providing technical assistance to other jurisdictions, reinforcing its commitment to global AML/CFT/CPF efforts. By continuously refining its approach, Mauritius not only safeguarded its financial system but also set a benchmark for other jurisdictions navigating similar risks.

National Risk Assessment

The primary objectives of this second NRA were to deepen the national understanding of ML and TF risks, evaluate their evolution since 2019[1], and support the development of targeted AML/CFT strategies and measures. This assessment serves as a strategic tool to prioritise identified ML and TF risks through both targeted national and operational actions and effective resource allocation. It, as such, outlines critical recommendations to address weaknesses identified and enhance the effectiveness of prevention and mitigation efforts whilst strengthening processes, systems and strategic frameworks to combat ML and TF risks proactively. In addition, the exercise will, amongst others, assist supervisors in conducting comprehensive risk evaluations, as well as guide reporting persons[2] in identifying and mitigating vulnerabilities. Covering the period from January 2018 to December 2024, the NRA provides a detailed snapshot of ML/TF activity, at national and sectoral levels for the period January 2018 to June 2022, and major developments including an updated assessment of emerging threats, for the period July 2022 to December 2024.

The NRA used the revised National Money Laundering and Terrorist Financing Risk Assessment Tool developed and provided by the World Bank, which included revised modules on National TF threat and vulnerability, along with a new module on TF sectoral risk. In accordance with the World Bank Tool, the following factors were assessed:

(a) the scale and characteristics of the proceeds of criminal activities from both internal and external sources;
(b) the scale and characteristics of TF in Mauritius;
(c) the weaknesses or gaps in the ability of Mauritius to combat ML and TF; and
(d) the ML and TF weaknesses or gaps arising from the financial services sector as well as Designated Non-Financial Businesses and Professions (DNFBPs) in the country.

In line with the World Bank methodology, Mauritius re-established the NRA Working Group (NRAWG) to conduct the risk assessment. The NRAWG comprised all AML/CFT stakeholders in Mauritius, including Law Enforcement Authorities (LEAs), the Financial Intelligence Unit (FIU), other intelligence agencies, Financial Institution (FI) and DNFBP supervisors, the National Sanctions Secretariat, the Registrar of Associations, the National Audit Office, the University of Mauritius and the private sector.[3]

[1] Data collection for the first NRA covered the period January 2014 to December 2017.
[2] Please refer to Table 5 regarding Sectors Assessed for the NRA exercise.
[3] More details on the composition of the NRAWG is found at Annex 1.

Key Findings

The Overall Money Laundering Risk

The overall ML risk for Mauritius was **Medium-High**. This rating was based on both the National ML Threat and National ML Vulnerability, each assessed as **Medium-High**.

ML threats originated from both domestic and international predicate offences, with external threats, primarily linked to fraud, corruption and tax evasion, posing a greater risk due to the open economy of Mauritius. At the domestic front, the NRA findings identified drug trafficking, fraud, and illegal bookmaking as the top three crimes generating illicit proceeds in the country.

The national ML vulnerability of **Medium-High** was informed by a combination of the national ML combatting ability which was rated **Medium,** and the overall sectoral ML vulnerability which was rated **High**.

The Overall Terrorist Financing Risk

The overall TF risk for Mauritius was **Medium-Low**. This rating was derived from a combination of both the National TF Threat and the National TF Vulnerability, which were both rated **Medium-Low**. While no active terrorist organisations or individuals have been identified, there were indications that some individuals were influenced by extremist ideologies and propaganda, and the number has slightly increased in the past years. Authorities remained vigilant, closely monitoring for potential TF risks and taking preventive action under existing legislation. Given the status Mauritius has as an International Financial Centre (IFC), the Government acknowledged its potential vulnerability to TF abuse and continues to implement robust safeguards to mitigate these risks.

A snapshot of the National ML and TF risks is highlighted in Table 1.

Table 1: National ML Risks and National TF Risks

National ML Risks:			**Medium High**
• National Threat:		Medium High	
Internal Threat	Medium		
External Threat	High		
• National ML Vulnerability:		Medium High	
Combatting Ability	Medium		
Sectoral Vulnerability	High		
National TF Risks:			**Medium Low**
National TF Threat:		Medium Low	
National TF Vulnerability:		Medium Low	

ML Sectoral Risks

The risk assessment revealed a **Medium-High** to **Low** level of ML risk across several sectors. A snapshot of the overall sectoral ML threat, vulnerability, and risk ratings is outlined in Table 2.

Table 2: Sectoral ML Threat, Vulnerability and Risk Ratings

Sector	ML Threat Rating	ML Vulnerability Rating	ML Risk Rating
Banking Sector			
Banking	High	Medium	Medium-High
Insurance Sector[4]			
General Insurance			
Miscellaneous, Transportation, Guarantee, Engineering	Low	Medium-Low	Low
Property, Accident and Health	Low	Medium	Medium-Low
Liability	Low	Medium-Low	Medium-Low
Motor	Medium-Low	Medium-Low	Medium
Long-term Insurance			
Long-Term Insurance (except Linked Long term insurance)	Medium-Low	Medium-Low	Medium-Low
Linked Long Term Insurance	Medium-Low	Medium	Medium
Securities Sector			
Securities	Medium	Medium	Medium
Other Financial Institutions (OFIs)			
OFIs- under BoM Supervision			
Cash Dealers	Medium	Medium	Medium
NBDTI	Medium-Low	Medium-Low	Medium-Low
Payment Service Providers	Low	Low	Low
OFIs- under FSC Supervision			
Leasing	High	Medium	Medium-High
Payment Intermediary Services	Medium	Medium	Medium
Credit Finance	Low	Medium-Low	Medium-Low
Investment Banking	Low	Medium	Medium-Low
Treasury Management	Low	Medium	Medium-Low
OFIs- Cooperative Credit Unions (CCUs)			
OFIs- CCUs	Medium-Low	Low	Medium-Low
Trust and Company Service Provider (TCSP) Sector			
TCSPs under FSC Supervision	High	Medium	Medium-High
CSPs under ROC Supervision	Low	Medium	Medium-Low
Designated Non-Financial Businesses and Professions (DNFBPs)			
Legal profession (excluding Notary)	Medium	Medium	Medium
Notary	Medium-High	Medium	Medium-High
Gambling	High	Medium	Medium-High
Real Estate	Medium	High	Medium-High
DPMS	Medium-High	Medium	Medium-High
Accountancy	Medium	Medium-Low	Medium

[4]The rating for the different classes of insurance was impacted by their importance, which was determined based on their market share percentages.

TF Sectoral Risks

The risk assessment revealed a **Medium** to **Low** level of TF risk across all the assessed sectors.

A snapshot of the overall sectoral TF threat, vulnerability, and risk ratings is outlined in Table 3.

Table 3: Sectoral TF Threat, Vulnerability and Risk Ratings

Sector	TF Threat Rating	TF Vulnerability Rating	TF Risk Rating
Banking Sector			
Banking	Medium	Medium-Low	Medium
Insurance Sector			
Insurance	Low	Medium-Low	Medium-Low
Securities Sector			
Securities	Low	Low	Low
Other Financial Institutions (OFIs)			
OFIs- under BoM Supervision			
Cash Dealers	Medium-Low	Medium-Low	Medium-Low
NBDTI	Low	Low	Low
Payment Service Providers	Low	Low	Low
OFIs- under FSC Supervision			
Custodian – Non-CIS	Low	Medium-Low	Medium-Low
Payment Intermediary Services	Medium-Low	Medium-Low	Medium-Low
Credit Finance	Low	Medium-Low	Medium-Low
Investment Banking	Low	Medium-Low	Medium-Low
Treasury Management	Low	Medium-Low	Medium-Low
OFIs- Cooperative Credit Unions (CCUs)			
OFIs- CCUs	Low	Low	Low
Trust and Company Service Provider (TCSP) Sector			
TCSPs under FSC Supervision	Medium-Low	Medium-Low	Medium-Low
CSPs under ROC Supervision	Low	Low	Low
Designated Non-Financial Businesses and Professions (DNFBPs)			
Legal professions (excluding Notary)	Low	Low	Low
Notary	Low	Medium-Low	Medium-Low
Gambling	Low	Medium-Low	Medium-Low
Real Estate	Low	Medium	Medium-Low
DPMS	Low	Medium-Low	Medium-Low
Accountancy	Low	Low	Low

Detailed analysis of ML and TF risks for each sector are highlighted in this report.

Looking Ahead

Mauritius is a leading financial hub in Sub-Saharan Africa, underpinned by strong economic performance, adherence to international standards, and robust regulatory frameworks. While emerging risks such as cybercrime, fraud, and illicit financial flows pose challenges, the country has demonstrated resilience through proactive reforms and global cooperation.

Mauritius remains committed to strengthening its AML/CFT framework by addressing the key risks and vulnerabilities identified in this second NRA. To safeguard the integrity of its financial system, the country will develop a comprehensive National AML/CFT Strategy, leading to a National Action Plan that will be implemented across all competent authorities with adequate resources.

To further enhance its risk mitigation capabilities, Mauritius is undertaking several strategic initiatives, including the establishment of a Centralised Information Management System to improve data collection and risk assessment efficiency, a mid-term independent assessment to evaluate compliance with FATF Standards ahead of the next Mutual Evaluation, and targeted risk assessment exercises focused on legal persons and legal arrangements, Proliferation Financing, VAs and VASPs and NPOs. These proactive measures reinforce dedication of Mauritius to maintaining a robust and internationally compliant AML/CFT/CPF regime and ensuring its continued recognition as a trusted and well-regulated IFC.

2. CURRENT SITUATION

The Economic Landscape

Mauritius is a small island nation in the Indian Ocean of approximately 1.3 million people. It has a relatively diversified economy and is recognised for its economic success in Sub-Saharan Africa, having evolved from a low-income, sugarcane-dependent nation in the 1960s to an upper-middle-income country with a per capita income exceeding USD 11,000.

Mauritius is one of Africa's largest IFCs and the global business sector is one of the key pillars of the economy. The financial sector comprises businesses such as monetary intermediation, financial leasing and other credit granting businesses, insurance, reinsurance and pensions.

With a track record of over three decades, Mauritius has established itself as a well-regulated and transparent IFC and a jurisdiction of substance in cross-border investment and finance. The financial sector plays a pivotal role in the Mauritian economy, contributing to 13.7% of the Gross Value Added in 2023. The financial sector is expected to grow by 4.4% in 2024, higher than 3.9% growth in 2023.[5]

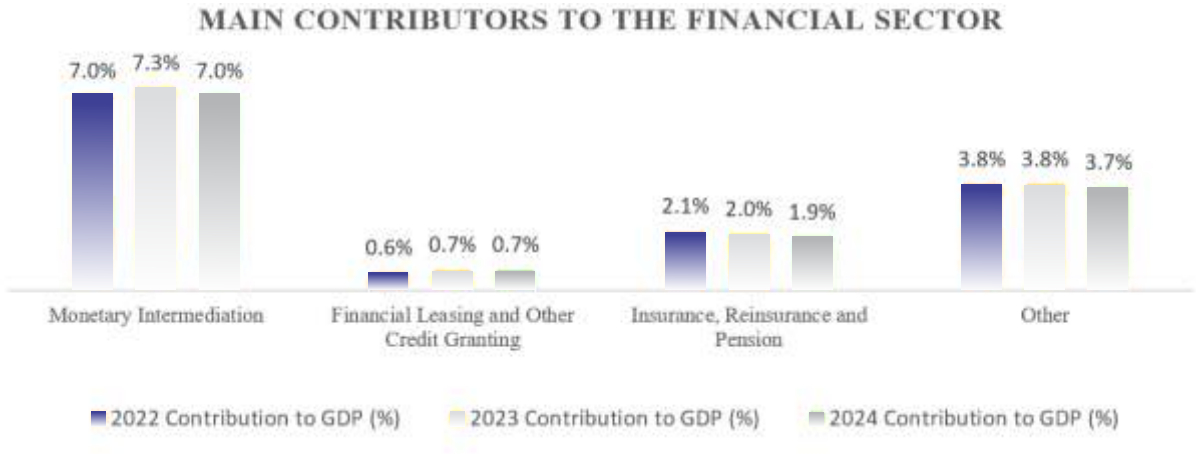


Chart 1 – Main Contributors to the Financial Sector

The Mauritius IFC continues to innovate, offering a wide range of financial products and services including VAs.

[5] Statistics Mauritius Dec 2024 publication.

Mauritius is also a jurisdiction of substance, complying with international norms and standards as testified by the rankings shown in Table 4.

Table 4: Performance of Mauritius in terms of international rankings

Index & Brief Description	Ranking
2024 Ibrahim Index of African Governance [6] (Measures African Governance Performance – based on 2023 figures)	2nd out of 54 countries
2024 Economic Freedom of the World (Fraser Institute) [7] (Measures degree to which policies and institutions are supportive of economic freedom – based on 2022 figures)	17th out of 165 countries
Democracy Index 2023 (Economist Intelligence Unit) Provides a snapshot of the state of democracy worldwide	20th out of 165 countries & 2 territories
2024 International Property Rights Index (Property Rights Alliance) A comprehensive insight into the status of property rights	41st out of 129 countries
2024 Global Peace Index (Institute for Economics and Peace)[8] World's leading measure of global peacefulness	22nd out of 163 countries
Global Free Zones of the year (FDI intelligence)	1st in Africa and 10th Globally (2022)
Global Innovation Index[9] (2024)	1st in Sub Saharan Africa and 55th Globally

The reputation of Mauritius as a well-regulated and attractive investment destination is also evidenced by its membership and participation in international standard setting organisations such as the International Organisation of Securities Commissions (IOSCO), International Association of Insurance Supervisors (IAIS), Organisation for Economic Co-operation and Development (OECD) and Islamic Financial Services Board (IFSB). Additionally, Mauritius is a founder member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) since 1999, which is an associate member of the FATF. Mauritius is also a key member of the African Union (AU), Southern African Development Community (SADC) and Common Market for Eastern and Southern Africa (COMESA).

[6] https://mo.ibrahim.foundation/sites/default/files/2024-10/2024-index-report.pdf
[7] https://www.heritage.org/index/pages/country-pages/mauritius
[8] https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf
[9] https://www.wipo.int/gii-ranking/en/rank

Initiatives to Promote Tax Good Governance Principles

Mauritius has always ensured its adherence to principles of good governance and transparency in the field of international tax. It has joined the Multilateral Convention on Mutual Administrative Assistance in Tax Matters and the Common Reporting Standard on the automatic exchange of financial account information, as well as signed various Double Taxation Avoidance Agreements and Tax Information Exchange Agreements, which altogether provide the right framework for cooperation with other jurisdictions in the combat against tax avoidance and evasion.

Moreover, Mauritius is an active participant in the Base Erosion and Profit Shifting (BEPS) project. Mauritius has, in fact, joined the OECD Inclusive Framework on the Implementation of the BEPS Recommendations and has formally committed to implement the BEPS standards. Under the BEPS project, Mauritius signed and ratified the Multilateral Convention to Implement Tax Treaty Related Measures to prevent BEPS (Multilateral Instrument or MLI) and the Country-by-Country Multilateral Competent Authority Agreement (MCAA) starting to exchange of Country-by-Country reports as from the fiscal year starting 1 July 2018 onwards.

Of note, the country, which has been assessed by the Global Forum on Transparency and Exchange of Information, established by the OECD, is rated as fully compliant with the OECD Standards on Transparency and Exchange of Information for tax purposes. In addition, the OECD Forum on Harmful Tax Practices, which has reviewed our tax regimes is satisfied that the regimes are fully compliant with the international standards and do not comprise any harmful features. This position is also shared by the European Union, which has in parallel also assessed our tax regimes.

Local Perspective: Building from 2019 to now

Since the completion of its MER in 2018 and subsequent listing on the FATF Grey List, Mauritius has made significant progress in addressing the deficiencies in the MER and the FATF Action Plan to improve technical compliance and effectiveness of its AML/CFT regime with the FATF Standards. Mauritius was, in the light of sustainable progress made, delisted from the FATF Grey List in October 2021.

Mauritius has been commended by the FATF for the progress achieved in addressing the strategic deficiencies especially under difficult circumstances caused by the COVID-19 pandemic. All measures taken demonstrated the underlying unflinching commitment of Mauritius to ensure the sustainability and effectiveness of efforts to combat ML/TF/PF in the future.

Setting up a Robust AML/CFT/CPF Coordination Mechanism

Compliance with the FATF Standards required effective coordination and collaboration with all stakeholders including the private sector. A robust AML/CFT/CPF coordination mechanism was put in place, starting with the Inter-Ministerial Committee which considered the recommendations of the Core Group and fostered effective implementation of strategic priorities.

In 2021, the Core Group was enshrined under section 19AA of the Financial Intelligence and Anti-Money Laundering Act (FIAMLA) to, amongst others, ensure the effective implementation of the FATF Standards on AML/CFT by the relevant competent authorities and make recommendations on matters, including implementation, strategy, and international developments, pertaining to AML/CFT.

The mandate of the National Committee, established under section 19A of FIAMLA since 2003, was broadened to coordinate the development, regular review and implementation of national policies and activities to combat ML, TF and PF, including the risks associated thereto.

Following the 2018 Mutual Evaluation, the National Committee set up eleven Immediate Outcome (IO) Sub-Committees to enhance institutional coordination at the technical level to ensure that Mauritius implemented an effective AML/CFT/CPF system to meet FATF Standards. The IO Sub-Committees reported regularly to the National Committee.

The following Committees were also established, namely:

(i) AML/CFT Statistics Committee – to coordinate and harmonise collection of AML/CFT Statistics by all relevant authorities;

(ii) Observatory Committee of Virtual Assets – to identify trends and patterns of VA transactions/activities, track unlicensed VASPs, and detect illegal activities within the VA ecosystem of Mauritius; and

(iii) National Sanctions Committee – established under the United Nations (Financial Prohibitions, Arm Embargo and Travel Ban) Sanctions Act 2019 (UNSA) to promote and coordinate the implementation of United Nations Security Council Resolutions (UNSCR).

Interagency collaboration was strengthened among the AML/CFT Supervisors and Law Enforcement Authorities (LEAs). The signing of a Memorandum of Cooperation (MOC) amongst AML/CFT supervisors in August 2020, and the setting up of the ICC, regrouping all AML/CFT supervisors, has proven to be an effective platform to continuously improve the AML/CFT supervisory effectiveness in different areas, notably, through enhanced collaboration, coordination and supervisory cooperation amongst the ICC Members, facilitating the exchange of information as well as the implementation of a risk-based approach to AML/CFT supervision by pulling resources together and conducting joint training for the benefit of supervisors and outreach sessions for the industry. Similarly, the LEAs have set up an AML/CFT Coordination Task Force to facilitate cooperation amongst LEAs regarding parallel and complex financial investigations.

Through the above-mentioned platforms, the supervisors and LEAs have been able to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat ML, TF, and PF.

The private sector, through various key initiatives and multi-disciplinary forum, also remains a key partner in the fight against ML and TF through close collaboration, coordination, and cooperation in the implementation of AML/CFT measures in order to ensure sustainability and effectiveness of the framework in place. A Public-Private Partnership Task Force has been set up under the FCC Act to (a) develop and promote cooperation between the public and private

sector in combatting financial crimes; (b) strengthen the fight against financial crimes with the collaboration and partnership of the public and private sectors; and (c) enhance collaboration and sharing of information by its members to assist the Financial Crimes Commission (FCC) in financial crimes investigation and prosecution.

Enhancing our AML/CFT/CPF Legal and Institutional Framework

Prior to the publication of its MER in September 2018, Mauritius embarked on the process of reviewing and strengthening its existing AML/CFT/CPF framework comprehensively to ensure full compliance with the FATF Standards.

In this respect, significant changes were brought to the FIAMLA and other existing legislations through the Finance (Miscellaneous Provisions) Act 2018, the AML/CFT/CPF (Miscellaneous Provisions) Act 2019, the UNSA, the AML/CFT/CPF (Miscellaneous Provisions) Act 2020 and the Finance (Miscellaneous Provisions) Act of 2021 and 2022.

In September 2020, the FCD was established at the level of the Supreme Court and Intermediate Court to deal with financial crime offences and ancillary matters. The setting up of the FCD of the Supreme Court and the FCD of the Intermediate Court ensured that financial crime cases were dealt with expeditiously, thereby furthering our compliance with FATF Standards. The FCD of the Supreme Court, in addition, has jurisdiction to hear and determine any other matter under any enactment which is connected or ancillary to a financial crime offence. Additionally, the aim of the FCD is to have specialised magistrates/judges, who are well versed in AML/CFT, to hear and determine cases, including those of a complex nature, thereby ensuring the timely disposal of cases and higher quality decisions on findings and sanctions especially in complex cases.

The UNSA provided the legal framework for the implementation of United Nations (UN) sanctions as adopted by the United Nations Security Council (UNSC) under Chapter VII of the UN Charter. This legislation also implemented the requirements of the FATF regarding Targeted Financial Sanctions (TFS) under the FATF Recommendations 6 and 7.

Mauritius has enacted a comprehensive legislation, the VAITOS Act, to regulate the business activities of and supervise VASPs and Issuers of Initial Token Offerings (IITOs).

A new piece of legislation, namely the FCC Act, was proclaimed in March 2024, providing for the establishment of the FCC which has subsumed the mandate of the Independent Commission Against Corruption (ICAC), Integrity Reporting Services Agency (IRSA) and Asset Recovery Investigation Division (ARID). The FCC has become the apex agency responsible for detecting, investigating, and prosecuting various financial crimes, including corruption, financing of drug dealing. The FCC also has responsibility for asset recovery in Mauritius.

To further reinforce its AML/CFT regime, an AML/CFT/CPF (Miscellaneous Provisions) Act was introduced in July 2024 with a view to addressing the remaining minor technical deficiencies and revisions pertaining to the FATF Recommendations, as well as legislative gaps identified during the MER 2018 and the risk assessment exercises.

These initiatives bear testimony to the commitment of Mauritius to safeguarding its financial system as well as ensuring that it remains a trusted IFC.

Conducting Risk Assessments

In 2019, Mauritius completed its first NRA exercise which enabled the country to identify, assess and understand its ML and TF risks. The findings of the NRA led to the development and adoption of a National AML/CFT Strategy 2019-2022 which aimed at enhancing the ability of Mauritius to prevent, detect and deter ML and TF (both in terms of the legal framework and operational capacity). It also contained a strategy for maintaining an ongoing dialogue with relevant private sector stakeholders to ensure effective implementation of AML/CFT requirements.

Risk Assessment for Legal Persons and Legal Arrangements

Based on the results of its NRA in 2019, Mauritius prioritised a separate ML risk assessment of all its Legal Persons. The exercise was completed in 2019.

Mauritius also developed a Typology Report illustrating the inherent risks posed by Legal Arrangements. A plethora of case studies which identify the vulnerabilities of Legal Arrangements as well as the red flags were also included in the report.

Risk Assessment for the Non-Profit Organisation sector

In line with FATF Recommendation 8 and IO 10, Mauritius completed its first TF risk assessment for the NPO sector in 2020, as part of its commitment to combat the financing of terrorism.

Risk Assessment for Virtual Assets and Virtual Assets Service Providers

In furtherance of the FATF Recommendation 15 which requires countries to identify, assess and understand the ML/TF risks emerging from VA activities and the activities or operations of VASPs, Mauritius conducted its ML/TF risk assessment of VAs and VASPs in 2021, following which the VAITOS Act was enacted.

Enhancing Human Capabilities and Technical Assistance

Several capacity building initiatives were taken to enhance the development of human capabilities within the AML/CFT agencies, enabling them to uphold their skills and knowledge and carry out their functions efficiently and effectively.

Significant technical assistance was received from various international bodies, encompassing capacity building programs, support in conducting risk assessments, enhancing the legal framework and providing expertise in AML/CFT supervision and investigations. The acquired knowledge and tools empowered Mauritius to meet international standards and sustain a robust AML/CFT regime.

Mauritius has, in turn, provided technical assistance to foreign countries with the objective of sharing experience gained and lessons learned in the fight against illicit financial flows. Several workshops/conferences were organised at the global and regional levels for the exchange of good practices and experiences relating to AML/CFT.

All these improvements have culminated in Mauritius joining the top-tier jurisdictions which are 'Compliant' or 'Largely Compliant' to all the 40 FATF Recommendations in September

2022. Additionally, these measures have contributed to enhancing effectiveness as well as maintaining sustainability of all AML/CFT reforms besides addressing emerging ML/TF risks. More details regarding the measures implemented by Mauritius since 2018 are at **Annex 2**.

3. AML/CFT/CPF INSTITUTIONAL FRAMEWORK

The main authorities/committees involved in the fight against AML/CFT/CPF in Mauritius are as follows:

(a) Prime Minister's Office and Ministry of Finance which is a key component of the Mauritius AML/CFT/CPF system. It has, through the Core Group, an important role in the fight against ML, TF and PF. The Core Group is established under section19AA of the FIAMLA and is chaired by the Financial Secretary. Its mandate is to ensure the effective implementation of FATF Standards by the relevant competent authorities, foster interagency cooperation, and make recommendations on relevant policies, strategies, and capacity building initiatives.

(b) Ministry of Financial Services and Economic Planning which oversees implementation of AML/CFT/CPF activities, and coordinates national AML/CFT/CPF legislative, administrative and policy reforms.

(c) Ministry of Foreign Affairs, Regional Integration and International Trade which is responsible for managing the country's diplomatic relations with other countries and international organizations.

(d) The Attorney General's Office (AGO) which is responsible for drafting legislation and providing legal advice to the Government.

(e) The Office of the Director of Public Prosecutions (ODPP) which is the authority which makes the decision on whether or not to prosecute any criminal offence, including any ML/TF offence in Mauritius.

(f) Core Group for Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation, and Combatting Foreign Bribery established under the FIAMLA to amongst others, ensure the effective implementation by the relevant competent authorities of the FATF international standards on AML/CFT/CPF; make recommendations to the Prime Minister on matters, including implementation, strategy and international developments, pertaining to AML/CFT/CPF; decide on matters pertaining to the implementation of AML/CFT/CPF Standards; ensure effective coordination and cooperation with the National Committee and among all competent authorities on matters pertaining to AML/CFT/CPF; formulate policies and make recommendations on skills development and capacity building initiatives, to enhance the capabilities of the competent authorities in the fight against financial crimes.

(g) National Committee for AML/CFT established under the FIAMLA, inter alia, coordinates the development, regular review and implementation of national policies and activities to combat ML, TF and PF collects and analyses statistics and other information from competent authorities to assess the effectiveness of policies and measures to combat ML, TF and PF; makes recommendations to the Minister of Financial Services and Economic Planning for legislative, regulatory and policy reforms for the purposes of combatting money laundering and the financing of terrorism and proliferation; and promotes co-ordination among the public sector

authorities with a view to improving the effectiveness of existing policies to combat ML, TF and PF.

(h) Bank of Mauritius (BoM) which is the licensing and AML/CFT supervisory body for the banks, Non-Bank Deposit Taking Institutions (NBDTI), cash dealers and Payment Service Providers (PSPs), and payment system operators. It issues Guidance Notes, guidelines, and instructions for this sector and has powers under the FIAMLA, the UNSA, the BoM Act, the National Payment Systems Act and the Banking Act to take regulatory sanctions for any breach of the FIAMLA, the UNSA, and guidelines issued to its licensed entities.

(i) Financial Services Commission (FSC) is the integrated regulator in Mauritius for the financial services sector (other than banking) and global business. It also looks at AML/CFT related matters for the non-banking financial institutions. The FSC is mandated under the Financial Services Act (FSA), the Captive Insurance Act, the Insurance Act, the Private Pension Schemes Act, the Securities Act, and the VAITOS Act to license, regulate, monitor and supervise the conduct of business activities in these sectors. As mandated under the FIAMLA, the FSC has issued AML/CFT Handbook[10]that applies to its licensees. It has powers under the FIAMLA, the UNSA and the FSA to take regulatory sanctions against its licensees for non-compliance with AML/CFT requirements.

(j) Gambling Regulatory Authority (GRA) which is the licensing authority and designated AML/CFT regulatory body for the gambling sector.

(k) Mauritius Police Force (MPF), where the Police, through its various specialised divisions investigates suspected ML and TF cases. This enables the gathering of admissible evidence for any prosecution which may follow.

(l) Financial Intelligence Unit (FIU), which has been established under FIAMLA and serves as a central agency for receiving, requesting, analysing, and disseminating information concerning suspected proceeds of crime from ML and TF. It is also the AML/CFT supervisory body for law firm, foreign law firm, joint law venture, foreign lawyer under the Law Practitioners Act, attorney, barrister, notary, as well as the real estate agent and jewellery sectors.

(m) Independent Commission Against Corruption (ICAC)[11] which had, as its core function, the responsibility to investigate and prosecute corruption and ML. It was also mandated to investigate TF as a predicate offence of ML. The ICAC started investigations based on reports and information from Government agencies and other sources. It was also able to start an investigation on its own initiative.

(n) Enforcement Authority (Asset Recovery Investigation Division- ARID)[12]which had the power to restrain and confiscate assets which were reasonably suspected to be

[10] Link: updated-aml-cft-handbook.pdf
[11] Now under the Financial Crimes Commission.
[12] Now under the Financial Crimes Commission.

proceeds of crime, instrumentalities, and terrorist property. The ARID operated under the authority of the FIU.

(o) Integrity Reporting Services Agency (IRSA)[13] was established under the Good Governance and Integrity Reporting Act. This legislation introduced the concept of 'unexplained wealth' which applied to any property that cannot be shown to have been acquired from legitimate sources. Such property may be subject to confiscation by the IRSA through Unexplained Wealth Orders. These are part of non-conviction-based asset confiscation which neither require criminal convictions nor imply any wrongdoing.

(p) Mauritius Institute of Professional Accountants (MIPA) which is responsible for the registration and AML/CFT supervision of professional accountant, public accountant, and Member Firms under the Financial Reporting Act.

(q) Registrar of Companies which is responsible for AML/CFT supervision of Company Service Providers (CSPs).

(r) Registrar of Associations which is responsible for CFT supervision of associations.

(s) Registrar of Cooperatives which is responsible for AML/CFT supervision of Cooperative Credit Unions (CCUs).

(t) Counter Terrorism Unit which is responsible to collect, collate and analyse terrorism-related intelligence and disseminate to investigatory authorities such intelligence concerning suspicious person or activity or terrorism-related offences.

(u) National Sanctions Committee, which is responsible for, inter alia, identifying a party that meets the listing criteria for designation as a listed party on a UN Sanctions List.

(v) Financial Crimes Commission (FCC) which, as of 2024, has subsumed the functions of the ICAC, ARID and IRSA, and is mandated to detect, investigate and prosecute a spectrum of financial crimes. It is also the central agency for asset recovery and declaration of asset matters.

[13] Now under the Financial Crimes Commission.

4. NATIONAL RISK ASSESSMENT METHODOLOGY

Objectives

Identifying, assessing, and understanding ML and TF risks is an essential part of the implementation of a national AML/CFT regime which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. Properly understanding ML/TF risks informs and supports a country's application of AML/CFT measures that are proportionate with the risks, i.e. the risk-based approach that is central to the FATF Standards and should assist countries in prioritisation and efficient allocation of resources[14]. In addition, the results of the NRA should provide useful information to FIs and DNFBPs to support their own assessments and risk mitigation measures.

The main objectives of the second NRA were to:

- Develop and maintain a comprehensive and shared understanding of ML and TF risks across the country, including a review of how these risks have evolved since the previous NRA conducted in 2019;
- Facilitate the development of AML/CFT strategies designed to mitigate the identified ML and TF risks;
- Assist competent authorities in the allocation and prioritisation of resources to combat ML and TF and ensure that appropriate measures are put into place in relevant sectors to mitigate the risks of ML and TF;
- Assist supervisors in conducting proper ML and TF risk assessments; and
- Assist reporting persons in identifying, understanding, managing, and mitigating the ML and TF risks.

Methodology

The NRA was conducted using the revised National ML and TF Risk Assessment Tool developed by the World Bank. In accordance with the World Bank tool, the following factors were assessed:

(a) The scale and characteristics of the proceeds of criminal activities from internal and external sources;
(b) The scale and characteristics of TF in Mauritius;
(c) The weaknesses or gaps in the ability to combat ML and TF; and
(d) The ML and TF weaknesses or gaps arising from the financial services sector as well as DNFBPs in the country.

[14] FATF ML National Risk Assessment Guidance at page 6 available at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf

Key Concepts and Terms

For the purpose of assessing ML/TF risk at national level, risk was regarded as a function of three factors: threat, vulnerability, and consequences, defined below:

(a) *Threats* mean assessing the predicate offences that generate proceeds of crime, the total size of the proceeds of crime, and the sectors in which the proceeds of crime are invested and laundered;
(b) *Vulnerabilities* mean identifying the weaknesses or gaps in relation to the threats that can be exploited for ML and TF activities; and
(c) *Consequences* are the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity. The assessment of consequences is included in the assessment of threats and vulnerabilities as opposed to being treated as a separate independent factor.

Main Revisions brought to the World Bank NRA Methodology

As compared to the NRA (2019) exercise, Mauritius used the TF Risk Assessment Tool (2022) of the World Bank which included revised modules on National TF threat and vulnerability along with a new module on TF sectoral vulnerability for the conduct of the second NRA exercise.

ML and TF Threat Assessment

The ML threat assessment included:

i. A review of all the incidents based on the seriousness and magnitude of domestic and international crimes;

ii. The estimated amount of proceeds generated and the potential of ML; and

iii. The capacity and resources of criminal actors and their level of sophistication to launder proceeds (including third-party launderers).

For the assessment of ML threat, the offences under the Mauritian Law were examined in line with the FATF categories of offences. The predicate offences referred to crimes that generated proceeds that were subsequently laundered to appear legitimate. ML threat ratings were assigned to the predicate offences.

The TF threat assessment was conducted to identify, analyse, and understand the threats associated with TF at both national and sectoral levels. It assessed all aspects of raising, moving, storing, and using funds to finance terrorist people, organisations, or operations.

National ML and TF Vulnerability Assessment

The assessment of ML and TF vulnerability aimed to:

(i) Identify the overall vulnerability of the country to ML and TF;

(ii) Identify the weaknesses and gaps in the country's ability to combat ML and TF; and

(iii) Prioritise actions that will improve the country's ability to combat ML and TF by strengthening AML and CFT controls at national level.

The level of national ML and TF vulnerability of a country depends on the level of:

(i) the national ability of the country to combat ML and TF; and

(ii) the overall sectoral ML and TF vulnerability which assesses the overall vulnerability of the sectors under assessment.

Assessment of National Ability to Combat ML and TF

The national combatting ability is a comprehensive assessment based on input variables assessed by the NRAWG. These variables attempt to capture the high-level factors in the country such as the quality of the judicial processes, the effectiveness of the law enforcement, domestic and international cooperation.

Assessment of sectoral ML and TF Vulnerability

Under the sectoral ML and TF vulnerability assessment, the variables assessed were broken down into two subcategories namely AML/CFT control variables and inherent vulnerability variables. The AML/CFT control variables relate to the quality and effectiveness of the AML/CFT controls. The inherent vulnerability variables relate to specific features and users of a particular product or business or profession.

Sectors Under Assessment

In line with the World Bank tool, the sectors listed in Table 5 were assessed as part of the NRA exercise:

Table 5: Sectors assessed for the NRA exercise

Sectors	AML/CFT Supervisory Authority
Financial Institutions (FIs)	
• Banking • Other Financial Institutions (OFIs) - Non-Bank Deposit Taking Institutions (NBDTIs) - Cash Dealers - Payment Service Providers (PSP)	Bank of Mauritius
• Insurance • Securities • Trust and Company Service Providers (TCSPs) • OFIs - Leasing Companies - Payment Intermediary Services (PIS) - Investment Banking - Treasury Management - Credit Finance - Asset Management - Distribution of Financial Products - Pension Scheme Administrators - Custodian (Non-CIS) - Family Office (Single) - Family Office (Multiple) - Peer to Peer Lending - Funeral Scheme Management - External Pension Schemes - Actuarial Services - Factoring - Credit Rating Agencies - Global Legal Advisory Services - Compliance Services - Crowdfunding - Fintech Service Provider - Robotic and Artificial Intelligence Enabled Advisory Services	Financial Services Commission

Sectors	AML/CFT Supervisory Authority
- Representative Office (for financial services provided by a person established in a foreign jurisdiction)	
• OFIs - Cooperative Credit Unions (CCUs)	Registrar of Cooperative Societies
Designated Non-Financial Businesses and Professions (DNFBPs)	
• Law firm, foreign law firm, joint law venture, foreign lawyer, under the Law Practitioners Act • Attorney • Barrister • Notary	Financial Intelligence Unit
• Professional accountant and public accountant under the Financial Reporting Act only where they are sole practitioners, partners or employed professionals within member firms • Member firms under the Financial Reporting Act	Mauritius Institute of Professional Accountants
• Dealer in jewellery, precious stones, or precious metals	Financial Intelligence Unit
• Real Estate Agents	Financial Intelligence Unit
• Person licensed to operate a casino and gaming houses	Gambling Regulatory Authority
• Company Service Providers (CSPs)	Registrar of Companies

CSPs and PSPs were new sectors under assessment in this NRA exercise.

Relative Importance of Sectors

The following indicators were used in order to assess size/share and importance of sectors: (i) contribution value per sector[15] as provided by Statistics Mauritius; (ii) maturity of the sector (in terms of AML/CFT Supervision); (iii) the level of international exposure; (iv) the key role of a particular profession/sector in multiple sectors; and (v) prevalence of informal business activities in the sector.

[15] For the year ended 2023.

Re-establishment of the NRA Working Group

In accordance with the World Bank Model, Mauritius re-established the NRAWG composed of all AML/CFT related stakeholders, including representatives from LEAs, FIU, FI and DNFBP supervisors, the National Sanctions Secretariat, the Registrar of Associations and the private sector. More details regarding the NRAWG are at **Annex 1**.

Data Collection

Collection of data is key to the NRA process as it provides for the identification of ML and TF risks and is the foundation for subsequent analysis and evaluation. In this respect, the second NRA exercise integrated both quantitative and qualitative data to ensure a comprehensive and robust understanding of ML/TF threats and vulnerabilities faced by Mauritius. The main sources of data used were as follows:

- Data from FIU and other Intelligence Agencies;
- Data from LEAs;
- Data from FI and DNFBP Supervisors;
- Data from FIs and DNFBPs;
- International reports including FATF typologies, Transparency International Report, Afrobarometer Index, US Trafficking in Persons Report and 'Know Your Country' Reports; and
- Local and international press articles.

Assessment Period

Covering the period from January 2018 to December 2024, the NRA provides a detailed snapshot of ML/TF activity, at national and sectoral levels for the period January 2018 to June 2022, and major developments including an updated assessment of emerging threats, for the period July 2022 to December 2024. Though the risk assessment is an ongoing process, Mauritius is transitioning to a more regular and dynamic process of assessing ML and TF risks that requires the collaboration of all authorities and private sector to continuously monitor and address risks posed to the jurisdiction. This approach aims to implement actions identified in the risk assessment and provide more frequent updates to both the private sector and the public regarding ML and TF risks.

Involvement of Private Sector Representatives

The private sector, including representatives from FIs and DNFBPs, was also involved in the sectoral assessments of ML as well as TF vulnerability, to ensure that industry insights were incorporated into the risk assessment. The involvement of the private sector also served to increase its awareness of the NRA, as FIs and DNFBPs are key audiences for the NRA.

The industry has contributed in the NRA exercise, namely, (i) through participation in sectoral teams, where members provided insights during meetings, for assessing various factors; and (ii) participation through surveys and focus group discussions.

National Analysis of ML/TF Risks

5. NATIONAL MONEY LAUNDERING RISKS

SUMMARY OF FINDINGS:

The overall ML risk for Mauritius was **Medium-High**, derived from a combination of the National ML threat rated as **Medium-High** and the National ML Vulnerability also rated as **Medium-High**.

National ML Threat

Threat identification was the starting point for understanding ML risks. The assessment of ML threats included the identification and quantification of the predicate crimes for ML and methods supporting ML in Mauritius. A proper understanding of the ML threats in Mauritius will allow for better policymaking and regulatory measures to prevent or mitigate ML practices effectively.

As outlined in Table 1, the overall ML Threat for Mauritius was rated **Medium-High**. The components of the ML threat rating in Mauritius were (i) internal sources – i.e., laundering of proceeds from offences committed domestically, and (ii) external sources - i.e., laundering of proceeds from offences committed abroad. The level of external ML threat (**High**) to Mauritius was assessed to be greater than the level of internal ML threat (**Medium**).

Domestic/Internal Threats

Key Findings

The Internal ML threat was rated **Medium**.

The three main sources of proceeds generating crimes were illicit trafficking in narcotic drugs and psychotropic substances, fraud, and illegal bookmaking. Illicit trafficking in narcotic drugs and psychotropic substances remained a significant concern, with traffickers often laundering money through various businesses, high-value asset purchases or lifestyle laundering. Fraud, including electronic fraud, saw a sharp increase during the COVID-19 lockdown. A certain level of sophistication was noted in the commission of illegal bookmaking. Bets were placed through WhatsApp, SMS messages, phone calls and payments were done through internet/ mobile banking.

Institutional Arrangements

The ICAC was the leading LEA for the detection, investigation and prosecution of ML and corruption offences since 2002. The ICAC was further conferred the mandate to enforce the provisions of the Declaration of Assets Act since 2019 following its proclamation. As of 2024, the ICAC has been subsumed by the FCC[16], which is now vested with the responsibility to

[16] The ICAC has been subsumed in the FCC established under the FCC Act which was proclaimed in March 2024.

detect, investigate, and prosecute, in addition to ML offences and corruption, a plethora of new offences - financial crimes as well the financing of drugs dealing. The ICAC, and now the FCC, works closely with the MPF in investigating ML cases.

The MPF is empowered to investigate all crimes, including ML. The MPF initiates an ML investigation in all funds-generating predicate offences, such as drug trafficking, fraud, and larceny. ML investigation may also be initiated as a stand-alone offence, e.g. where huge sums of money have been secured during a raid conducted by the Anti-Drug and Smuggling Unit (ADSU).

Another major development since the last NRA exercise was the setting up of an AML/CFT Coordination Taskforce (A.C.T) in 2021 under the chairmanship of the ODPP to ensure multilateral coordination into the investigation of ML cases. The A.C.T is dedicated to providing assistance to all agencies in overcoming any challenge to effectively coordinate AML/CFT investigations and prosecutions.

For the period January 2018 to June 2022, LEAs have investigated 1,613 ML cases compared to 711 in the last NRA report. Out of the 1,613 ML investigations, 625 cases are still live, 97 cases are pending trial before Court and convictions were obtained in 64 cases.

Cases where investigation has been discontinued stood at 685 as, amongst others, no ML offences were identified. The status of the remaining 142 cases are as follows:

- Cases suggested for prosecutions and pending advice from ODPP: 112
- Cases kept in abeyance: 1
- Cases dismissed at Court level: 29

During the period under review, there was a significant increase in the number of ML investigations by the MPF due to the fact that since the MER 2018, several measures in relation to ML investigations were initiated which resulted in the increase of cases investigated, prosecuted and convicted as compared to the last NRA.

Comparison of ML Threat Rating

Table 6 summarizes the internal ML threat associated with each predicate offence in Mauritius and makes a comparison with the last NRA.

Table 6: Comparison of ML Threat ratings

2014-2017	2018-June 2022
High	**High**
▪ Illicit trafficking in narcotic drugs and psychotropic substances ▪ Fraud ▪ Illegal bookmaking	▪ Illicit trafficking in narcotic drugs and psychotropic substances ▪ Fraud ▪ Illegal bookmaking
Medium-High	**Medium-High**
▪ Robbery/theft (Larceny) ▪ Tax Crimes	▪ Robbery/theft (Larceny) ▪ Corruption
Medium	**Medium**
▪ Corruption ▪ Trade-Based Money Laundering	▪ Tax Crimes ▪ Trade-Based Money Laundering ▪ Trafficking in human beings and migrant smuggling/Sexual exploitation, including sexual exploitation of children
Medium-Low	**Medium-Low**
▪ Environmental crime – Illegal Fishing ▪ Insider Trading and Market Manipulation ▪ Trafficking in human beings and migrant smuggling/Sexual exploitation, including sexual exploitation of children	▪ Environmental crime – Illegal Fishing ▪ Insider Trading and Market Manipulation ▪ Professional Money Laundering
Low	**Low**
▪ Extortion ▪ Illicit arms trafficking ▪ Illicit trafficking in stolen and other goods ▪ Counterfeiting currency ▪ Counterfeiting and piracy of products	▪ Trading without Licence ▪ Piracy ▪ Illegal public collection ▪ Extortion ▪ Smuggling

▪ Murder, grievous bodily injury ▪ Kidnapping, illegal restraint and hostage-taking ▪ Smuggling ▪ Piracy	

Based on the comparison of ML threat rating, the analysis revealed that rating remained the same between the two assessment periods in terms of illicit trafficking in narcotic drugs and psychotropic substances, fraud, and illegal bookmaking which continue to have the highest rating.

Predicate Offences identified as High Money Laundering Threats

(a) Illicit trafficking in narcotic drugs and psychotropic substances

Illicit trafficking in narcotic drugs and psychotropic substances remained a critical threat to the national security, social stability, and financial integrity of Mauritius. The Dangerous Drugs Act (DDA) criminalises drug-related offenses. Section 30 of the DDA provides a broad definition of drug dealing, encompassing activities such as organising, financing, importing, manufacturing, distributing, selling, and transporting dangerous drugs. Section 41(4) categorises individuals as drug traffickers if the street value of seized drugs exceeds MUR 1 million (approximately USD 25,000).

Nature and Scope of the Threat

The illicit drug trade in Mauritius has evolved significantly due to globalisation, improved transportation, and enhanced communication technologies. The primary narcotics found in Mauritius included heroin, cocaine, synthetic drugs, methamphetamine, ecstasy, and cannabis. Drug trafficking generated substantial illicit proceeds and remained a primary source of ML cases.

During the period January 2018 to June 2022, a total number of 6,539 cases related to drug dealing. Out of these reported cases, 1,118 resulted in convictions, representing 17% of the total drug dealing cases. Between 2018 and June 2022, drug seizures in Mauritius had an estimated street value of USD 267,522,821, while cash secured in drug related cases amounted to USD 3,501,100, reflecting the scale of drug-related offences.

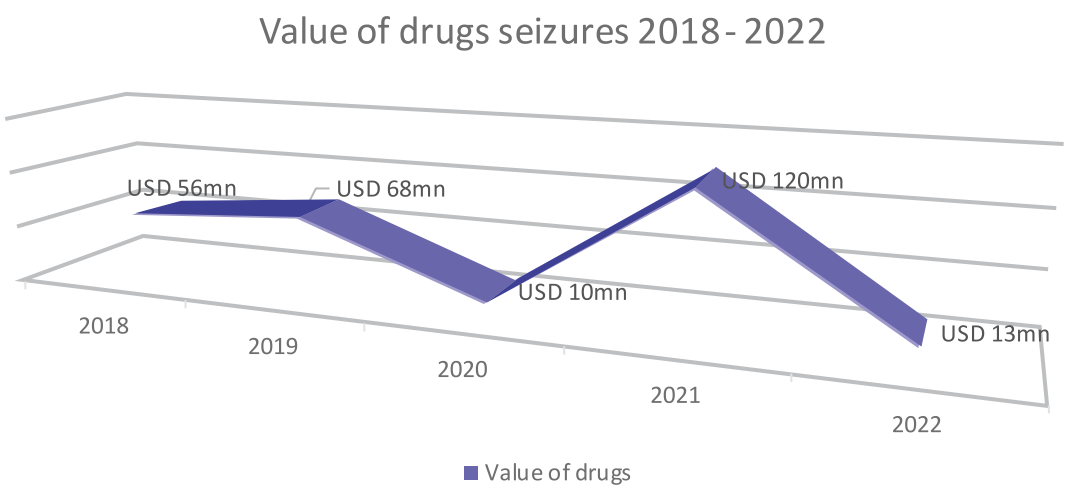


Chart 2: Value of drug seizures 2018 - 2022

Mauritius witnessed the biggest drug seizure in its history in May 2021 where approximately 26 kilograms of hashish and 244 kilograms of heroin, with a total estimated value of approximately USD 104 million, were discovered buried on a plot of land in the north of the island.

Synthetic Cannabinoid compounds reach the shore of Mauritius from the East Asian market primarily in the form of precursors. This drug is mostly consumed by youngsters as it is cheap. Synthetic cannabinoid is of heightened concern for law enforcement as local dealers mix the precursors with locally available licit substances, thus posing serious threat to public health.

Money Laundering Techniques Related to Drug Trafficking

Intelligence gathered highlighted the following methods used to launder illicit drug proceeds:

- Casinos: Drug proceeds were converted into gambling chips and later redeemed as 'winnings'.
- Luxury Items: High-value purchases such as jewellery, watches and art were resold to integrate illicit funds.
- Real Estate: Property transactions, renovations and rental income were used to clean dirty money.
- Shell Companies: False invoicing and complex corporate structures obscured illicit financial flows.
- Cryptocurrencies: Used for anonymous cross-border transactions and layering illicit funds.
- Trade-Based Money Laundering: Manipulation of invoices and fictitious trade transactions to conceal proceeds.

For the period under review, there were 650 ML investigations where drug trafficking was alleged to be the predicate offence. Out of the 650 ML cases, 204 cases were investigated by the ICAC and 446 cases were initiated by the MPF (ADSU). The number of ML prosecutions and convictions were 98 and 30, respectively.

(b) Fraud

Fraud is an illegal act of using deception to obtain ill-gotten benefits such as money, goods, services, and other valuables. There are a number of offences under the Mauritian legislation which effectively encompass fraudulent behaviour. The categories of fraudulent behaviour which were most prevalent in Mauritius included embezzlement, swindling and forgery. The number of fraud cases reported for the period under review was 3259, and the total amount of money defrauded through various schemes amounted to USD 57,365,749.44. Embezzlement, forgery, and electronic fraud generated the most proceeds.

Out of the 3,259 predicate cases of fraud, 99 ML investigations were conducted by the MPF and 131 ML cases by the ICAC. The total number of prosecutions and convictions for both MPF and ICAC stood at 71 and 22, respectively.

Electronic fraud such as bogus investment schemes and crypto scams emerged as the highest threats in terms of occurrence, the amount of money involved, and the difficulty in identifying and tracing the suspects who may be operating across borders. During the period under review, a total of USD 11,552,274 was defrauded. The fraudsters targeted both private individuals and management companies. While individuals were lured to engage in dubious investment schemes, the management companies were victims of hacked e-mail accounts, following which they were instructed to divert money to foreign bank accounts.

(c) Illegal Bookmaking

Bookmaking in Mauritius involves the taking of bets on horse racing and football. Bookmaking on horse racing is confined to local events, whereas football bookmaking involves international matches. Bookmaking is regulated by the GRA under the Gambling Regulatory Authority Act 2007 (GRA Act), whereby bookmakers have an obligation to register with the GRA. During the period under review, a gradual increase was noted in the number of bookmakers conducting activities without a licence, particularly post COVID -19 pandemic.

During the period under review, a total of USD 73,436 associated with illegal betting was secured, and these include 34 cases of illegal bookmaking. ML investigations were initiated in all cases, and they are ongoing.

ML investigations demonstrated that there was a link between horse racing and drug trafficking where drug traffickers emerged as big punters. During 2022, USD 217,391 was confiscated in relation to one such case.

A change in the modus operandi used by illegal bookmakers included new modes of payments such as mobile payment systems. Proceeds derived from illegal bookmaking were used by perpetrators to acquire moveable properties in Mauritius. Most of the offenders were business

owners (shop and restaurant owners) who commingled proceeds derived from their illegal activities and their business activities.

Predicate Offences identified as Medium-High Money Laundering Threats

(a) Robbery or Theft (Larceny)

In Mauritius, robbery or theft is referred to as larceny and criminalised under different sections of the Criminal Code. Section 301 of the Code cater for simple larceny cases whereas sections 303 to 306 pertain to larceny with aggravating circumstances for which a higher penalty is imposed. In relation to cases of larcenies, sections 40 and 40A of the Criminal Code deal with the possession of stolen property and dealing in stolen goods. Additionally, under section 123 of the Criminal Procedure Act, the charge for larceny can be substituted to that of embezzlement which falls under the category of fraud.

During the period under review, 41,118 cases of larceny were investigated. Simple larceny represented 82% of the number of cases and the remaining 18% were cases of larceny with aggravating circumstances. The number of prosecutions secured were 10,188 and convictions were secured in 20,298 cases. Proceeds generated by these cases amounted to USD 43,869,641, out of which, an amount of USD 17,539,216.50 represented High Value Larceny.

During the period under review, 317 ML investigations were initiated by the MPF for larceny, out of which 57 ML investigations were triggered for High Value Larceny cases. Of these cases, 21 cases were prosecuted. Additionally, the ICAC investigated 11 ML cases with a predicate offence of larceny by a person in receipt of wages.

ML investigations revealed that most cases were self-laundering through the acquisition of property and merry making. Third-party laundering involved the use of intermediaries to dispose of property stolen and was particularly related to cases where items such as jewellery and other valuables were stolen.

(b) Corruption

Corruption remained a challenge in Mauritius, with the country's threat level for ML linked to corruption rated as **Medium-High**. The offence is criminalised under the Prevention of Corruption Act 2002 (POCA). Acts of corruption include offering or accepting bribes, abusing public office for personal gain, and influencing public officials illegally.

Despite the challenge, Mauritius has made some progress, improving its position in the Transparency International Corruption Perception Index, rising from 57th to 55th in 2023. The ICAC initiated 1,437 corruption investigations during the period under review, with a particular focus on cases involving bribes and facilitation payments. The total proceeds seized/attached were USD 10,171,699. Many of these investigations, especially post-COVID, were related to tenders allocated during the pandemic emergency. The number of prosecutions and convictions stood at 72 and 48, respectively.

Some of these investigations are still ongoing. A closer look at the ML investigations connected to corruption (29 cases during the period under review) revealed a pattern of siphoning Government funds through corrupt practices, often involving the public sector. Out of the 29 ML cases predicated on corruption, 17 cases were prosecuted.

Predicate Offences identified as Medium Money Laundering Threats

(a) Tax Crimes

Mauritius has a self-assessment tax system whereby taxpayers compute their tax liability, file their returns, and pay their taxes accordingly. The country has achieved almost 100% e-filing, reflecting a culture of tax compliance, ranking 5th in the World Bank's Ease of Paying Taxes Index (2020). A 2023 Mauritius Revenue Authority (MRA) taxpayer satisfaction survey revealed that 94% of participants believe that the trust of taxpayers in MRA has improved, while 90% affirmed that MRA is doing a lot to detect tax evasion.

Residents are taxed on local income as well as foreign income remitted to Mauritius, while non-residents are taxed only on Mauritian-sourced income. To recover taxes not paid by taxpayers, the MRA conducts investigations which may result in either assessment in cases where additional taxes have to be paid or prosecution in cases where offences are detected.

On average, tax assessments by the MRA accounted for 3% of the total returns filed. Between financial years 2016/2017 and 2020/2021, the MRA collected MUR 445 billion (USD 12.3 billion), out of which around MUR 28 billion (around USD 795 million) was collected through assessments raised on individuals and legal persons.

Investigation and Prosecutions

The MRA, through its Legal Services Department, initiated prosecution proceedings against taxpayers where offences were established under Revenue law. These offences ranged from non-submission of returns/documents to tax evasion. The MRA lodged 171 cases at Court during financial years 2016/2017 to 2021/2022 and there were 148 Court decisions for the same period, securing USD 500,473 as the total amount of fines imposed on the court decisions obtained. The said value encompassed both cases of suspected tax evasion and cases involving a genuine misunderstanding of the Revenue law by taxpayers. It was, therefore, difficult to accurately determine the exact proportion of the value of proceeds emanating from deliberate tax evasion.

In financial year 2019/2020, 3 out of 150 tax investigations were referred to prosecution for tax evasion. By financial year 2021/2022, this number rose to 20, which may be due to a significant increase in investigations completed (from 150 to 667) and trainings provided to investigators in detection of tax evasion cases. The number of investigations in 2019/2020, (150), was relatively lower due to the national lockdown. The average percentage of number of cases referred for prosecution for tax evasion was around 3% of total number of investigations completed during income years ending 30 June 2020 to 30 June 2022, which represents a reasonably low level of tax evasion cases.

Tax Evasion Typologies/Trends identified during investigations

Most of the cases pertaining to individuals referred for prosecution for tax evasion were allegedly involved in drug trafficking. The investigations revealed that these individuals held substantial funds in their bank accounts which did not corroborate with their income tax declarations. Similarly, the majority of the companies referred to for prosecution were owned and controlled by persons who were also involved in drug cases. Some of the companies were involved in VAT fraud whereas several companies overclaimed their expenses or underdeclared their turnover.

MRA investigated into cases where FIU reported punters evading the 10% tax on winnings in casinos, by sharing their gains with other punters at times of pay-outs. Investigation has been completed into 20 such cases and assessments of an approximate amount of MUR 16 million have been issued. One such case has also been referred to ICAC for ML investigation and prosecution proceedings have been initiated for failure to submit information and particulars under the Income Tax Act.

The OECD flagged the use of 'phantomware' and 'zapper' by taxpayers to manipulate sales records in its report namely 'Technology Tools to Tackle Tax Evasion and Tax Fraud.' Phantomware is a software installed in sales registers to manipulate sales records, while zapper is an external device or program that connects to the cash register to perform the same function. The OECD report also flagged the risk of false invoicing, i.e., seeking to over-report deductions, and to falsify invoices to mask non-deductible personal expenses as legitimate deductions. With a view to addressing the above tax evasion typologies, MRA introduced an e-Invoicing system at the national level in a phase-wise approach. With the advent of this e-Invoicing system, providers of products and services will be required to fiscalise their invoices or receipts in real time with the MRA before issuing them to their customers. It will be mandatory for economic operators to issue fiscal invoices. Initially, economic operators having an annual turnover exceeding MUR 100 million are required to join the MRA e-Invoicing system. Subsequently, e-Invoicing will be extended progressively to other taxpayers.

Collaboration with LEAs

Following signature of an Memorandum of Understanding (MOU) between the MRA and ICAC in May 2021, the number of cases referred by MRA to ICAC having tax evasion as a predicate offence for ML increased from 13 referrals during income year ended 30 June 2021 to 20 referrals in income year ended 30 June 2022. The MOU strengthened the existing collaboration between the two agencies as regards exchange of information in cases having both tax evasion and ML. In one case of tax evasion, which was lodged at the FCD, prosecution proceedings have been completed, and the taxpayer was sentenced to pay the tax fine. Enquiry has been completed in another VAT fraud case which will be lodged for prosecution shortly. This case is being prosecuted for ML offences.

During the period under review, the MRA referred 8 cases to the Police des Jeux. The MPF requested information on 5 cases, which were promptly provided. Additionally, the MPF referred 6 cases to the MRA concerning suspected illegal bookmaking activities. Investigation was completed in two cases, and one did not result in any additional tax liability, while the other led to assessments of MUR 482,333. Investigations are still ongoing into the 4 other

cases. It is worth noting that the number of cases investigated, and assessments raised in relation to illegal bookmaking represents a small proportion of the total number of investigations completed (0.4%) and the total amount of assessments issued (0.1%), respectively.

Moreover, the MRA conducts risk-based desk and field audits on all persons. The MRA has adopted the risk scoring system (based on OECD) and predictive model (based on IMF) methodologies for selection of cases for audits. It has implemented a Compliance Risk Management System and Tax Risk Management System through which the MRA identifies cases where taxpayers have failed to properly declare their income.

One of the key Recommended Actions of the previous MER was that the MRA should investigate and prosecute tax evasion offence as a predicate offence to ML. Since then, a series of reforms and efforts have been made to address the Recommended Action. The figures reported above show this positive trend. Tax evasion cases are now being prosecuted not only under Revenue laws but also referred to ICAC to be investigated and prosecuted as a predicate offence to ML.

Following amendments to the Income Tax Act through the Finance Act, gains or profits derived from the sale of VAs have been exempted from income tax, effective from 01 July 2024. Moreover, investigations have, so far, not revealed any cases of tax evasion where VAs have been used.

(b) Trade Based Money Laundering

MRA customs registered 5,575 cases of under-invoicing where the declared value of goods was considered to be low and were subsequently adjusted to reflect the actual value. The additional customs duties and taxes collected were MUR 98,281,201.

Investigation was also conducted into cases of double invoicing which have resulted in payment of additional duties, taxes and penalties amounting to MUR 3,418,507.

Furthermore, after preliminary investigation, MRA Customs referred suspected cases of ML and Trade-Based Money Laundering to the ICAC for in-depth and comprehensive investigation. The investigation is ongoing.

Although ICAC detected and investigated only one case of Trade-Based Money Laundering during the period under review, it acknowledges that such cases are hard to detect and investigate because of their complex nature.

(c) Trafficking in human beings and migrant smuggling/Sexual exploitation, including sexual exploitation of children

Trafficking in human beings and migrants and sexual exploitation are criminalised in Mauritius under The Combatting of Trafficking in Persons Act 2009 and The Children Act 2020. There have been relatively few reported cases of trafficking in human beings and migrants, as well as the sexual exploitation of children, foreigners, and Mauritians in the country. The types of trafficking in persons cases detected, involved the exploitation of foreigners mainly

Bangladeshi and Malagasy nationals at their workplace and the sexual exploitation of female foreigners from Eastern European countries. The domestic cases related mostly to sexual exploitation of female sex workers and female juveniles. The proceeds of the crimes were generally laundered through the acquisition of property, investment in businesses amongst others.

During the period under review, it was observed that an average of 4 cases of child exploitation and 2 cases of human trafficking involving adults were reported yearly. The child exploitation cases related to minors (females) being forced for child prostitution by their relatives. It was also observed that children were involved in cases of forced labour, where school dropouts were forced to work in the construction and commercial sector. Money earned was remitted to their relatives to procure their basic needs.

There were no ML cases associated with this predicate offence during the period under review.

According to intelligence gathered, foreigners from African countries and Eastern Europe, who came to Mauritius on tourist visas, were involved in prostitution. However, investigations so far did not indicate the existence of any organised crime or networking related to human trafficking. In recent years, there has been a significant increase in foreign workers as well as the arrival of tourists visiting the country. There is the risk that traffickers can exploit foreign migrants for human exploitation. As such, the exploitation of foreign workers is geared towards profit making, which generates higher returns. On the other hand, the domestic cases are mainly associated with poverty. Hence, the ML risk associated with foreign workers/nationals is higher than domestic human trafficking cases.

Predicate Offences identified as Medium-Low Money Laundering Threats

(a) Illegal Fishing

Illegal fishing in Mauritius falls into two categories namely those committed in the lagoon and those committed in the high seas within the Mauritian Exclusive Economic Zone. Most of the cases detected were in the lagoon and were very few in number. The fish were meant mainly for own consumption. During the period under review, there was only one instance of illegal fishing detected by the National Coast Guard in the high seas. The coast guard discovered a certain quantity of sharks of different species, intended for foreign markets, stored in the hold of a ship. Due to the vastness of the Exclusive Economic Zone of Mauritius, illegal fishing is likely to be undetected. As a result, despite the limited number of illegal fishing cases detected, there is the potential for foreign countries to carry out illegal fishing in the Mauritian waters while remaining undetected. The sale of fish in the international market is likely to be significant. Taking all of this into consideration, the ML related to illegal fishing is considered as **Medium-Low.**

(b) Professional Money Laundering

In the previous NRA, professional ML in terms of domestic predicate offences in Mauritius was relatively rare. However, during the period under review, it was noted that professionals were exposed to tremendous amounts of information and acted on behalf of their customers in many transactions. Some of these transactions were highly vulnerable to ML risks due to the nature of the product or service offered.

(c) Insider Trading and Market Manipulation

According to the FATF, insider trading involves situations where the person who buys and sells securities, whether a company insider or not, does so in violation of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Market manipulation, on the other hand, refers to conduct that is intended to deceive investors by controlling or artificially affecting the market for a security. In that respect, the offence of 'insider trading and market manipulation' is criminalised under section 111(4) of the Securities Act (2005) in Mauritius.

Predicate Offences identified as Low Money Laundering Threats

(a) Other Offences

A **Low** ML threat was also attributed to the following categories of offences: extortion, trading without licence, illegal public collection, smuggling, and piracy. This was because statistics and information on each of these categories of offences indicated a small number of reported cases, low capacity in terms of sophistication, networks and resources, a very reduced scope of activity, low criminal proceeds, and very few ML cases linked to the predicate offences.

External Threat

Cross-Border Threats

Given its unique and strategic location in the Southern Indian Ocean, Mauritius is intimately tied to developments in both Sub-Saharan Africa and South Asia and, as a result, is bound to experience both domestic and external ML threats. Accordingly, an assessment of cross-border ML threats to Mauritius needs to include not only examining the laundering of proceeds of crime committed outside the country, but also the laundering of domestically generated proceeds of crime in other jurisdictions.

Financial Inflows and Outflows

Mauritius registers significant cross-border financial flows mostly geared towards investments globally. The data points to insignificant exposure to countries of high risk of unwarranted flows. It is also worth noting that in spite of the adverse impact of the COVID-19 pandemic, the Mauritius IFC demonstrated much resilience, rebounding promptly in 2021 with the Net Asset position of the country standing at USD 41 billion compared to USD 18 billion in 2020[17]. The main cross-border financial flows were in the form of direct investment flows. Country data indicated that the main direct investment source countries included the United States, Cayman Islands, and Singapore, while the main direct investment destination countries were

[17] Source – BoM

India, Singapore, and the United Kingdom. As of end December 2021, Mauritius direct investment assets stood at USD 304 billion compared to USD 261 billion in 2020, while its direct investment liabilities were USD 348 billion higher than USD 308 billion a year ago[18].

Mutual Legal Assistance

Mauritius has a comprehensive legal framework relating to international cooperation and has the ability to provide international legal assistance through the Mutual Assistance in the Criminal and Related Matters Act, the Extradition Act, and other forms of international cooperation. This assistance is provided based on multilateral and bilateral treaties and arrangements, MOU, administrative arrangements and membership of law enforcement/sector and regulatory groupings.

The types of assistance that usually require a formal request are, inter-alia, the following: obtaining of a testimony witness; interviewing a person as a suspect; obtaining account information and documentary evidence from banks and OFIs; requesting for a search and seizure; obtaining internet records and the contents of emails; and the transferring of consenting persons into custody for testimony to be given.

The Attorney General is the Central Authority responsible for processing incoming and outgoing requests pertaining to Mutual Legal Assistance (MLA) in Mauritius. In respect of incoming requests, the Central Authority considers the request and considers the statutory requirements for providing assistance and the relevant grounds for refusal, if any. Where the Central Authority grants a request, an ex parte application is made to the Judge in Chambers, where appropriate, for: (a) an evidence-gathering order; (b) a restraining order in relation to proceeds of crime located in Mauritius; (c) the registration of foreign restraining or confiscation orders; (d) the issue of a search warrant; or (e) a virtual evidence-gathering order. Regarding execution and transmission of evidential material to the requesting state, the evidence is produced to the Court pursuant to a court order. The Court then order that the evidence is handed over to the Central Authority for transmission to the requesting state either via diplomatic channels or by courier (in case of urgent matters). In respect of outgoing requests, same is drafted as per instructions and requirements of the Mutual Assistance in the Criminal and Related Matters Act and sent to the requested state via diplomatic channels.

External Money Laundering Threats

(a) Fraud

Mauritius has a robust financial services sector, but it is not immune to fraudulent activities. Instances of investment scams, ponzi schemes, and unauthorized financial services providers have been reported in the past. Given the nature of its financial services sector,

[18] Source - Coordinated Direct Investment Survey (CDIS) by the International Monetary Fund (IMF)

Mauritius may be subject to abuse for ML purposes by persons who attempt to move proceeds of frauds committed elsewhere through Mauritius. The FSC plays a crucial role in regulating and monitoring financial entities to prevent fraud. The financial services sector adheres to an internationally recognized legal framework that includes the FSA, the Securities Act, and the Insurance Act. However, intelligence indicates that there have been several cases in the past where suspected fraud proceeds were received in Mauritius, particularly through Global Business Companies (GBCs). These alleged cases relate to proceeds generated overseas in various types of fraud such as embezzlements, electronic fraud, pension fraud and securities fraud. These funds are either directed to or transited through the Mauritian banking sector.
The ML threat associated with international fraud is considered **High**.

(b) Corruption

The 2020 amendment to the POCA in Mauritius made significant strides in combatting corruption and criminalising offenses involving foreign public officials and legal entities. The 2018 Financial Secrecy Index highlighted concerns over missing public funds and corruption, often funnelled through Mauritius, particularly within its global business sector. This sector has been linked to several international scandals, especially involving Politically Exposed Persons (PEPs) from Asia and Africa.

Mauritian authorities actively engaged in handling such cases, exchanging information with foreign LEAs through formal channels such as the FIU, as well as informal intelligence-gathering and MLA requests.

As the nearest financial centre to Africa, Mauritius is seen as a potential platform for laundering proceeds of corruption using complex corporate structures. Investigations have identified instances where alleged corruption proceeds were routed through Mauritius via kickbacks and illicit transactions. One such case involved two foreign PEPs from Africa who were linked to fraudulent acts and ML through their involvement in five GBCs. These PEPs, who were subject to international arrest warrants, had connections to the companies as shareholders, Beneficial Owners (BOs), or authorized signatories, resulting in the attachment of their bank accounts in Mauritius.

The investigation is ongoing, with authorities awaiting further information from foreign counterparts to trace the origin of the illicit funds. The investigation has resulted in the attachment of all the bank accounts held in Mauritius in names of the 5 GBCs and the quantum of the attached funds are USD 13,219,502. Additionally, new technologies, such as the use of cryptocurrencies like Bitcoin, are emerging as potential tools for foreign PEPs to obscure the source of corruption proceeds, posing new challenges for financial crime investigations.

The ML threat associated with international corruption is considered **Medium-High**.

(c) Tax Evasion

Financial sectors are major contributors to economies worldwide. The flipside of this fact is that they can be abused by foreign individuals and entities to launder proceeds of crime, including the proceeds generated from tax evasion abroad. Mauritius is no exception to this.

Despite the fact that the financial sector of the Mauritian economy has over the years emerged and positioned itself as a reputable and resilient IFC compliant with international standards, the possibility that it may be used to launder the proceeds of tax evasion perpetrated abroad exists. There are some alleged cases of tax evasion/offences reported from open-source information. For instance, the Kenya Revenue Authority found in their 2021 audit that a company disguised more than USD 200 million with the help of bankers and other professionals. It is alleged that the Kenyan real estate firm with ties to the Chinese government may have evaded tens of millions of dollars in taxes by making fake loans and "fictional" imports to businesses in Mauritius[19].

Moreover, Mauritius Leaks, an investigation by the International Consortium of Investigative Journalists and 54 journalists from 18 countries, sheds light on how western corporations and African oligarchs can potentially make use of shell companies incorporated in Mauritius by paying tax at a lower tax rate in Mauritius and less tax to African nations where these companies actually do business.[20]

However, it must be noted that there has not been any reported tax evasion in Mauritius following the publication of these two above-noted articles.

International Cooperation

Mutual Legal Assistance

For the period under review, 6 incoming requests were received for MLA which relate to tax crimes and tax evasion as predicate offence. Out of the 6 requests received, 5 requests had an ML component.

Table 7: Mutual Legal Assistance Predicate Offences

Predicate Offence	2018	2019	2020	2021	2022
Tax Crimes and Tax Evasion	1	2	2	1	Nil

Exchange of information under Double Taxation Avoidance Agreements

Mauritius has signed Double Taxation Avoidance Agreements with 46 countries with a view to assisting in the administration of the laws in relation to taxes of every kind and description, and foreign tax, covered under the arrangements. Statistics on the number of exchanges of information under Double Taxation Avoidance Agreements are outlined in Table 8:

Table 8: Number on exchange of information

Fiscal Year	2019	2020	2021	2022
Incoming requests	277	201	205	194
Outgoing requests	4	1	10	6

19 https://www.icij.org/investigations/mauritius-leaks/kenyan-firm-fined-for-elaborate-tax-evasion-scheme-routed-through-mauritius/

20 https://www.icij.org/investigations/mauritius-leaks/treasure-island-leak-reveals-how-mauritius-siphons-tax-from-poor-nations-to-benefit-elites/

Measures Taken

Mauritius has signed the country-by-country Multilateral Competent Authority Agreement and has passed legislation to enable exchange of country-by country reports as from 1 July 2018. Furthermore, in order to combat tax evasion and tax avoidance, the country signed and ratified the Multilateral Convention on Mutual Administrative Assistance in Tax matters in 2015, and has a broad network of Double Taxation Avoidance Agreements and Tax Information Exchange Agreements, providing mechanisms for exchange of information with some 146 jurisdictions. It also concluded an intergovernmental Foreign Account Tax Compliance Act (FATCA) agreement with USA in 2012. Mauritius has been assigned an overall rating of "Compliant" by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes in its last review[21]. The country also joined the initiative on automatic sharing of Beneficial Ownership information launched by the UK, France, Germany, Italy, and Spain.

In its 2022 peer review report of the Action 5 transparency framework, the Forum on Harmful Tax Practices noted that Mauritius met all aspects of the Terms of Reference for the calendar year 2021, and no recommendations were made.

The country has further undertaken other measures as follows:

(i) In the Income Tax Act, provisions were made, allowing the MRA to aid other tax authorities in the collection of taxes such as:

- As of 1 January 2019, the core income generating activities of the global company should be in or from Mauritius to be tax resident in Mauritius. It is worth noting that a non-resident for tax purposes in Mauritius will be taxed on Mauritius-source income only.
- Mauritius recently adhered to the OECD Inclusive Framework, namely Pillar Two, which introduced a global minimum effective corporate tax rate of 15% for multinational groups on income arising in low-tax jurisdictions and forcing the multinational group to declare profits and pay more tax in the countries where they carry out business.

(ii) Mauritius joined the Inclusive Framework to implement the minimum standards under the BEPS project in November 2017. Mauritius has thus signed the Multilateral Convention to implement tax treaty related measures to prevent BEPS. 41 of our 43 treaties were listed as Covered Tax Agreements and these treaties as amended would include the minimum standards under the Multilateral Instrument, with the 'Principal Purpose Test' as the main anti-abuse provision;

[21] Ratings based on Second round of reviews

(iii) Mauritius joined the Yaoundé Declaration in May 2018, which is accompanied by a call for action that requests African Heads of State to support the substantial reduction of illicit financial flows through international tax cooperation; and

(iv) The MRA signed an MOU with the South African Revenue Services regarding the avoidance of double taxation and tax evasion.

In light of the above and the exposure of the country as an IFC, the external ML threat associated to tax evasion was rated **Medium-High**.

Direction of Threat

Open-source information and referral from Supervisory Authorities revealed alleged predicate offences which may have been committed in Mauritius but laundered abroad or vice-versa.

Funds wired to other foreign jurisdictions mainly emanated from the inflows received from foreign entities. In order to increase the layering process, the funds were wired in the local bank accounts of GBCs as investments and subsequently transferred to other foreign bank accounts as payment for consultancy fees, loans, or investments. The transactions were suspicious as it defeats the objectives of the Mauritian companies.

Investigations revealed that only a meagre amount of the inflows remained in the local bank account of the companies/suspects which were used for the payment of fees, salaries, and other such expenses. Most of the inflows were wired back to other foreign bank accounts.

In the previous NRA report, the direct and potential High ML threat emanated from the following countries: Madagascar, India, UK, South Africa, Tanzania, and Kenya. A Medium-High ML threat was assigned to Reunion Island, China, Dubai, and France. The illicit drug trafficking was also identified as the major domestic predicate offence generating substantial proceeds which were laundered in other jurisdictions.

However, the trend of the inflows and outflows has changed. The potential **High** ML threat now lies mainly from countries such as Hong Kong, UK, Cyprus, and South Africa. Now, tax evasion and electronic fraud have been identified as the major predicate offence generating substantial proceeds which are laundered in Mauritius and other jurisdictions.

A **Medium-High** ML threat was maintained against Reunion Island, China, Dubai, and France. A **Medium-High** ML threat has also been assigned to Sri Lanka, India, Malaysia, Venezuela, Seychelles, Nigeria, Singapore, Luxembourg, Madagascar, Denmark, Australia, Kenya, Mexico, and Malta.

Sectoral Analysis

The sectoral threat assessment revealed that a **High** ML threat was associated with the following sectors, namely, Banking, OFI (Leasing companies), TCSPs, and Gambling. The ML threat associated with the Dealers in Precious Metals and Stones (DPMS), and Notary Sectors was rated as **Medium-High**, as shown in Table 9:

Table 9: ML Sectoral Threat Ratings

High ML Threat	Medium High ML Threat	Medium ML Threat	Medium Low ML Threat	Low ML Threat
• Banking • Leasing Companies • TCSPs • Gambling	• DPMS Sector • Notary	• Real Estate • Legal Sector • Securities Sector • Cash Dealers • Payment Intermediary Services • Accountancy Sector	• Long-term Insurance • Motor Insurance • NBDTIs • Credit Unions	• General Insurance (except Motor class) • Credit Finance • Treasury Management • Investment Banking • CSPs • PSP

Major Developments from July 2022 to June 2024

At International Level

Key global risks across social, environmental, and technological issues, focusing on emerging threats, are becoming more complex and widespread. Based on international typologies, these threats include cyberattacks, the misuse of artificial intelligence, online child sexual exploitation, trafficking in arts and antiques, and illegal wildlife, amongst others. PF and the misuse of VAs remain ongoing challenges.

- **Online Child Sexual Exploitation:** This crime has been on the rise, particularly affecting the most vulnerable members of society. It is important to monitor financial transactions and behavioural patterns that could signal exploitation, underlining the need for more effective global cooperation to safeguard children.

- **Misuse of Artificial Intelligence:** AI is being exploited to create realistic deepfakes and spread misinformation. Augmented reality and deepfake technology are being used to manipulate information in physical spaces, furthering societal biases. The sophistication of artificial intelligence systems also means that they can be used maliciously in cyberattacks, enabling more effective phishing attempts or bypassing security measures. Suspected use of deepfake media in fraud schemes, targeting FIs and their customers is also on the rise.

- **Virtual Assets**: VAs, including privacy-focused cryptocurrencies and decentralised platforms, have rapidly grown in popularity. While they offer privacy, these tools also complicate efforts to trace financial transactions, making it harder to detect illegal activities like ML, TF and PF.

- **Cyberattacks**: Financial flows linked to ransomware attacks have surged, with related payments in 2020 and 2021 increasing fourfold compared to 2019, largely facilitated

through VAs. Concerns are also rising over the use of VAs for PF, particularly by North Korea, and for TF by groups like Islamic State of Iraq and the Levant (ISIL) and Al Qaeda.

At Domestic Level

The status of Mauritius as an IFC and its openness to trade, investment and business, makes it vulnerable to be misused for ML purposes. Some of the emerging trends noticed at domestic level are electronic fraud, larceny of copper wire and stolen jewellery, human trafficking and land fraud.

- **Electronic Fraud:** There has been an increasing trend in online scams and fraudulent activities since COVID-19. Criminals are increasingly using social media platforms and structured networks to carry out these activities. Investigations revealed that victims provided their account numbers and OTPs to the accused via WhatsApp or SMS, enabling the criminals to debit funds through internet banking. In some cases, victims even sent their debit cards to the perpetrators.

  All of the offenders were found to be foreigners, particularly from Dubai and Bangladesh, who were often the masterminds behind these devious stratagems. They targeted vulnerable groups, especially divorced women or those seeking foreign partners through matrimonial sites. These sites used artificial intelligence to profile potential partners who may be scammers. The scammers subsequently gained access to the victims' bank account details, which they exploited through internet or mobile banking applications to transfer funds. To lure the victims, scammers requested them to make payments through local bank accounts.

  Common scams included romance scams, investment in fraudulent bogus schemes or offering of foreign loans, especially after 2022.

  During the COVID-19 pandemic, a rise in foreign loans without guarantees, where victims were required to pay exorbitant fees, sometimes as high as MUR 400,000 for a loan of MUR 500,000 was observed. Fraudulent investment schemes, particularly those involving cryptocurrency, have also soared.

  Use of international and domestic bank accounts

  Perpetrators employed modus operandi, such as phone calls, informing victims that they had won lottery tickets, followed by requests to share bank details and pay fees to claim the money. Funds were then transferred incrementally to the perpetrators' bank accounts.

  Cardless transactions

  While individual cardless transactions may be minimal and not sufficient in amount for ML prosecution, when combined, they can be significant.

- **Larceny of copper wire and stolen jewellery:** A rising trend in the number of larceny cases in relation to copper wire and stolen jewellery by drug addicts has been noted. While the copper is bought by scrap metal dealers operating around the island who in

turn sell same to licensed traders, the gold ingots are either sold to jewellers at a low cost or exported, often disguised as scrap metals in shipping containers or transporting same through speedboats to Reunion Island, Madagascar, and Pakistan. It was also observed that in some instances, the drug addicts engaged in a form of barter system, trading the stolen jewelleries for drugs from drug peddlers. Once in the hands of drug peddlers, the stolen jewellery is melted down and turned into gold lingots and subsequently declared at the Assay Office to establish ownership and the value.

- **Human Trafficking:** Emerging human trafficking trends relating to sexual exploitation have also been observed. Intelligence revealed that female individuals (mainly from Madagascar and Eastern Europe) were trafficked using social networks and communication applications such as WhatsApp and Telegram.

  All payments, which were either made in cash or through platforms like MoneyGram, were spent largely on the perpetrators' luxury lifestyles. In other instances, it was observed that the proceeds of the exploitation were being laundered through front businesses such as beauty parlours and spas, which secretly function as brothels. The daily proceeds from these escort services were estimated to be around MUR 30,000 - 40,000. It was also noted that those involved in this network are wealthy individuals.

- **Land Fraud:** Land fraud has emerged as another threat. It was observed that perpetrators use forged documents such as affidavits, procurations, powers of attorney, National Identity Cards, fake site/location plans and other relevant papers to sell land fraudulently. It was observed that perpetrators were Mauritians operating as a network and hiring proxies who act as sellers. Unused lands that had been left unoccupied for 4-5 years were particularly targeted.

National ML Vulnerability

National ML vulnerability was determined at both the level of the national ability of the country to combat ML and the overall sectoral ML vulnerability. The vulnerability assessment identified areas in Mauritius at risk of being exploited for ML activities. Several factors were taken into consideration, with some factors having a direct impact, while others were more indirect. By understanding these vulnerabilities, Mauritius is able to prioritise resources and strengthen measures where they are most needed, allowing for more targeted strategies to mitigate ML risks effectively.

The national ML vulnerability of Mauritius was rated **Medium-High**. This rating was informed by a combination of the national ML combatting ability which was rated **Medium,** and the overall sectoral ML vulnerability which was rated **High**.

It must be highlighted that since the NRA (2019) which outlined gaps in its AML framework, significant strides have been made to strengthen the system, resulting in Mauritius achieving technical compliance with all 40 FATF Recommendations. Ongoing initiatives aim to further enhance the capabilities and resources of investigative bodies, ensuring they are well-equipped to handle sophisticated financial crimes. Establishing the FCD of the Supreme Court and the Intermediate Court has significantly improved the timeliness of case processing.

As previously outlined, there also has been the introduction of the FCC Act establishing the FCC on 29 March 2024. Furthermore, efforts to enhance interagency and international cooperation are continuous, demonstrating the commitment to maintain robust oversight and enforcement to protect the country's financial borders.

National ML Combatting Ability

Mauritius, in addition to having a robust AML Policy and Strategy, has comprehensively defined ML offences in its legislation as a separate or ancillary offence to a predicate crime. With the introduction of the FCC Act in March 2024, ML is now governed by section 36 of the FCC Act, superseding the previous provisions under section 3 of the FIAMLA.

Furthermore, ML sanctions under the FCC Act and Dangerous Drugs Act are also enhanced by provisions of the Criminal Code which criminalises various forms of participation in crime. For example, persons who conspire to launder money or who aid, abet, facilitate, or counsel money launderers are considered as their accomplices and are punishable as if they were the money launderer under S37 of the Criminal Code and S45 of the Interpretation and General Clauses Act.

Section 39 of the Dangerous Drugs Act also provides that every person who obtains any goods, resources or rights derived from any offence under the Act, shall commit an offence. A person may be convicted for an offence under section 39, notwithstanding the absence of a conviction in respect of the predicate offence which generated the goods, resources or rights thereto alleged to have been laundered.

The NRA (2019) highlighted the absence of a legal definition for fraud under Mauritian law. Although no specific legislation defining fraud was enacted between 2019 and March 2024, various offences under Mauritian law effectively addressed fraudulent behaviour, including: Swindling under section 330(1) of the Criminal Code; embezzlement under section 333(1) of the Criminal Code; and Corporate Fraudulent Activities under the Companies Act 2001.

However, the FCC Act now criminalises a range of fraud offences such as fraud by false representation, fraud by failing to disclose information or fraud by abuse of position. This broader scope of predicate offences now enables Mauritius to more effectively combat ML. These developments highlight its continued efforts to improve its AML measures and reinforce legal mechanisms to tackle illicit financial activities.

6. NATIONAL TERRORIST FINANCING RISKS

SUMMARY OF FINDINGS:

The overall TF Risk was assessed **Medium-Low** derived from a combination of TF threat and TF Vulnerability both rated **Medium-Low**.

Despite the fact that there were no active terrorist organisations or individuals identified in Mauritius, the authorities remained vigilant, monitoring for any signs of TF or terrorism activities, with existing legislation allowing for preventive action against suspected cases.

The authorities were aware that, as an IFC, Mauritius could be vulnerable to TF abuse and therefore remained vigilant in this respect.

National TF Threat

The overall TF threat was rated **Medium-Low**.

There is no known-terrorist organisation or individual physically or actively operating within the Mauritian jurisdiction. As of the date of this report, no individual in Mauritius has been prosecuted or convicted for terrorism activities, nor has Mauritius designated any individual or entity as a 'designated party' under the UNSA.

Despite the absence of any reported terrorist attack and terrorist organisations/groups/individuals in Mauritius, the country was to some extent exposed to TF. There were indications that some individuals were influenced by extremist ideologies and propaganda, and the number has slightly increased in the past years.

Two distinct modes of TF activities have been observed in the last few years, namely (i) the cross-border movement of funds by suspected Foreign Terrorist Financiers to a Mauritian citizen embracing ISIS ideologies; and (ii) the raising and outward movement of funds to support Foreign Terrorist Fighters through locals as well as foreign intermediaries which have been identified as terrorist financiers.

Domestically, the funds raised and channelled to Foreign Terrorist Fighters were from legitimate sources, mainly through donations, and other means, such as salary and pension. Intelligence tended to suggest that social media could be exploited as a vehicle to raise funds which could also be used for terrorism activities.

Foreign nationals having suspected links with terrorist organisations/groups could be seeking opportunities to channel funds through companies in Mauritius. The identified methods used for raising funds are donations and crowdfunding, whereas the channels used for transferring funds are wire transfers and Money or Value Transfer Services (MVTS).

National TF Vulnerability

The level of TF vulnerability was assessed **Medium-Low**.

National TF vulnerability was determined at both the level of the national TF combatting ability of the country, and the overall sectoral TF vulnerability. The vulnerability assessment evaluated the strength of defence mechanisms, including the controls and measures adopted to detect and combat TF. Various factors were considered, some with direct impacts and others more indirect. By understanding vulnerabilities to identified threats, the country can better prioritise resources and enhance measures where they are most needed, allowing for more focused and effective strategies to mitigate TF risks.

Mauritius has a legal framework to combat TF and has acted promptly to implement TFS legislation and complied with the UNSCR relating to the prevention and suppression of terrorism and TF. However, the effectiveness of legislation and procedures established are yet to be determined given that there has not been any prosecution or conviction for the TF offences.

National TF Combatting Ability

The National Combatting Ability against TF was rated **Medium-Low**; as internal TF, incoming TF, outgoing TF, and transiting TF all were rated **Medium-Low**.

Mauritius enacted legislations which effectively criminalise terrorist financing, including the Prevention of Terrorism Act 2002 (POTA), the Convention for the Suppression of the Financing of Terrorism Act 2003 (CSFTA) and UNSA. Regulations have been implemented to supplement these Acts, and Mauritius ratified and acceded to other relevant UN Conventions and Protocols. Mauritius has made legislative amendments under the AML/CFT/CPF (Miscellaneous Provisions) Act of 2019, and the Finance (Miscellaneous Provisions) Acts of 2021 and 2022 to further strengthen the POTA and UNSA. The NRA (2019) identified limitations in the jurisdiction's established CFT framework, which the country has since worked to mitigate.

The initial legislation which criminalises terrorism is the POTA, which was last amended by the Finance (Miscellaneous Provisions) Acts of 2021 and 2022. These amendments criminalise people who collect funds or provide funds to a terrorist or a terrorist organisation, even if the funds have not actually been used for any terrorist act.

Although principally concerned with defining and prohibiting terrorism related offences, the POTA also allows the Court on conviction of POTA offences to order the forfeiture of terrorist funds and property, and material used as instrumentalities of terrorism.

Mauritius criminalises, under section 4 of the CSFTA, instances where any person who, by any means whatsoever, wilfully and unlawfully, directly or indirectly, provides or collects funds with the intention or knowledge that it will be used, or having reasonable grounds to believe that they will be used, in full or in part, to commit in Mauritius or abroad an act of terrorism.

TF offence has been comprehensively defined in Mauritian law. While there is an effective legal framework in place, including the prompt freezing of funds or assets of designated individuals or entities, these laws are yet to be tested. As of the date of this report, there have been no prosecutions or convictions for TF, nor any designated individuals or entities. Continued efforts are crucial to fully addressing the challenges of TF and ensuring effective enforcement.

Sectoral Analysis of ML/TF Risks

The risk assessment revealed a **Medium-High** to **Low** level of ML risk across several sectors. Sectors such as Banking and TCSPs were identified as higher risk, due to their contribution to the economy which is material. Furthermore, the overall assessment of the ML Risk of the Banking and TCSP sectors rated these sectors as **Medium-High** (ranked amongst the 1st and 2nd in importance across the financial sector), having considered the characteristics of the sector including the different services provided (for banking sector) and the composition of the customer-base, as well as assessing the input variables for these sectors**.**

Some activities in the Insurance sector were identified with a lower level of risk, indicating less prevalence of laundering activities compared to other sectors. The assessed market infrastructures, that is, Securities Exchanges, Clearing and Settlement Facilities, and Securities Trading Systems, were also identified as low as they do not handle investors' monies.

Additionally, it is important to note that the FATF, in its Interpretive Notes to Recommendation 10 (INR10)[22], has outlined examples of potentially lower risk situations. These included certain customers, products, services, transactions or delivery channels when assessing the ML and TF risks, provided that they emanated or were situated in countries identified by credible sources - such as mutual evaluation or detailed assessment reports - as having effective AML/CFT systems as well as countries identified by credible sources as having a low level of corruption or other criminal activity:

(a) FI and DNFBPs – where they are subject to requirements to combat ML and TF consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored in accordance with the Recommendations to ensure compliance with those requirements.

(b) Public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.

(c) Public administrations or enterprises.

(d) Life insurance policies where the premium is low (e.g. an annual premium of less than USD/EUR 1,000 or a single premium of less than USD/EUR 2,500).

(e) Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral.

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

(g) Financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

[22] FATF_Recommendations_2012.pdf.coredownload.inline.pdf (fatf-gafi.org)

Sectoral TF Risks

The risk assessment reveals a TF risk of **Medium** for the Banking Sector and a TF Risk of **Medium-Low** for the following sectors: Insurance, TCSPs, Notary, Gambling, Real Estate, DPMS, Cash Dealers, Custodian (Non-CIS), PIS, Credit Finance, Investment Banking and Treasury Management. The Securities Sector, CSPs, Legal Profession (excluding Notary), Accountancy, PSPs, NBDTIs and OFI (CCUs) were rated **Low** for TF.

7. BANKING SECTOR

SUMMARY OF FINDINGS:

As an IFC, Mauritius is significantly exposed to cross-border financial flows, increasing the risks of ML from foreign individuals and entities. The banking sector, due to its central role in economic activity and the broad range of products and services offered, has been assessed as inherently **High** Risk for ML. There are genuine concerns that the jurisdiction may be used as a transit point for illicit funds.

The assessment identified key proceeds-generating crimes in Mauritius, including drug trafficking, fraud, illegal bookmaking, high-value larcenies, tax crimes, and corruption. External threats primarily stemmed from fraud, corruption and tax evasion committed outside Mauritius. Many detected ML cases involved illicit funds moving through the financial sector, either directly by criminals or through professional money launderers. Among domestic predicate offences, drug trafficking, fraud, and high-value larceny were the most prominent at various stages of investigation, prosecution, and conviction.

The ML risks facing Mauritius and its banking sector have become increasingly complex due to technological advancements, the introduction of new financial products, and evolving delivery channels. As a result, the banking sector remains one of the highest-risk sectors for ML in the jurisdiction. Banks manage a large and diverse customer base, including high-risk clients from jurisdictions with elevated ML risks, customers engaged in high-volume cross-border transactions, and those utilising complex financial products and structures. To mitigate ML risks and threats, the BoM has implemented various supervisory measures, including instruction letters, guidelines, risk-based on-site examinations and off-site surveillance, targeted thematic reviews, and awareness-raising outreach sessions.

During the review period, the COVID-19 pandemic and subsequent lockdown led to a surge in electronic fraud and heightened cybersecurity challenges within the banking sector. Additionally, the growing interest in VAs and the sophisticated techniques used by criminals to exploit them for illicit fund transfers have made financial crime detection more challenging, further increasing the sector's vulnerability.

Overview of the Sector

The Banking sector is a predominant pillar of the financial system in Mauritius. As of 30 June 2022, the banking industry comprised 19 licensed banks, 6 of which were domestic-owned, 10 were foreign-owned and 3 were branches of foreign banks. The total asset size aggregated around USD 46.3 billion, representing over 370% of Gross Domestic Product (GDP) and servicing around 2.68 million customers. As of 30 June 2024, the banking industry comprised 20 licensed banks (out of which 1 bank had received a licence but had not started operation), 6 of which were domestic-owned, 11 were foreign-owned, and 3 were branches of foreign banks. The total asset size aggregated around USD 53.4 billion, representing around 350% of GDP and servicing around 2.80 million customers.

As of 30 June 2022, domestic owned banks held 62.2% of the assets, whilst branches of foreign banks and foreign controlled banks accounted for 2.6% and 35.2% of the assets, respectively. Concentration in the banking landscape persisted, with the two largest banks which were domestic-owned accounting for around 46% of total deposits, 51% of total advances, and 47% of total assets.

As of 30 June 2022, deposits held by GBCs accounted for 34.2% of total deposits, whilst deposits held by non-residents and residents represented 22.8% and 43.0%, respectively. Loans and advances to non-residents and residents represented 49.1% and 50.9%, respectively. As of 30 June 2022, the customer base in the banking sector comprised 95% residents (Low risk: 71%; Medium risk: 23%; and High risk: 1%) while non-resident customers represented 5% (Low risk: 2%; Medium risk: 2%; and High risk: 1%) of customer base.

The customer base comprised mostly individuals, representing nearly 93% of total customers, followed by corporates representing 6% of total customers, while the remaining 1% related to NPOs, Trusts and DNFBPs.

Besides the traditional banking products, (i.e., loans and deposits), banks offered a wide range of other products and services to customers, such as trade finance, electronic banking, custodial services, safe deposit box services, wealth management, private banking services, treasury products and specialised finance. Additionally, with the enactment of the VAITOS Act, banks may now onboard clients dealing in VA-related activities or even become a VASP themselves.

ML Risk

The inherent vulnerability of the sector for ML was assessed as **High**. Considering the controls in the sector, the overall vulnerability of the sector for ML was **Medium**. Considering that the ML threat to the sector was **High**, the ML risk that the sector is exposed to was **Medium-High**.

ML Threat

Based on local typologies, the laundering of domestic tainted money was mostly done through cash deposits, followed by several interbank transfers. In some cases, different bank accounts were opened at several banks simultaneously with bank accounts registered in the name of accomplices in order to render detection of suspicious and unlawful activities difficult. For example, it is well-known that drug traffickers use accomplices to deposit drug proceeds in their bank accounts in small denominations pretending that they had allegedly won at races or

in casinos (photocopies of winning racing betting stakes were even produced to support their claim).

The most prevalent predicate offences associated to ML in the Banking Sector were embezzlement/larceny by persons involving receipt of wages, electronic fraud, forgery and drug dealing. Money launderers used retail banking facilities such as cash deposit to launder their proceeds as being their legitimate income derived from their business activities or salaries. Money launderers, mostly drug dealers, also abused cash deposit as a means to obscure their source of funds through a third party or 'Prete Nom.' Another common typology noted was that credit facilities offered to the retail customers were frequently settled in cash over very short intervals of time.

Hence, the level of threat in this sector was rated **High**.

ML Vulnerability

The Banking sector, in general, carried significant inherent ML risks in view of its characteristics such as exposure to international businesses entailing cross-border flows of funds, cash-intensive activities of its customers, broad spectrum of corporate and individual customers and diverse delivery channels.

The ML risks were heightened by the vulnerabilities present in the banks' customer segments such as High Net Worth Individuals (HNWI), corporates with complex structures, GBCs, trusts and PEPs, and the characteristics of its products/services, e.g., retail and corporate deposits, credit, trade finance, private banking, correspondent banking, wire transfers and electronic banking.

However, with the strengthening of financial regulations for countering ML risks, criminals were also seeking sophisticated means to launder money through trade finance, wire transfers, private banking and technology-based products such as electronic banking (including internet banking and cards).

The quality of the AML general controls in banks was rated High mainly based on the strong control environment from the assessment of the comprehensiveness of the AML legal/regulatory framework, the availability and effectiveness of entry controls, the effectiveness of supervision and compliance functions, integrity and AML knowledge of banking staff, and effectiveness of Suspicious Activity Monitoring and Reporting, amongst others, for the sector.

Over recent years, the AML legislative framework has been revamped to further reinforce the sector. Starting in 2020, the BoM reviewed and significantly revised the off-site framework for the supervision of ML risks in the banking sector for the development and implementation of the Risk Based Supervisory Framework which also determined the risk-based onsite examination. Banks have robust AML/CFT systems and controls in place to help them take appropriate measures to manage and mitigate the risks identified for ML and have established a full-fledged compliance function. Training to supervisors and banking staff are ongoing to enhance their AML/CFT understanding.

Product Analysis

ML Vulnerabilities of the main banking products/services, offered by banks in Mauritius, were assessed as follows:

(a) Deposits

Deposit activities comprise the mobilisation of funds from the public and placing them into savings, current, and term deposit accounts. Compared to term deposits which carry lower risks, current and savings accounts are more exposed to ML risks given that they are transactional accounts, which are used for movements of funds though the risks associated with deposits for salaried individuals may be lower.

i) Legal persons – non-domestic and GBCs

The deposit accounts of non-domestic legal persons and GBCs were rated inherently high risk. Such business relationships were mostly non-face-to-face, and, in the case of GBCs, the transactions were conducted through their Management Companies. Amongst other factors, the nature of their business, the country risk, the complex ownership structures, transactions conducted through wire transfers, all combined contribute to the high ML risks. GBCs usually deposit large amount of foreign currencies in the banking system for onward transfer to other jurisdictions, mostly for investment purposes.

Notwithstanding the fact that the level of cash activity for this category was virtually non-existent, it remained vulnerable to ML risk. Money launderers may use front companies engaged in legitimate business to commingle the proceeds of illicit activities with legitimate funds in order to conceal their unlawful activities. Specific thresholds were set on the transaction monitoring system of banks for this product. Processes were established for initiating internal investigations on unusual activity identified and reported by any bank officer. The final ML vulnerability of this product was assessed as **Medium.**

ii) Deposits accounts of Legal persons – Domestic

Second-hand car dealers, betting companies, other cash-intensive businesses, trading companies including those, involved in import/export, etc., may use this product for large volume cash and/or cross-border transactions, hence its vulnerability to high ML risks. Deposits accounts of legal persons included deposits such as savings, current and term deposit accounts, of legal entities, excluding GBCs, which are incorporated in Mauritius. The ML risk was higher for the current and savings accounts of legal persons than the term deposits as they are transactional accounts with higher volume of flows.

The main ML vulnerabilities associated with this product were (i) accepting non-exempt cash deposit in excess of MUR 500,000; (ii) the failure to detect a suspicious transaction in a timely manner; (iii) the risk of receiving fake documents in support of transactions; and (iv) when transactions were not in line with the business profile of the client. It was noted that banks had internal controls to monitor accounts of legal persons, including cash intensive businesses.

Based on the above, a **Medium** ML vulnerability rating was assigned to this product.

iii) Retail Deposits

This product comprised demand, savings, and time deposits of individuals. Retail deposits carry ML risk in as much as they may be used to launder cash. Cash transactions are one feature of the placement phase of ML, whereby illicit proceeds are introduced into the financial system. Typologies indicate that the laundering of domestic money is carried out primarily through low value, high frequency cash deposits and even through mules. Retail deposits of self-employed individuals engaged in cash-intensive businesses also represented an ML risk as this product may be used to commingle illicit and legitimate business funds. Cash transactions were one feature of ML, whereby illicit proceeds were introduced into the financial system. Internal controls for this product included standard Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) depending on the risk profile of clients. For instance, banks set thresholds on their systems to prevent cash transactions in excess of MUR 500,000 and above. The final ML vulnerability associated with this product was assessed as **Medium**.

(b) Trade Finance

Trade Finance may be used as a means to conceal criminal proceeds. Trade Finance was considered as an inherently high-risk product in terms of ML risk since it involved cross-border remittances which may be utilised to transfer illicit funds. This trade-based activity involved multiple parties and could involve collusion for under or over invoicing or fraudulent documentation or phantom/sham trades. In order to mitigate ML risks, AML controls such as appropriate transaction screening and monitoring, transactional limits, verification of conformity of transactions with business activity in terms of size were in place. Based on the above, a **Medium** ML vulnerability rating was assigned to this product.

(c) Private Banking

Private banking business pertains to the business of offering banking and financial services and products to HNWI, including but not limited to an all-inclusive wealth-management relationship. This product was rated inherently high ML risk in view of (i) the profiles of the customers; and (ii) the features such as complex accounts/transactions, high volume deposits, average transaction size, cross border transfers and non-face-to-face customers. Further, this product may be used as a vehicle to obfuscate the proceeds of illicit activities (tax evasion, corruption, fraud etc.)

One major challenge for banks offering this product/service was to ascertain the source of wealth/source of funds for private banking customers, particularly for non-face-to-face customers. Further, the wealth management services offered under the private banking business accentuate the ML risk.

Private banking clients were subjected to EDD and closer monitoring, which included controls at on-boarding and on an ongoing basis with regard to Know Your Customer (KYC) verification/documentation, screening against applicable sanctions listings, and transaction monitoring. Additional controls applied were ongoing, including scrutiny of transactions through AML Solution software, risk-based customer reviews and establishing the source of wealth/funds. Consequently, a **Medium** ML vulnerability rating was assigned with the private banking business.

(d) Wire Transfers

Banks carry out wire transfers, i.e., electronic transfers of funds, both cross-border and domestic, via the SWIFT network. Wire transfers can be used for placement of unlawful proceeds into the financial system and consequently, this payment channel carries high ML risk and even the potential risk of being used by terrorists. Given the large volumes of funds involved in cross-border fund flows, illicit funds can readily be concealed in such transactions.

Most banks executed wire transfers for their account holders only. In such cases, the customers were subjected to the CDD process before execution of the transactions. Banks applied additional internal controls for transactions involving high risk countries. In view of the above, a **Medium** ML vulnerability rating was assigned to this product.

(e) Credit products for retail customers

Banks, prior to granting loans, make an in-depth assessment of the customer's repayment capacity and source of funds. The risk for ML could potentially be high in the event where the payment for loan instalments was made in cash. A **Low** rating for-ML vulnerability was assigned to this product.

(f) Credit products for small and medium size businesses

Credit to small and medium size businesses represented a small proportion of the overall loans and advances portfolio for the banking sector. Similar to above, banks, prior to granting loans, make an in-depth assessment of the customer's repayment capacity and source of funds. A **Low** ML vulnerability rating was assigned to this product.

(g) Credit products for large businesses

Credit products for large businesses included giving credit products to large corporates such as credit cards, letters of credit, and overdraft facilities. Also, banks assessed the credit worthiness of the large businesses by using, amongst others, credit information from the Mauritius Credit Information Bureau.

There may be cases where proceeds from illicit activities were used to repay loans, but it was noted that banks carried out due diligence prior to offering this product to large businesses. Therefore, a **Medium-Low** ML vulnerability rating was assigned to this product.

(h) Treasury Products

Treasury products included foreign exchange transactions, currency options, dual currency deposits, interest rate futures and interest rate swaps. All these products were offered to customers, whose KYC profile was assessed and were carried out from the accounts of established customers except for foreign exchange transactions which were carried out over the counter with walk-in customers, for whom due diligence was conducted accordingly.

Therefore, a **Medium** ML vulnerability rating was assigned to this product.

(i) Electronic Banking –Mobile banking

Mobile banking, including mobile payment services, as well as instant payment services, provided by banks required the approval of the BoM. The number of transactions effected through mobile banking had increased considerably in recent years. This may be attributed to the Covid-19 pandemic, during which merchants and customers alike were encouraged to make use of electronic banking for payment purposes. Transaction thresholds and thorough transaction monitoring as well as sanctions screening were carried out on these products. Additional controls, such as links to customers' bank accounts for funding the wallet, limit the risk of this product being abused for ML. All transactions are conducted domestically. A **Low** ML vulnerability rating was therefore assigned.

(j) VAs and VASPs

The VA eco system was rated **Very High** as per the ML/TF Risk Assessment Report of VA and VASPs. It was noted that banks had not yet introduced specific controls and appropriate transactions monitoring tools. But some banks were aware of those VA related transactions occurring through the use of debit and credit cards by customers. Thus, a **High** ML Vulnerability rating was assigned to VAs and VASPs.

Other products/services offered by the Banking sector which have ML Vulnerabilities are:

(i) Safe deposit box services

Only a few banks offered this service. As part of their terms and conditions for the operation of safe deposit boxes, banks specify the prohibited goods that should not be kept therein. However, as there is no visibility on the contents of the boxes, this service is exposed to ML risks.

(ii)Money or Value Transfer Services (MVTS)

MVTS are used to a great extent for migrant workers' remittances and are subject to limits per transaction. There are inherent high ML risks in this product which is, at times, used for group and linked transactions and may be directed to jurisdictions which do not have equivalent AML standards as Mauritius. There are currently very few banks providing these services. However, banks have robust transaction monitoring systems and implement adequate AML controls.

(iii) Prepaid Cards

Many banks had discontinued the offering of prepaid cards to customers. Only a few banks were offering prepaid cards, specifically for overseas travel, online purchases, and educational purposes, provided that the prepaid cards (i) are issued to customers of the bank only, subject to the EDD requirements and taking into account the customer's profile; (ii) have an expiry date of less than one year, a reloading limit, and the name of the cardholder embossed on it; (iii) are used for low-value transactions; and (iv) are restricted to transfers from the bank account held by the customer at the same bank only.

Conclusion

Given that the ML threat for the banking sector was rated **High,** and that the overall vulnerability of the sector to ML risk was rated **Medium**, the ML risk was **Medium-High**.

TF Risk

The inherent vulnerability of the sector for TF was assessed as **Medium-Low**. Considering the controls in the sector, the overall TF vulnerability of the sector was **Medium-Low**. Considering that the TF threat to the sector was **Medium**, the TF risk that the sector was exposed to was **Medium**.

Global typologies tend to indicate that TF through the banking sector is often small-scale and indistinguishable from the multitude of legitimate financial transactions undertaken each day (Vidino et al, 2020[23]). Some cases involved structured deposits of cash into bank accounts followed by international funds transfers out of the jurisdictions. While individual transactions may be small, these can cumulate into substantial amount of funds over time. More complex methods using business accounts as fronts for sending funds offshore through the banking sector could also be potentially explored by terrorists/terrorist financiers. Moreover, the growth and integration of financial technology presents these criminals with new intermediaries and methods to abuse the sector as means for concealing criminal activity, thereby posing a terrorism financing risks (HMT, 2020).

TF Threat

There is a potential risk that banks in the jurisdiction may be used as a conduit for TF through cross-border transactions. TF threat may also occur through the transfer of small value high frequency transactions, as well as some products/services offered by banks such as wire transfers, MVTS, and prepaid cards may be at risk of being abused by criminals and/or radicalized individuals for TF purposes. Thus, the TF threat was rated **Medium** based on the assessment of factors such as the TF threat implied by typologies, demographic and geographic factors as well as the National TF threat rating to which the sector is exposed.

For the period under review, there were no cases or intelligence disclosing the use of hawala system for financing terrorism domestically or abroad. However, the NRA (2019) had identified hawala as a potential TF threat. Given its underground nature, the extent to which hawalas prevail in Mauritius remained obscure. Moreover, since Mauritius has a multi-ethnic community and a rising number of foreigners from high-risk jurisdictions, coupled with the fact that there was no visibility on the underground activities of hawalas for TF purposes, the TF threat associated with the informal sector was, thus considered to be **Medium-Low**.

[23] VIDINO, L., LEWIS, J. & MINES, A. 2020. *Dollars for Daesh: Analyzing the Finances of American ISIS Supporters*. NCITE. [Online]
Available at:
https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Dollars%20for%20Daesh%20final%20report.pdf

TF Vulnerability

Similar to the robust systems and controls which banks have in place for ML risk, they have developed same for the mitigation of TF risk. Most AML/CFT software used in the sector cater for both ML and TF risks which, in turn helps banks to take appropriate measures to manage and mitigate the risks identified. Further, banks have written policy and procedure as well as procedure manuals and circular notes which are available to staff regarding the implementation of TFS requirements to effectively comply with the obligations under the Sanctions Act and the Guidelines. Banks also have in place transaction monitoring system to monitor and mitigate TF risks.

Other specific internal controls implemented for TFS requirements at the level of banks include appropriate screening tools which are embedded in their AML/CFT software. These tools are used to screen prospective clients, existing clients and their related parties, including directors and BO, at time of onboarding and on an ongoing basis, including during file review or trigger event.

Details of incoming and outgoing cross border and domestic transactions such as name of remitter, name of beneficiary, country of remitter, country of beneficiary amongst others are screened through SWIFT sanction screening. As and when the UNSC Consolidated List is updated/changed and circulated by the BoM, verifications are immediately carried out by banks against their customer database and the supervisors are informed within 24 hours.

Furthermore, in so far as sanctions risks exposure is concerned, the domestic Mauritius Central Automated Switch (MauCAS) instant payment systems , owned and operated by the BoM, generally pose a lower risk of sanctions exposure on account of the fact that participants are primarily domestic banks which are subject to stringent regulatory requirements and supervisory examinations by the BoM. MauCAS instant payment systems participants are already performing risk-based due diligence on their customers at onboarding and at regular intervals, thereafter, including screening their customers to identify a potential sanctions nexus. Accordingly, domestic instant payment transactions generally pose a lower sanctions risk.

Banks have established robust systems and controls to address both ML and TF risks, as detailed in the ML assessment report. These measures have been further strengthened by the new provision under section 53A of the Banking Act, which mandates banks to identify and assess potential ML and TF risks associated with the introduction of new products, business practices, and technologies, and to implement appropriate measures to manage and mitigate these risks. Further, as part of their TFS obligations banks carry out customer/related party screening and transactions screening.

The quality of general CFT controls was assessed as **Medium-High** mainly based on the strong control environment from the assessment of the comprehensiveness of the CFT legal/regulatory framework, the effectiveness of supervision and compliance functions, effectiveness of TFS implementation as well as the availability and effectiveness of entry controls, amongst others, for the sector.

Conclusion

The TF threat to the sector was assessed as **Medium** while the vulnerability of the sector to TF was rated **Medium-Low,** resulting in a TF Risk rating that the sector was exposed to as **Medium**.

8. INSURANCE SECTOR

SUMMARY OF FINDINGS:

The assessment of ML risks in the insurance sector revealed varying levels of exposure across different insurance products.

Linked long-term insurance was rated **Medium** for ML risk, primarily due to its investment flexibility, liquidity, and capacity to process large fund volumes. Other long-term insurance products were rated **Medium-Low.**

In terms of ML risks, for general insurance, motor insurance was found to be **Medium**, primarily due to fraudulent claims to launder money. Other general insurance products were rated **Low** or **Medium-Low**, given their limited potential for ML exploitation.

The ML threat in the insurance sector was found to be **Medium-Low** for long-term insurance, due to its potential misuse in crimes such as drug trafficking, swindling, and embezzlement. The ML threat for general insurance was rated **Low** except for motor insurance which was rated **Medium-Low.**

The sector's overall ML vulnerability was assessed as **Medium**.

Regarding TF, the overall TF risk for the insurance sector was rated **Medium-Low**. Although no domestic TF cases were reported during the assessment period, international typologies indicated that terrorists may exploit insurance products through fraudulent claims, early policy cancellations, and the misuse of financial resources. The TF threat was particularly associated with deceptive compensation claims and the use of prepaid life insurance policies to fund terrorism-related activities; the TF threat was thus rated as **Low**.

Overview of the Sector

As a well-regulated and evolving industry, the insurance sector has grown in sophistication and diversity, offering a wide range of products and services, from life and non-life insurance to reinsurance and captive insurance.

The insurance sector comprises long-term and general insurance companies as well as intermediaries such as brokers. Long-term insurance is segmented into Linked Long-Term Insurance (LLTI), Life Insurance Plans with a Cash Value and Investment/Savings component, Pure Protection Life Insurance Plans, Other Life Insurance Plans, and Annuities and Pensions.

The General Insurance is made up of Motor, Accident & Health, Property, Miscellaneous, Liability, Transportation, Engineering, and Guarantee classes.

The contribution of the insurance, reinsurance and pensions sector to GDP amounted to 1.9% in 2023 with an annual growth rate of 4.8%. In 2022, gross premiums for long-term insurance reached USD 282 million, while gross premiums for motor insurance amounted to USD 98 million and non-motor business totalled USD 217 million. As of 30 June 2024, the insurance sector comprised 1,144 entities/individuals, including insurance agents and salespersons. 1,088 of those entities pertain to the domestic sector, representing 95% of the total insurance sector.

For the purpose of the assessment, the population consisted of Long-term insurers, General insurers, External insurers, Professional reinsurers, Captive insurers, Insurance Managers, Captive Insurance Agents, and Insurance Brokers, totalling 122 licensees operating in the domestic and global business sectors as of June 2022.

ML Risk

The ML Risk of long-term insurance products were rated as follows, as shown in Table 10:

Table 10: Long-Term Insurance ML Risk

Long-Term Insurance	
Product	**ML Risk**
Linked Long-Term Insurance (LLTI)	Medium
Life Insurance plans with Cash Value and Investment/Savings component	Medium-Low
Pure Protection Life Insurance Plans	
Other Life Insurance Plans	
Annuities and Pensions	

Linked Long-Term Insurance Class

All long-term insurance products were assessed with a **Medium** final ML vulnerability rating. After applying the threat score of **Medium-Low**, the final vulnerability score, and importance (market share) using the World Bank Tool, the ML risk for LLTI remained at **Medium**, while other long-term insurance products shifted to **Medium-Low**. LLTI as having the highest level of cash activity among long-term products.

General Insurance Class

The ML Risks of general insurance products was rated as shown in Table 11 below:

Table 11: General Insurance Risks

General Insurance	
Product	**ML Risk**
Motor	Medium
Miscellaneous	Low
Transportation	
Guarantee	
Engineering	
Property	Medium-Low
Liability	
Accident & Health	

Motor insurance class

After the application of the final ML vulnerability score of **Medium-Low**, the threat score of **Medium-Low** and importance (market share) using the World Bank tool, the ML risk for motor insurance was assessed to be **Medium**. The ML threat associated to general insurance in Mauritius was assigned **Low** because such products offer limited scope of use to launder money, except for the motor insurance class which was rated **Medium-Low** due to the existence of local predicate offence where one individual was found to purposely cause road accidents and damage vehicles to benefit from insurance claims. The case revealed sufficient elements for a ML case and forgery as predicate offence against the suspect and the case is currently undergoing trial before the FCD.

ML Threat

Two local typologies were reported for ML investigation, prosecution or conviction based on forgery case against products falling under the insurance sector.

Long-Term Insurance

The ML threat associated with long-term insurance was rated **Medium-Low** to acknowledge the observed predicate offence associated with the sector namely drug trafficking, swindling and embezzlement, international typologies, and the potential for criminal exploitation. This rating allowed for the implementation of proportionate risk management measures while keeping a watchful eye on any emerging threats.

General Insurance

The ML threat associated with General Insurance was **Low** because these products offered limited scope of use to launder money except for Motor Insurance class which was rated as **Medium-Low**. However, given that perpetrators may defraud insurance companies, the proceeds of which may be used for ML, the threat associated with this sector exists.

ML Vulnerability

The final ML vulnerability level of the insurance sector was rated **Medium**.

Product Analysis

Long-Term Insurance

Long-term or life insurance is a type of insurance policy that provides financial protection to the beneficiaries of the insured in the event of the insured's death or, in some cases, critical illness or disability. It is primarily designed to ensure financial security for dependents or cover long-term financial commitments. According to the World Bank Tool, long-term insurance comprises the following classes:

(a) Linked Long-Term Insurance

LLTI was assigned a **Medium-High** inherent vulnerability rating. The vulnerability stemmed from LLTI's investment flexibility, liquidity, and capacity to handle large fund volumes. LLTI holds a substantial market share compared to other long-term insurance products. LLTI has significant level single premium policies and other class of long-term insurance products in comparison to regular premium policies. LLTI also had a higher cash usage compared to other products. A local typology involving a single life policy highlighted a case where an insurance employee conspired to launder from a deceased policyholder's insurance policy using forged documents for payout.

(b) Life Insurance Plans with Cash Value and Investment/Saving

Life insurance plans with a cash value and investment or savings component are policies designed to combine protection with long-term wealth creation. These plans offer a death benefit alongside a savings or investment element, which grows over time and can be accessed during the policyholder's lifetime. Life insurance plans with a cash value and investment/savings component serve as both a protection tool and a financial planning instrument for the long term. It includes some level of single premium paying policies, term assurance, endowment policies. This product was rated as **Medium-Low** given its low size, client base, low use of agents and its availability of cross-border use for inherent vulnerability.

(c) Annuities and Pensions

Annuities and Pensions are contracts involving liabilities related to human life or annuities, excluding health and accident insurance. Policies under Annuities and Pensions are paid mostly with regular premium. Annuities and Pensions had a **Medium-Low** inherent vulnerability rating, with regular premium. Annuities and Pensions had a **Medium-Low** inherent vulnerability rating, with a minimal market share, low use of agents, and low cash

activity. Investment-type policies are prominently available, and the existence of ML typologies and evidence of fraud or tax evasion risks adds to its inherent vulnerabilities.

(d) Pure Protection Life Insurance Plan

A Pure Protection Life Insurance Plan is a life cover designed to offer financial protection to the insured person's family in the event of the insured's death. Policies under this plan were mostly regular payment of premium. The inherent vulnerability of this product was rated as **Medium-Low** given its low market share. The use of agents and the level of cash activity in relation to this product was found to be moderate. The ML typologies on the abuse of the product and its use in insurance fraud or tax evasion schemes existed. The availability of cross border use was moderate while the anonymous use of this product was not available.

(e) Other Life Plans

This product was assigned a **Medium-Low** rating driven by its moderate use of agents. In addition to this, the client base and level of cash activity were noted to be fairly low. The market share was low while this product was not known to have anonymous use. ML typologies related to the misuse of this product in insurance fraud or tax evasion schemes. While investment-type policies were available, their presence was limited, as other life plans pertain to long-term insurance business, thereby, contributing to the overall level of ML vulnerability.

General Insurance

General insurance refers to non-life insurance policies that provide financial protection against risks such as property damage, accidents, health issues, or liability claims. General insurance covers tangible assets and liabilities, offering compensation for specific financial losses. General insurance comprises the following classes of insurance business:

(a) Motor Insurance

Motor insurance provides financial protection against losses or damages involving motor vehicles. Motor insurance class had an inherent vulnerability risk rating of **Medium** due to its substantial market share, use of cash transactions, and existence of local predicate offence. Premium payments were primarily made via bank transfer followed by cheque and cash, with the use of cash transactions being notably higher than other insurance segments. A domestic typology involving staged accidents and fraudulent claims was also reported.

(b) Property

Property insurance provides benefits for risks related to the use, ownership, loss, or damage of property. Property insurance had a **Medium** inherent vulnerability, driven by its moderate market share, use of agents, client base, and cash activity. ML typologies and evidence of its use in fraud or tax evasion schemes further contributed to its risk level, though investment-type policies are not applicable.

(c) Engineering

Engineering insurance provides coverage with risks associated with machinery, equipment, construction, or machinery breakdowns. Engineering insurance exhibited a **Medium-Low** inherent vulnerability. It had a low market share and there was no evidence of ML typologies or use in fraud or tax evasion schemes. However, its use of agents and client base moderately elevated its ML vulnerability.

(d) Liability

Liability insurance provides protection against claims resulting from injuries and damage to other people or property. This product had a **Medium-Low** inherent vulnerability as ML typologies on the abuse of such product and its use in insurance fraud or tax evasion schemes did not exist. Furthermore, the level of cash activity and availability of cross-border use associated with this product were found to be less likely to increase its vulnerability.

(e) Transportation

Transportation insurance is a policy that provides coverage for the insured's property while it is in transit from one location to another, using any necessary mode of transport. A **Medium-Low** inherent vulnerability was assigned to this product as the market share and availability of cross-border use were found to be minimal. This was followed by moderate use of agents, client base and level of cash activity. However, the ML typologies on the abuse of the product and its use in insurance fraud or tax evasion schemes existed.

(f) Guarantee

Guarantee insurance means a contract in terms of which a person, other than a bank, in return for a premium, undertakes to provide policy benefits where an event, contemplated in the policy as a risk relating to the failure of a person to discharge an obligation, occurs. This product was assigned a **Medium-Low** rating due to the fact that the use of agents, client base and availability of cross-border use were found to be at a moderate level. The level of cash activity was found to be low while the market share was minimal. This product did not exhibit anonymous use.

(g) Miscellaneous

Miscellaneous insurance policy refers to a broad category of insurance policies that cover a wide range of risks not specifically addressed by other specialized types of insurance. A **Medium-Low** inherent vulnerability was assigned to this product as the market share and availability of cross-border use was low. This was followed by moderate use of agents, client base and level of cash activity. In addition, the anonymous use of this product was not available.

The insurance sector benefits from the robust AML legal framework, supported by the FSC's risk-based supervision framework, which assesses compliance of FIs under its purview and mitigates sectoral risks.

The FSC's AML/CFT Risk-Based Supervision further enables FSC to maintain an up-to-date understanding of the ML/TF risks of the FIs through:

(a) Offsite monitoring;
(b) Onsite inspections; and
(c) Follow-up.

Based on onsite inspections conducted, it was observed that insurance companies improved their compliance with respect to AML obligations as they have implemented, amongst others:

(i) AML systems to enable identification of high-risk transactions (PEPs, clients from non-equivalent jurisdictions, clients on the watch list etc.), which enables the companies to take appropriate measures to minimise the risks associated with these particular client types; and

(ii) customer acceptance policies and procedures for risk profiling of clients and conduct of periodic reviews of high-risk clients.

In addition, it has been observed that most insurers:

(i) reported screening their clients and transactions against Sanctions Lists and adverse media/negative news; and

(ii) screened customers and connected parties to determine whether they are PEPs or controlled by PEPs and if they are listed on UN Sanction List.

Conclusion

Considering the ML vulnerability and ML threat for both general and long-term insurance, the ML risk of the insurance sector was **Medium.** Strong regulatory frameworks and supervision mitigated many risks, but certain product types, like LLTI and motor insurance, remained more susceptible to abuse.

TF Risk

The inherent vulnerability of the sector for TF was assessed as **Medium-Low**. Considering the controls, the final TF vulnerability of the sector was determined as **Medium-Low.** Given that the TF threat to the sector was **Low**, the overall TF risk of the sector was assessed as **Medium-Low**.

TF Threat

The Insurance sector is not immune to TF risks. While the sector may not be as directly exposed as other financial industries, certain products and services can still be exploited by terrorists or those seeking to finance terrorism. Terrorists may attempt to file fraudulent insurance claims to generate funds. Examples include early cancellation, using fraudulent or suspicious claims as a means of extracting funds from insurance companies, which can then be used for financing terrorism.

For the Insurance sector, no domestic TF case was reported for the period under assessment; accordingly international typologies for TF for the Insurance sector were considered. International typologies show that the TF Threat associated with the insurance sector arises from the use or misuse of the sector by terrorists to hide their financial activities, the use of deception to fraudulently obtain damage compensation and the acquisition, and usage of

financial resources stemming from a cancelled life insurance policy paid beforehand to finance terrorism activities, including the travel of Foreign Terrorist Fighters to or from conflict zones. The TF threat is thus rated **Low**.

TF Vulnerability

Taking assets as a basis of measure, general insurance business is more significant than long-term insurance. Likewise, in terms of assets, the domestic market is more substantial than the global business segment. As such, gross premiums were used as the basis to determine the significance of each class of insurance. A final rating of **Medium-Low** was assigned to insurance sector and its products, owing to the amendments made to the FIAMLA and the introduction of the FIAMLR, which further reinforced the requirement to have appropriate mechanisms to identify and monitor high-risk customers. It must be highlighted that the risk associated to intermediaries was mitigated by the fact that insurers must onboard their respective insurance agents under their compliance programme/function by virtue of a letter issued by the FSC.

The TF vulnerability of the Insurance sector was rated **Medium-Low**. This is explained by:

- insurance products with and without investment component which were all rated Medium-Low for TF Risk;
- the level of outward international transactions and operations of business entities was a factor as significant outwards transactions were conducted from within Mauritius;
- a low level of total outward transactions was carried out with high-risk jurisdictions;
- the level of inward international transactions and operations of business entities was identified in the insurance sector, where most of the transactions were carried out from outside of Mauritius;
- moderate level of total inward transactions emanated from high-risk jurisdictions; and
- the level of cash activity ranged from Medium to Medium-Low across all classes of insurance business.

Insurance entities are required to comply with the full range of AML obligations. This includes, amongst others, requirements to have in place a compliance framework, appoint compliance officers and Money Laundering Reporting Officers (MLROs), conduct CDD and EDD for high-risk clients/situations, establish source of wealth and source of funds, sanctions screening and report suspicious transactions. These FIs are subject to the FSC's on-site and off-site supervision, in line with its risk-based approach to supervision.

The Insurance sector has in place CFT measures, including internal controls and procedures in their compliance programmes to comply with TFS obligations. There are areas of improvement in understanding TF risks and limitations in typologies, which may impact the overall effectiveness of the measures implemented.

It was indeed observed that majority of the insurance entities have adequate policies and procedures, systems and controls in place to meet TFS requirements, namely:

(a) screening systems that had been effectively designed and tested;

(b) sufficient and quality data about the customer to identify whether the customer was sanctioned; and
(c) documented sanctions screening searches.

Conclusion

Considering the TF vulnerability which was **Medium-Low,** and TF threat, which was **Low**, the TF risk of the Insurance sector was **Medium-Low**.

9. SECURITIES SECTOR

SUMMARY OF FINDINGS:

The Securities sector was assessed as having a **Medium** ML risk, primarily due to the international nature of transactions, complex legal structures, and high-value assets. The most vulnerable entities were Collective Investment Schemes (CIS), Closed-End Funds (CEF), and Investment Advisers (Unrestricted) due to their global client base, portfolio management activities, and sophisticated financial products. Securities Exchanges and Clearing and Settlement Facilities posed **Low** ML risk, as they do not handle investor funds and maintain stringent disclosure and audit requirements. The highest ML vulnerability was associated with structured products, while traditional securities like shares and bonds were determined as lower risk.

The main ML risk was linked to the source of funds rather than specific products, with key risk drivers being the type of services offered, client profiles, and level of controls applied. Despite these risks, comprehensive AML controls helped to mitigate risks relating to ML vulnerabilities, resulting in a **Medium** residual ML risk rating. The ML threat was also rated **Medium**, leading to an overall **Medium** ML risk for the sector.

The TF risk was assessed as **Low**, with no reported cases, Suspicious Transaction Reports (STRs), or identified typologies in Mauritius. The use of GBCs contributed to potential TF risks, but stringent CFT measures made the sector unattractive to terrorist groups. Market infrastructures had Low TF risks due to strict controls and audit trails. However, there is a need for enhanced knowledge of TF risks and typologies among supervisors and FIs to further strengthen CFT measures in the sector.

[24] *Source: Statistics Mauritius*

Overview of the Sector

The Securities sector is one of the key pillars of the financial services sector in the Mauritian economy. This sector is included as a sub-sector in the Monetary Intermediation and contributed to 7.0% to the GDP of Mauritius in 2024[24]. The Securities sector in Mauritius is composed of the funds industry, market intermediaries and market infrastructures. Entities operating in the Securities sector are licensed under the Securities Act, which is in line with best practices such as IOSCO Objectives and Principles.

The Securities sector comprises both domestic and global business players. For the NRA exercise, the following institution types were assessed:

- Investment Dealers
  - Investment Dealers are categorised as Investment Dealer (Full-Service Dealer including Underwriting), Investment Dealer (Full-Service Dealer excluding Underwriting), Investment Dealer (Discount Broker), and Investment Dealer (Broker). The core activity of Investment Dealers involves the execution of trade orders on behalf of clients, and they do not hold clients' funds. Investment Dealers derive their income primarily from brokerage fees, which depend on the volume of orders executed.
  - Investment Dealer (Discount Broker) are authorised to execute orders for clients without giving advice. Investment Dealer (Broker) are authorised to execute trade orders for clients, manage portfolios of clients and give advice on securities transactions to clients. Investment Dealer (Full-Service Dealer including Underwriting) and Investment Dealer (Full-Service Dealer excluding Underwriting), in addition to executing orders, provide portfolio management services and provide advice on securities transactions to clients which is ancillary to the normal course of their business activities.
- Investment Advisers
  - The core activity of Investment Advisers involves the provision of investment advice to clients. The different categories of Investment Advisers are Investment Adviser (Restricted), Investment Adviser (Unrestricted) and Investment Adviser (Corporate Finance Advisory). In the case of Investment Adviser (Unrestricted) in addition to providing advice to clients, they also manage a portfolio of clients.
- CIS Managers
  - CIS Managers are licensed by the FSC to manage Collective Investment Schemes (CIS) and Closed-End Funds (CEF).
  - The domestic market relates mainly to retail funds, which are generally attractive to the public and retail clients. Funds in the global business sector are mostly Expert Funds or Professional CIS that target expert investors, sophisticated investors, and HNWI.
- Custodians
  - Custodians, which in Mauritius must be a bank or a bank subsidiary, are responsible for the safekeeping of the assets of a CIS or a CEF. The banks are usually providing custodial services to their clients as part of their broader

banking services, and the custody business segment is insignificant when compared to their overall banking activities.

- Market Infrastructures
    - These consist of securities exchanges, clearing and settlement facilities and securities trading systems which provide a platform for trading of securities.

As of 30 June 2024, the sector comprised 2,185 licensees[25] (142 domestic entities and 2,043 GBCs). The securities institution types assessed were all categories of Market Intermediaries consisting of 173 Investment Dealers and 361 Investment Advisers, Market Infrastructures (2 Securities Exchanges, 2 Clearing and Settlement Facilities, and 1 Securities Trading Systems), 396 CIS, 502 CEF, and 11 Custodians[26]. The types of securities that are most traded by investors are shares, bonds, Exchange Traded Funds, Depositary Receipts and structured products. On this basis, only a general product analysis for the domestic market was assessed to determine which products are vulnerable to ML risks.

Over recent years, the legislative framework has been revamped to further reinforce the sector. As from 2020, the FSC reviewed and significantly revised the supervisory framework for the supervision of ML/TF risks for the development and implementation of the Risk Based Supervisory Framework which also determined the risk-based onsite inspections and offsite reviews.

Both domestic and global business entities are required to comply with the full range of AML/CFT obligations. This includes, amongst others, requirements to have in place a compliance framework, appointing compliance officers and MLROs, conducting CDD and EDD for high risk, establish their source of wealth and source of funds, sanctions screening and reporting suspicious transactions. These FIs are subjected to the FSC's on-site and off-site supervision, in line with its risk-based approach to supervision. Given the sector is assessed to pose Medium ML risks, the FSC continues to apply supervisory focus on this sector with greater scrutiny on the higher risk areas in the activities within the sector.

ML Risk

The inherent vulnerability of the sector for ML was assessed as **Medium**. Considering the controls (**Medium-High**) in the sector, the overall ML vulnerability of the sector was **Medium**. Considering that the ML threat to the sector was **Medium**, the ML risk that the sector was exposed to was **Medium**.

ML Threat

During the period under review, the Securities sector was not subject to any enquiry by the LEAs and there was no case under investigation, prosecution or conviction. In addition, there is no local typology for the Securities sector.

However, based on international typologies, the illegal funds laundered through the Securities sector might be generated by illegal activities both from outside and from within the sector.

[25] Source: FSC Statistics.
[26] Source: FSC Statistics.

For illegal funds generated outside the sector, securities transactions were used as a mechanism for concealing or obscuring the source of these funds. In the case of illegal activities carried out within the securities market itself – for example, embezzlement, insider trading, securities fraud, market manipulation, etc. – the illegal funds generated from these activities may further be laundered through the securities transactions or related manipulations.
It was also perceived that the highly international nature of the securities industry meant that criminals could use operations involving multiple jurisdictions to further complicate and thus obscure the various components of a ML scheme.

ML Vulnerability

The inherent risks observed for CIS and CEF are higher as their clients included PEPs, clients from high-risk jurisdictions, institutional investors and HNWI, representing a higher risk to the jurisdiction, hence triggering an enhanced assessment. CIS and CEF usually make use of legal persons and legal arrangements to structure their investments. Given that both investors and investments are based outside Mauritius, non-face-to-face dealings with clients, which is a feature of the global business sector, tends to prevail. However, in this NRA exercise, the inherent vulnerability for CIS and CEF was reduced to **Medium-High** as the data available indicated the risk factors were present but to a lesser extent.

Another institution type in the Securities sector which is most vulnerable to ML risks is Investment Adviser (Unrestricted). This activity involves providing advice under a mandate for clients and the management of portfolios of securities which includes sophisticated and complex products. Investment Advisers managing portfolios of securities, especially under a discretionary mandate, may be more vulnerable to ML risks. This may include complex products depending on risk appetite and clients' investment objectives. As such, the ML inherent vulnerability for this activity was **Medium**. The other categories of investment advisers do not involve the management of portfolios of securities and thus do not deal with clients' funds, resulting in **Low** ML inherent vulnerability.

Investment Dealers are licensed market intermediaries involved in the execution of securities on behalf of clients. Investment Dealers activities are characterised by a large number of domestic and global business retail clients. The use of complex products rather than traditional equity-based products increases the ML risk by making transactions more difficult to red flag and to trace. Moreover, the potential abuse of ML may also be higher when dealing with certain types of clients such as PEPs and clients from high-risk jurisdictions.

Considering the above, the ML inherent vulnerability of Investment Dealer (Discount Broker) and Investment Dealer (Full-service Dealer including Underwriting) have been rated as **Medium-Low**, whilst that of Investment Dealer (Full-Service Dealer excluding Underwriting) and Investment Dealer (Broker) have been rated **Medium.**

The ML vulnerability assessment also demonstrated that Securities Exchanges, Clearing and Settlement Facilities, and Securities Trading Systems provide a platform for trading and settlement of securities, respectively. The ML vulnerability for the assessed market infrastructures were **Low** as they do not handle investors' monies. They provide trading and settlement platforms for members/participants to trade and settle securities on behalf of

investors. In addition, they have a complete audit trail of all transactions executed and settled on their respective systems and have stringent disclosure requirements.

Though there are various areas of vulnerability in the Securities sector, these vulnerabilities are being addressed by FIs in the Securities sector through their AML/CFT compliance programmes. The assessment noted an increase in the compliance culture by FIs because of extensive supervisory engagements by the FSC. However, there are further improvements required in the application of the AML/CFT measures as a low number of internal disclosures and STRs has been noted considering the size of the population of the Securities sector.

Product Analysis

The product that is more vulnerable to ML risks is structured products, and the less risky ones are the traditional ones such as shares and bonds. The main risk associated with securities products in terms of ML is the source of funds used by investors to trade in these products. The product types do not trigger specific risks or increase the risk to ML. The risk is rather driven by the type of service provided, the client profiles, international nature of transactions, and the level of controls applied. Complex legal structures used in the securities sector may render beneficial ownership difficult to trace, hence increasing the vulnerability to ML risks.

Conclusion

Considering the assessment and analysis, the ML threat to the sector was rated **Medium**, the overall ML vulnerability of the sector was **Medium**, hence the ML risk that the Securities sector is exposed to was **Medium**.

TF Risk

The inherent vulnerability of the sector for TF was assessed as **Low**. Considering the controls in the sector, the overall TF vulnerability of the sector was **Low**. Considering that the TF threat to the sector was **Low**, the TF risk that the sector is exposed to was **Low**.

TF Threat

A large portion of the assets under management are sourced from investors outside Mauritius. Hence, they are exposed to cross-border transactions, including those relating to high-risk jurisdictions. TF Threat may be present to the extent of the high-risk jurisdictions. However, no connection to TF was detected and law enforcement authority has not observed the misuse of this sector.

As there was no known TF case emanating from the Securities sector either on the domestic front or in the global business sector, and the fact that there was no terrorist group/organisation in Mauritius, the threat associated with the Securities sector was considered as **Low**.

TF Vulnerability

The majority of players in the Securities sector are GBCs and this feature may be seen as a factor which contributes to the movement of funds and hence poses the main TF risk for the

Securities sector. Even though the Securities sector could be used for moving funds for TF purposes, the existing stringent controls render the sector unattractive to terrorist groups/ organisations.

Most of the transactions in the Securities sector pertain to the global business sector and hence are international in nature. Investment Dealers and Investment Advisers are incorporated and licensed in Mauritius and function as service providers mainly in the global business sector; hence transactions between these service providers and their clients are primarily held in their respective bank accounts in Mauritius. The outward international transactions to higher risk geographical locations for the sector were 0.38% for the period 1 July 2021 to 30 June 2022, and for the same period, the inward international transactions from higher risk geographical locations for the sector were 0.74%. The number of clients from high-risk jurisdictions and clients having business links with high-risk jurisdictions accounted for 7% of the total client base for the Investment Dealers and Investment Advisors of the global business sector. For CIS and CEF, investors from high-risk jurisdictions and investors having business links with high-risk jurisdictions accounted for 8% of the total investor base for the global business sector.

It was observed that 0.17% of the respondents used cash as payment mode. Hence, the level of cash activity for the Securities sector was considered **Low**.

Like for ML vulnerability, the TF vulnerability for the assessed market infrastructures were low as they did not handle investors' monies and they just provided trading and settlement platforms for members/participants to trade and settle securities on behalf of investors.

For the Securities sector, no TF cases were reported for the period under review. No STR was filed for TF purposes with the FIU for the period under review. In the absence of domestic typologies, international typologies for TF for the Securities sector were considered. International typology for the Securities sector indicated that insider trading, market manipulation and securities-related fraud were identified as predicate offences for TF.

In terms of controls, the Securities sector account for CFT measures, including the conduct of sanction screening, in their AML/CFT compliance programmes. Nevertheless, on both the supervisory front and the application of CTF measures by FIs in the Securities sector, there were limitations in terms of knowledge on TF risks and typologies, therefore, impacting to some extent, the reporting of STR for TF and the overall effectiveness of the actions being taken.

Conclusion

Based on the assessment, the TF threat to the Securities sector was rated **Low**, the overall TF vulnerability of the sector was rated **Low**, hence the TF risk that the Securities sector was exposed to was rated **Low**.

10. OTHER FINANCIAL INSTITUTIONS

1. Other Financial Institutions under supervision of the Bank of Mauritius

(1) NBDTIs

SUMMARY OF FINDINGS:

The NBDTI sector, being a sector onboarding primarily domestic/resident customers mainly on a face-to-face basis, was assessed as inherently less vulnerable to ML and TF risks. Considering the strong AML/CFT controls that were in place and the mitigation for both ML and TF risks, the final ML and TF risks of the NBDTI sector were assessed as **Medium-Low** and **Low** respectively.

Overview of the Sector

Six NBDTIs operating as of end-June 2024 were authorised by the BoM to mobilize term deposits from the public. As of end-June 2022, total assets of NBDTIs represented 3.2% of total assets of NBDTIs and banks combined. NBDTIs used their funds to invest mainly in finance leases and grant mortgage loans. Leasing companies are licensed and regulated by the FSC. Findings of the assessment of leasing products have not been covered under this section but were done separately.

NBDTIs are not allowed to hold current accounts, that is transactional accounts for effecting movement of funds and hence they are less exposed to ML risks.

ML Risk

The inherent vulnerability of the sector for ML was assessed as **Medium-Low**. Considering the controls in the sector, the overall ML vulnerability of the sector was **Medium-Low**. Considering that the ML threat to the sector was **Medium-Low**, the ML risk that the sector was exposed to was **Medium-Low**.

ML Threat

In view of negligible cases of ML investigations with respect to term deposits and mortgage loans, the ML threat was rated **Medium-Low**.

ML Vulnerability

The final ML vulnerability of the NBDTI sector, considering the vulnerability of each assessed product and strength of mitigating AML controls was rated **Medium-Low**.

The quality of the general AML controls at NBDTIs was assessed as strong, in view of the fact that they are subject to the same stringent legal and supervisory requirements as banks, and they have in place a full-fledged compliance function with adequate policies and procedures to

mitigate ML risks. They also have strong monitoring systems with on-going training of staff on AML matters. Further, NBDTIs are also subject to the same rigorous entry controls as banks with risk-based supervision being applied to them by BoM. Over the recent years, various improvements were brought to the AML/CFT legislative framework to reinforce the sector. Moreover, the spectrum of products offered was also limited and carried low levels of ML vulnerability.

Product Analysis

(a) Term Deposits

Term deposits were assessed as having **Medium-Low** ML vulnerability because the majority of customers were citizens of Mauritius and were onboarded face-to-face. The level of cash activity was minimal as most term deposits were largely effected through bank transfers. Further, no international transaction was involved.

(b) Savings Deposits and Retirement Savings Schemes

Only 2 of the 6 NBDTIs offered these products which accounted for 5% of the total deposits of NBDTIs sector at end of June 2022. These products were offered largely to retail domestic customers. Cash transactions were not significantly involved with these products. Savings deposits were assessed as having **Medium-Low** ML vulnerability while Retirement Savings Schemes were assessed as **Low** ML vulnerability given that the source of fund could be easily identifiable.

(c) Mortgage Loans

2 of the NBDTIs offered this product which accounted for 32% of total credit granted by NBDTIs. One of the NBDTIs was specialized in the provision of finance for construction and acquisition of houses/apartments and its mortgage credit represented 80% of total credit facilities. Most credit was granted to domestic clients who were onboarded face-to-face. This product was assessed as having **Medium-Low** ML vulnerability.

(d) Other Credit Facilities

Four NBDTIs were offering other credit facilities which were mostly low value transactions. Most of the customers availing of these facilities were categorized as low risk. Cash transactions were not significant. All client relationships were conducted face-to-face. This product was assessed as having **Medium-Low** ML vulnerability.

Conclusion

Taking into consideration that both the ML threat and the ML vulnerability of the NBDTI sector was rated as **Medium-Low**, the final ML risk was rated as **Medium-Low**.

TF Risk

The inherent vulnerability of the sector for TF was assessed as **Low**. Considering the controls in the sector, the overall TF vulnerability of the sector was **Low**. Considering that the TF threat to the sector was **Low**, the TF risk that the sector is exposed to was **Low**.

TF Vulnerability

TF vulnerability of the NBDTI sector was s considered **Low** given the absence of current account deposits (transactional accounts) and cross border flows, transfers into deposit accounts being made predominantly through bank transfers, use of limited products, and majority of customers being resident.

The quality of general CFT controls at NBDTIs was assessed as strong in view of the robustness of their systems for mitigating TF risks. They have in place adequate policies and procedures, screening, and transactions monitoring systems for monitoring and mitigating TF risks. Further, staff are continuously trained on TF requirements.

Conclusion

Considering the TF threat was **Low** and TF vulnerability was **Low**; the TF risk was assessed as **Low**.

(2) Cash Dealers

SUMMARY OF FINDINGS:

The cash intensive nature of the Cash Dealer sector allows large amounts of cash transactions to occur thereby making it easier for individuals involved in ML or TF to use facilitators and intermediaries for converting and moving funds without leaving a clear financial trail. The ML risk of the Cash Dealer sector took into consideration the ML threat of the sector and the final vulnerability of the sector to ML. The ML threat was assessed as **Medium**, due to potential unlicensed money changers being used to exchange Mauritian Rupee into foreign currencies while the final ML vulnerability was assessed as **Medium**, considering the vulnerability of each assessed product and the strength of controls. The final ML risk was therefore assessed as **Medium**.

The TF threat for the Cash Dealer sector was rated as **Medium-Low** considering the number of intelligences received concerning TF with respect to Cash Dealers (during the period under review), the limited number of TF cases under investigations, and cases which led to conviction. The residual TF vulnerability for the Cash Dealer sector was assessed as **Medium-Low** resulting in a **Medium-Low** rating for the sector.

Overview of Sector

Cash Dealers comprised Money Changers and Foreign Exchange Dealers. As of end June 2024, there were 12 Cash Dealers in operation, namely 6 Money Changers and 6 Foreign Exchange Dealers.

Money Changers conducted solely spot buying and selling of foreign currency notes over the counter.

In addition to spot buying and selling of foreign currency notes over the counter, Foreign Exchange Dealers were authorised to also carry out remittance businesses, including MVTS and wire transfers, as well as conducting forward exchange transactions through banks. 5 of the Foreign Exchange Dealers offered MVTS through RIA, Western Union and MoneyGram.

None of the Cash Dealers conducted any transaction in VAs or had VASPs as customers.

ML Risk

The inherent vulnerability of the sector for ML was assessed as **Medium**. Considering the controls in the sector, the overall ML vulnerability of the sector was **Medium**. Considering that the ML threat to the sector was **Medium**, the ML risk that the sector was exposed to was **Medium**.

ML Threat

The money-changing business is cash intensive in nature, and is market characterised by walk-in customers who carry out one-off transactions making it particularly vulnerable at the placement stage of the ML process.

MVTS were largely used by migrant workers to repatriate funds to their home countries.

The ML threat for the Cash Dealer sector was **Medium**, considering the risk of unlicensed operators and the absence of ML investigations.

ML Vulnerability

The final ML vulnerability of Cash Dealers was assessed as **Medium** considering the fact that transactions were conducted face-to-face, were mostly of low value, and cash transactions of more than MUR 500,000 were prohibited. Internal transaction limits which were much lower than MUR 500,000 were also set by the Cash Dealers.

The quality of general AML controls of Cash Dealers was assessed as strong in view of the rigorous licensing requirements as well as the close monitoring and effective supervision particularly over the transactions reported on a daily basis by BoM. All Cash Dealers have in place policies and procedures for mitigating ML risks. It is also mandatory for them to have in place an AML/CFT software for transaction monitoring purposes. Further, compliance functions exercise continuous monitoring over AML matters. Extensive training and outreach programmes were provided to Cash Dealers and their staff to raise awareness on topical issues.

Product Analysis

(a) Over the counter purchase and sale of foreign currency notes

Foreign exchange services were assessed as having **Medium** ML vulnerability because the individual transactions were mostly of low value. Cash transactions of more than MUR 500,000 were prohibited. This environment involved walk-in clients who conducted largely one-off transactions. All transactions were conducted face-to-face, and no agents were used. During the financial year ended 30 June 2022, 38% of the customers were tourists with less than 1% of the customers being rated as high-risk. There was no cross-border exposure.

(b) Remittance business (including spot and forward exchange transactions through wire transfers offered by Foreign Exchange Dealers only)

Remittance business was assessed as having **Medium-Low** ML vulnerability. As of end June 2022, only 2 Foreign Exchange Dealers offered this service to their customers. Most of these transactions were conducted with resident customers and very few of them were classified as high-risk. These transactions were largely carried out through bank transfers. KYC/CDD information/documents of customers as well as information on originators and beneficiaries of funds were mandatory for this product.

(c) Money or Value Transfer Services (offered by Foreign Exchange Dealers only)

MVTS was offered exclusively to individuals, on a face-to-face basis only. Further, there was a daily limit per client/transaction, which ranged from USD 1,700 to USD 7,500. Most of the customers using this product were foreigners/migrant workers and non-residents, some of whom were categorised as high-risk. Although the majority of transactions were conducted in cash, bank transfers could also be used to transfer funds to the Cash Dealers. Cash transaction of more than MUR 500,000 was prohibited. Given the cash intensiveness of the product and the cross-border exposure, MVTS was therefore assessed as having **Medium-High** ML vulnerability.

Conclusion

Given that the ML threat for the Cash Dealer sector was assessed as **Medium**, and the final ML vulnerability for Cash Dealer sector was assessed as **Medium**, the ML risk of the Cash Dealer sector was therefore rated **Medium**.

TF Risk

The inherent TF vulnerability of Foreign Exchange Dealers was assessed as **Medium**, while the TF inherent vulnerability of Money Changers was assessed as **Medium-Low**. Considering the controls in the sector, the overall TF vulnerability of the Cash Dealer sector was rated **Medium-Low**. Considering the TF threat to the sector as **Medium-Low**, the TF risk of that sector was determined as **Medium-Low**.

TF Threat

The cash intensive nature of the Cash Dealers allows large amounts of cash transactions to occur thereby making it easier for individuals involved in TF to use facilitators and intermediaries for converting and moving funds without leaving a clear financial trail. Furthermore, Cash Dealers could be exploited for cross border transfer of terrorist-related funds. Terrorist or terrorist financiers could use Money Changers as well as Foreign Exchange Dealers to commingle legitimate and illicit funds, which could be exchanged for foreign currencies. The foreign currencies obtained could then be transferred to other jurisdictions to support terrorist activities. The TF threat for the Cash Dealer sector was **Medium-Low**, considering the limited intelligence received concerning TF with respect to Cash Dealers, the absence of TF cases under investigation and cases which led to conviction.

TF Vulnerability

Foreign Exchange Dealers were at a higher risk of being involved in TF than Money Changers because they dealt with cross-border transactions, making them more vulnerable to TF activities. The inherent TF vulnerability of Foreign Exchange Dealers was assessed as **Medium**, while the inherent TF vulnerability of Money Changers was assessed as **Medium-Low**.

The quality of CFT controls was assessed as strong largely in view that Cash Dealers have the obligation to screen all customers and transactions prior to processing same. Further, transactions conducted by them were subject to close monitoring by BoM.

Conclusion

Given that the TF threat of Cash Dealers was collectively evaluated as **Medium-Low,** and the TF vulnerability of Cash Dealers was assessed as **Medium-Low** as well, the TF risk of the Cash Dealer sector was assessed as **Medium-Low.**

(1) PSPs

SUMMARY OF FINDINGS:

PSPs is a new sector since the previous NRA exercise. They are entities which provide payment services, other than entities licensed by the FSC to conduct payment intermediary services exclusively outside Mauritius. There are three PSPs operating in Mauritius. The ML risk of the PSPs sector took into consideration the ML threat of the sector and the final vulnerability of the sector to ML. Both the ML threat and the TF threat were assessed as **Low**. The final ML and TF vulnerability was assessed as **Low**, and the final ML and TF risk was accordingly assessed as **Low**.

Overview of the Sector

As per the definition of the National Payment Systems Act, PSPs are entities which provide payment services, other than entities licensed by the FSC to conduct payment intermediary services exclusively outside Mauritius. The PSPs licensed by the BoM since November 2021 provide mobile payment services, card services and e-money services to the public.

As of end June 2024, three PSPs were licensed by the BoM to offer payment services to the public.

Two of the PSPs are subsidiaries of the two largest Telecom Network (telco) Operators in Mauritius, one of which has been incorporated specifically for the purpose of offering payment services in Mauritius. One of the telco PSPs, which is also the largest telco company in Mauritius, provides payment services in the form of e-money issuance and mobile payment services to the public. The second telco PSP offers only mobile payment services to the public. The third PSP is a large non-banking financial institution in Mauritius, which is also engaged in other lines of business, regulated by the FSC and listed on the Official Market of the Stock Exchange of Mauritius. This PSP offers card services to the public.

With the coming into operation of the MauCAS which is a national payment switch owned and operated by the BoM, payments are channelled through bank accounts via the Instant Payments System[27], whereas e-money issuance consists of electronically stored monetary value as represented by a claim on the issuer, which is issued on funds (legal tender) of an equivalent amount for the purpose of making payment transactions and is redeemable for cash or a deposit into a bank account on demand. Only one PSP allowed cash at counter for cash e-wallet funding, however, no cash withdrawals were allowed from e-wallets by the PSP. As from September 2024, this PSP has stopped accepting cash at counter. All its transactions are now account to account.

[27] The Instant Payments System is component of the MauCAS and is a fast retail payment system which processes payments in real-time on a 24/7 basis. It enables interoperability among participants for electronic payments through channels such as mobile and internet banking.

Total sector assets amounted to USD 605 million based on the PSPs' latest available audited financial statements, which represented only 1% of total banking sector assets[28] as of 30 June 2024 and is considered to be on the low side.

ML Risk

The overall final ML vulnerability for the PSP sector was rated **Low** on the following premises:

(a) The PSP sector constitutes only 1% of the Banking sector which has ML risk of **Medium-High**;
(b) Transactional activities, including cash and cross-border transactions, of the PSP sector are deemed to be small when compared to the Banking sector;
(c) Only 1 PSP deals in cards which may be used in cross-border transactions. Thresholds are applied to such transactions, commensurate with customer risk profile and these are generally low;
(d) The other 2 PSPs deal only in domestic transactions and set thresholds on transactions, in line with customer profile and these are generally low;
(e) The customer base of PSPs comprises mostly individuals, which largely mitigates customer risk in the sector; and
(f) The sector no longer has any cash activity.

Taking into consideration the above, and the fact that PSPs have not reported any STR for the period under review and have not been subject to ML investigations, the ML threat was assessed as **Low**.

Conclusion

With a ML threat rating of **Low** for the PSP sector, and a **Low** ML Vulnerability rating, the ML risk rating reached for the sector was **Low**.

TF Risk

With the growing popularity of digital payment services comes the increased risk of financial crime and the global PSP sector has suffered heavily in recent years. For example, high profile terrorists such as Islamic State of Iraq and Syria (ISIS) have been financing their activities through well-known PSP and e-commerce scams[29]. However, during the period under review, there were no STRs or reported cases in our jurisdiction involving the misuse of PSPs for TF purposes.

TF Threat

The fact that PSPs have not reported any STRs for the period under review and have not been subject to any TF investigations, the TF threat rating for this sector was assessed as **Low.**

[28] BoM Monthly Statistical Bulletin July 2024.
[29] RISKSCREEN, 2022. Why Payment Service Providers must embrace technology to counter the threat of ML. [Online]
Available at: https://riskscreen.com/blog/why-payment-service-providers-must-embrace-technology-to-counter-the-threat-of-money-laundering/

TF Vulnerability

An inherent **Low** TF vulnerability rating was assigned to the PSP sector having regard to the following factors:

(a) The overall size/turnover of the sector is relatively small (the same analysis for ML risk assessment applies for this area), particularly when compared to the banking sector;
(b) Outward International transactions, which are subject to audit trail, are at a relatively low level (low aggregate value) and are conducted only through cards by only one PSP, primarily for online purchase of goods and services in countries with acceptable country risk ratings in line with the country risk policies of PSPs;
(c) Limits are set to card transactions by this PSP, commensurate with the customer risk profile and these are generally low. The upper limits for such card transactions are by far lower than the upper limits for banking sector customers;
(d) Inward international transactions are not allowed and therefore non-existent, which mitigates the TF risks in this area;
(e) The other 2 PSPs deal only in domestic transactions and have set thresholds on transactions in line with customer profile and these are generally low;
(f) The client base profile and level of cash activity are assessed as low risk and the same analysis as for the ML risk assessment applies; and
(g) The sector no longer has any cash activity.

Conclusion

With a TF threat rating of **Low** for the PSP sector, and a **Low** TF Vulnerability rating, the TF risk rating reached for the sector was **Low.**

2. OFIs under supervision of FSC

SUMMARY OF FINDINGS:

Leasing, Credit Finance and Factoring are OFI activities that are involved in the business of providing credit facilities to individuals and corporates and may thus be exposed to misuse by criminals. The OFI activities do make use of online payments, wire transfers or cash which could increase the potential risk of ML. Large volume of cross-border transactions have been identified in activities such as Treasury Management, Credit Finance, Investment Banking and the risk of ML arising from international transaction is present. The client base was reported as including PEPs and HNWI thus heightening the ML risks. However, the level of ML risk was much lower than those faced by banks.

The financial services landscape has evolved significantly over the past three years and the FSC is licensing numerous new products including Fintech-related activities. It is an industry with growing opportunities, but increasingly exposed to risk of ML as a result of continued diversification of products and use of technological platform which may allow illicit funds to be moved across borders.

The findings of the ML risk assessment showed that the bulk of the exposure to ML risk arises from Leasing, Payment Intermediary Services, Credit Finance, Investment Banking and Treasury Management.

There have been no reported cases in our jurisdiction involving the misuse of these activities for TF purposes. Nonetheless, the risk assessment showed that the potential channel for TF activities may arise from Payment Intermediary Services, Custodian (Non-CIS), Credit Finance, Treasury Management and Investment Banking.

Overall, the ML risk level for most activities in the OFI Sector was **Medium-Low**. Leasing was identified to have the highest residual risk level as **Medium-High,** followed by Payment Intermediary Services with a **Medium** risk. The TF risk level for the activities in the OFI sector ranges from **Medium-Low** to **Low**.

Overview of the Sector

The OFI sector under the supervision of the FSC consists of 24 activities with 172 licensees as of June 2024 comprising both domestic and global business. These activities are Asset Management, Distribution of Financial Products, Custodian Services (non-CIS), Family Office (Single), Family Office (Multiple), Peer to Peer lending, Payment Intermediary Services (PIS),

Funeral Scheme Management, Pension Scheme Administrator, External Pension Schemes, Actuarial Services, Credit Finance, Factoring, Leasing, Registrar and Transfer Agent, Treasury Management, Credit Rating Agencies/Rating Agencies, Investment Banking and Global Legal Advisory Services, Compliance Services, Crowdfunding, Fintech Service Provider, and Robotic and Artificial Intelligence Enabled Advisory Services and Representative Office (for financial services provided by a person established in a foreign jurisdiction). The activities are set out in section 14 (Second Schedule) and 79A of FSA, section 12 of Private Pension Schemes Act 2012, and Financial Services (Other Financial Business Activities) Rules 2008.

The main vulnerabilities and threats to ML risks were assessed individually for only 19 out of the 24 activities falling under the AML/CFT supervisory purview of FSC, as there were no licences which were yet issued to the remaining 5 activities[30].

ML Risk

The overall ML vulnerability of all the activities under the OFI sector ranged from **Medium** to **Low**, considering the controls in the sector. Taking into account the ML threat to the sector was **High** for Leasing, **Medium** for PIS and **Low** for all the other activities in the OFI sector, the ML risk which these sectors were exposed to ranged from **Medium-High** to **Low**.

It was observed that the ML risk for most activities in the OFI Sector was **Medium-Low**. Leasing was identified as having the highest ML risk level as **Medium-High** followed by PIS with a **Medium** Risk level as depicted in Table 12:

Table 12: ML Risk Ratings of 5 most risky activities in the OFI sector

Activities	Threat	Vulnerability	Risk Level
Leasing	High	Medium	Medium-High
Payment Intermediary Services	Medium	Medium	Medium
Investment Banking	Low	Medium	Medium-Low
Treasury Management	Low	Medium	Medium-Low
Credit Finance	Low	Medium-Low	Medium-Low

ML Threat

Except for leasing activity, there were no local typologies on the OFI activities falling under the supervision of the FSC.

Leasing companies were regarded as being more exposed to ML threat. This was specially observed in drug trafficking cases whereby traffickers were leasing motor vehicles. Based on reported cases, it was noted that drug traffickers were using leasing facilities either to acquire vehicles on the names of their relatives or using 'prête-noms'. There were also instances where the funds (cash) used for the repayment of the lease emanated from criminal proceeds.

[30] Compliance Services, Crowdfunding, Fintech Service Provider, and Robotic and Artificial Intelligence Enabled Advisory Services and Representative Office.

PIS providers act as a facilitator for the transfer of funds between two or more parties, such as merchants and consumers, without the need for direct interaction between them, enabling seamless, secure, and efficient transactions that criminals may exploit for illicit purposes.

There is one ongoing case relating to a PIS licensee against whom the FSC has received several complaints. The latter has failed to settle funds for its clients in line with the services provided.

Based on the assessment, out of all the activities falling under the OFI sector, only leasing companies and PIS were exposed to ML Threat. The threat level associated with Leasing companies and PIS were rated **High** and **Medium,** respectively. All the other products falling under this sector were rated **Low**.

ML Vulnerability

Analysis of the 5 riskiest activities in the OFI sector

(i) Leasing

The Second Schedule of the FSA provides for leasing as one of the financial business activities and requires that a licence be issued under section 14 of the FSA. Leasing activity provides an alternative means to raise money other than debt or term loan financing. Most leasing companies are locally based. The total assets and turnover for leasing were relatively significant when compared to other activities within the OFI Sector. The operators made use of agents for carrying out their business and the use of cash for repayments was also noted. The main ML vulnerability arises mostly from the lessee who may be laundering the proceeds.

The residual vulnerability for Leasing was assessed as **Medium**.

(ii) Payment Intermediary Services

PIS is related to the processing and execution of payment transactions whereby the consents of counterparties are required for the execution of the payment transactions. Holders of a PIS licence can only conduct business exclusively outside Mauritius. Most of the transactions are carried out through wire transfers and online systems with a relatively high frequency of transactions. There was limited use of agents, and no cash transactions were involved for the period under assessment.

The residual vulnerability of the PIS was assessed as **Medium**.

(iii) Investment banking

The Investment Banking activity regroups activities like investment advisory, investment advisory (corporate finance), investment dealer (full service including underwriting), distribution of financial products and asset management under a single umbrella licence in Mauritius. The financial products and services offered are subject to investors' demand, market conditions, and advances in technology. Product offerings are vast, and may be complex, with some devised for sale to the general public at large and others tailored to the specific needs of a single purchaser. Companies licensed to carry out investment banking by the FSC are all domestic entities providing the activities that are allowed under the scope of the licence to both local and foreign clients. The frequency and value of international transactions was assessed as significant.
The residual vulnerability for Investment Banking was assessed as **Medium.**

(i) Treasury management

Treasury Management involves the process of managing the cash and investments of the business, mostly within group entities. The goal of these activities is to optimise current and medium-term liquidity and make financial decisions involving invested and investable assets within a group of related companies.

Although the volume of international transactions was large, the potential ML risk associated with this type of activity was intuitively lower given that treasury management services are provided mostly to related entities within the same group of companies. The main ML vulnerability associated with treasury management activities resides with the payments resulting from foreign trade business.

The residual vulnerability for Treasury Management was assessed as **Medium.**

(ii) Credit Finance

Credit Finance provides alternative sources of financing (generally short-term loans) to household and corporates. Credit Finance providers are internationally recognised as being vulnerable to ML as loans could be repaid with illicit funds. Although the risk associated with cash repayment is generally high, it was noted that the repayment value was low for credit financing businesses.

The residual vulnerability for credit Finance was assessed as **Medium-Low**.

The supervisory actions of the FSC have had a positive impact on the level of compliance across the OFI sector. All licensees under the OFI sector applied CDD checks, maintained proper records and reported suspicious transactions. They are also required to conduct EDD checks when any customer or BO of a customer is of higher risk, such as a PEP, including the need to establish their source of wealth and the need for identifying the BO for all legal persons and legal arrangements. All transactions conducted by the OFI sector need to be recorded and are easily retrievable.

Conclusion

Overall, it was observed that the ML risk level for most activities in the OFI Sector was **Medium-Low**. Leasing was identified to have the highest ML risk level as **Medium-High** followed by Payment Intermediary Services with a **Medium** ML risk level.

TF Risk

The overall TF vulnerability of all the activities under the OFI sector ranged from **Medium-Low** to **Low**, considering the controls in the sector. Both the TF threat and the TF risk that the sector is exposed to ranged from **Medium Low** to **Low**.

The findings of the TF risk assessment showed that potential channels for TF activities are PIS, Custodian (Non-CIS), Credit Finance, Treasury Management, and Investment Banking and they were assessed as **Medium-Low** as depicted in Table 13. All the other activities in the OFI sector were assessed as **Low**.

Table 13: TF Risk Ratings of 5 most risky activities in the OFI sector

Activities	Threat	Vulnerability	Risk Level
Payment Intermediary Services	Medium-Low	Medium-Low	Medium-Low
Custodian services (Non-CIS)	Low	Medium-Low	Medium-Low
Credit finance	Low	Medium-Low	Medium-Low
Treasury management	Low	Medium-Low	Medium-Low
Investment banking	Low	Medium-Low	Medium-Low

TF Threat

There was no existence of local typologies/cases relating to the activities in the OFI sector under the purview of the FSC. Mauritius has had no experience of domestic terrorist activity; however, it remains vulnerable to TF activities and the possibility of terrorist attacks in Mauritius cannot be eliminated. During the period of assessment, there have been no reported cases of transfer of funds for TF purposes. For the assessment, international typologies including FATF typologies were considered to gather insights into TF trends and whether similar risks may exist in Mauritius. PIS was found to be more exposed to TF risk given the existence of typologies globally for this type of activity and the high level of cross border transactions.

Taking into consideration the above, the TF threat rating for this sector was assessed as **Low** except for PIS which was **Medium-Low**.

TF Vulnerability

The risk factors considered for assessing the TF vulnerability of the above-mentioned activities related mainly to the size of the entities involved, and the cross-border nature of the transactions carried out by these sectors. PIS licensees conducted their business exclusively outside Mauritius and a relatively high frequency of international transactions were noted. In respect of Custodian (Non-CIS) services, some companies were engaging with high-risk clients, albeit at a limited level, and had large volume of international transactions.

Based on findings of supervisory engagements including onsite inspections, it was observed that most entities in the OFI sector have effectively implemented their obligations in relation to TFS. As part of their compliance functions, clients were subject to sanctions screening against the UNSC list at onboarding stage and also whenever the UNSC list was changed. All transactions were also subject to screening sanctions. Existing accounts were screened on a regular basis, that is, as and when the UNSC list was changed. It was also noted that enhanced measures were applied prior to onboarding all high-risk clients such as seeking senior management's approval.

Other activities exposed to TF Risk

To the extent that no local cases were relevant to the activities in the OFI Sector, international typologies indicated potential risk for Peer-to-Peer (P2P) lending whereby terrorist financiers used online financing technologies to move funds through online platforms. In the Mauritian context, no intelligence and investigation revealed the potential misuse of P2P lending for TF purposes.

Crowdfunding also has been identified as vulnerable for TF on the international front, as they can be exploited for illicit purposes, including instances where the true purpose of the funding campaign is masked. It represents an emerging TF threat as individuals and organisations seeking to raise funds for terrorism and extremism support may claim to be engaged in legitimate charitable or humanitarian activities. There is no licensee for crowdfunding at the time of assessment and thus considered non-existent.

Conclusion

Overall, it was observed that the TF risk level for activities in the OFI Sector ranged from **Medium-Low** to **Low**.

3. OFIs - Co-operative Credit Union Sector

SUMMARY OF FINDINGS:

Members of Credit Unions are solely citizens of Mauritius and legal entities registered domestically. As at date, no cases have been reported where CCUs have been misused for ML/TF purposes. The overall ML risk for the sector is **Medium-Low**, while the overall TF risk for the sector is **Low**.

Overview of the Sector

Nature and Structure of CCUs

Co-operative Credit Unions (CCUs) are classified under the financial services class of society registered under the Co-operatives Act and supervised by the Registrar of Co-operative Societies. The primary objectives of CCUs are to foster financial discipline by promoting thrift among their members and providing access to credit facilities.

In Mauritius, CCUs function exclusively at the domestic level and operate as single entities, with only one community-based CCU maintaining three branches across the country. These credit unions are broadly categorized into two types:

- **Industrial-Based Credit Unions**: Membership is restricted to individuals linked by a common bond, including government employees, workers in parastatals, hotels, educational institutions, and employees of private organizations.
- **Community-Based Credit Unions**: These are formed by members of specific communities who share a common locality or social connection.

Statistics and Economic Contribution

As of 30 June 2022, a total of 164 active CCUs were providing deposit and loan facilities to approximately 58,913 members. The sector's total asset size was valued at around USD 70 million, with issued loans amounting to approximately USD 15 million. The co-operative sector's contribution to the GDP between 2018 and 2022 ranged from 0.17% to 0.23%.

CCUs are classified as reporting persons under the FIAMLA. As such, they are obligated to implement AML/CFT preventive measures, including:

- Conducting CDD/Identification procedures
- Monitoring financial transactions
- Ascertaining the source of funds
- Identifying and reporting of suspicious transactions
- Record-keeping

Membership and Operational Scope

Membership in CCUs is limited to Mauritian citizens and domestically registered legal entities. Among the 164 credit unions, only 1 has a legal entity (domestic) as a member. Furthermore, only 1 CCU operates three branches and maintains an affiliation with an international strategic partner.

Statistics concerning the number of domestic PEPs within Industrial-Based and Community-Based CCUs was not available. However, it was observed that PEPs were primarily present in Industrial-Based CCUs, comprising individuals employed in Government, private enterprises, and parastatal bodies.

To date, no instances of ML or TF linked to CCUs have been reported.

Transactional Limits and Practices

Cash deposits and loan repayments within CCUs adhere to specific limits as per their regulatory frameworks:

- **Community-Based CCUs**: Cash deposit limits are capped at MUR 50,000 (approximately USD 1,100), with loan repayment transactions not exceeding MUR 10,000 (approximately USD 220).
- **Industrial-Based CCUs**: Cash deposits are limited to MUR 100,000 (approximately USD 2,200).

Most transfers to CCUs occur through direct debit transactions. Notably, non-face-to-face transactions do not exist in either Industrial-Based or Community-Based CCUs. Additionally, CCUs do not engage in international transactions.

ML Threat

For the period under review no cases of ML were registered (prosecution, investigation, conviction) where CCUs were involved. However, as per statistics from the MPF, 3 cases of predicate offence were registered where CCUs were involved. As such, the ML threat associated to CCUs was considered **Medium-Low**.

ML Vulnerability

Considering the total size/volume, client base profile, level of cash deposits and transactions in the sector, the inherent vulnerability was assessed as **Low.**

However, although a comprehensive legal and regulatory AML/CFT framework exists for credit unions, the supervisory regime was not supported by appropriate powers vested in the Registrar of Co-operatives for AML/CFT supervision (on-site/off-site monitoring and inspections) and enforcement powers in case AML/CFT compliance breaches were detected.

Regulatory reforms are presently in progress, not only to strengthen financial integrity, but also to boost public confidence in CCUs, ensuring that they continue to serve their members efficiently while remaining safeguarded against illicit activities.

Nonetheless, the availability and effectiveness of entry controls at market entry was rated at **Medium-High** having regard to the requirements for formation, registration, supervision and regulation of both categories of credit unions under the Co-operatives Act, amongst others.

The Residual ML Vulnerability was assessed as **Low**.

Conclusion

The overall ML risk for the sector was **Medium-Low**, after considering the vulnerability of **Low** and ML threat of **Medium-Low**.

TF Risk

During the period under review, no intelligence and investigation revealed the misuse of CCUs for TF purposes. It was also found that none of the CCUs registered in Mauritius was exposed to entities and persons affiliated with active terrorist threat or persons that may be sympathetic to terrorist persons or ideologies. Additionally, no terrorist organisation/group/person was funded through funds obtained from CCUs.

TF Threat

Based on the overall threat rating of the sector's threat factors, the TF Threat associated with the sector was considered as **Low**.

TF Vulnerability

The inherent vulnerability was also assessed as **Low** taking into consideration the size of the sector, the level of transactions which is primarily domestic. No cases of TF were registered in the CCU sector.

Conclusion

The overall TF risk for the sector was **Low**, after considering the vulnerability rated as **Low** and TF threat rated as **Low**.

11. TRUST AND COMPANY SERVICE PROVIDERS SECTOR

SUMMARY OF FINDINGS:

The TCSP sector comprises management companies and trust service providers supervised by the FSC as well as company service providers regulated by the Registrar of Companies (ROC).

Management companies and trust service providers face a **Medium-High** ML risk in Mauritius due to the nature of the products being serviced notably GBCs and trusts. The entities managed by TCSPs include higher risk client profiles, non-face-to-face dealings, complex legal structures and cross border transactions, which may make the sector vulnerable to ML by presenting opportunities for illicit funds to move across borders undetected while concealing the identities of those involved.

These ML vulnerabilities are mitigated by the AML controls implemented by the TCSPs as set out in the comprehensive AML/CFT legal framework in Mauritius. The AML measures of TCSPs include rigorous CDD procedures and ongoing monitoring of business relationships and transactions. While most management companies have demonstrated that they have strong controls in place, there are few TCSPs that need to improve in undertaking mitigating measures commensurate to the risk of their clients.

The TF risk of the TCSP sector is **Medium-Low** given the low prevalence of TF related cases in the Mauritian jurisdiction. The TCSP is vulnerable to TF due to the cross-border nature of the sector facilitating financial transactions including to and from high-risk jurisdictions. TCSPs also manage Charitable Trusts which may be abused to raise and channel funds for terrorist purposes. TCSPs have applied necessary safeguards to mitigate their TF risk which is reinforced through robust licensing regime and ongoing supervision. Further actions need to be taken in respect of TF risk understanding and specific CFT mitigating measures.

CSPs are supervised by the ROC. In 2022, 228 CSPs were under ROC supervision, with no natural persons registered as CSPs. The most common services provided were secretarial services, formation agent and registered address services for many clients.

The CSP sector has been assessed as posing a lower level of ML risks as compared to the other sectors of the DNFBPs. The CSP sector had a **Medium-Low** ML risk, with a **Low** ML threat and **Medium** vulnerability. Only some CSPs were linked to clients with high-risk factors, whilst others had clients posing a lower level of risk. No local evidence suggested ML misuse. For TF, both the threat and vulnerability were **Low**, resulting in an overall **Low** TF risk.

1. TCSPs under the Supervision of FSC

Overview of the Sector

The TCSP sector servicing GBCs and trusts consists of Management Companies and the Trust Service Providers, also referred as Qualified Trustees (QTs). The range of services provided by TCSPs includes formation and management of legal entities such as GBCs and trusts. In Mauritius, MCs are licensed under section 77 of the FSA. All QTs are licensed and supervised by the FSC. Both Management Companies and QTs are regulated as FIs and therefore are required to comply with the full range of AML/CFT requirements. Their obligations include conducting thorough due diligence on their clients, monitoring clients' transaction and activities, conducting frequent audit reviews and establishing mechanisms to report suspicious transactions and unusual transactions.

As of June 2024, the TCSP sector comprised 257 entities broken down into 180 MCs, 29 corporate trustees and 48 authorised qualified trustees, administering around 13,000 GBCs, 6,000 Authorised Companies (ACs) and 5,500 Trusts.

GBCs are resident corporations, holding a licence from the FSC, whose majority of shares or beneficial interest are held or controlled by a person who is not a citizen of Mauritius and conduct business principally outside Mauritius. ACs are companies which conduct business principally outside of Mauritius and it has its central management and control outside Mauritius.

The TCSP sector plays an important role in the economic development of Mauritius by contributing to direct employment of around 5,600[31] people as of December 2023. The global business sector contributed 8.4%[32] to GDP in 2023. The aggregate assets of the global business sector had reached USD 705 billion[33] as of June 2023 with an annual growth rate of 3.9%[34] as of 2023.

ML Risk

The inherent vulnerability of the sector for ML was assessed as **Medium-High**. Considering the controls in the sector, the overall vulnerability of the sector was **Medium**. Given that the ML threat to the sector was **High**, the ML risk that the sector was exposed to was **Medium-High**.

ML Threat

The TCSP sector was exposed to ML threats due to the possibility of TCSPs being misused by criminals to create legal structures or arrangements in multiple jurisdictions to obfuscate the flow of illicit funds and reduce traceability. Based on typologies, it is globally observed that money launderers may abuse the services of TCSPs to set up companies to then facilitate the movement of illicit funds and obfuscate beneficial ownership. Furthermore, TCSPs are used to facilitate the setting up of multiple layers of corporate vehicles and complex structures which make it challenging for authorities to trace origin of funds.

---

31 FSC Mauritius, Statistics.
32 FSC Mauritius, Statistics.
33 Financial Stability Report, December 2023, BoM.
34 FSC Mauritius, Statistics.

In some instances, bank accounts of foreign legal persons were used as a conduit to channel funds allegedly to be proceeds of crime to other foreign counterparts. Over the period, the trend of investigation showed that the most used types of corporate structures were mostly GBCs.

Intelligence reports indicated that proceeds of crime emanating from foreign jurisdictions were suspected to be laundered through the bank accounts of some clients of TCSPs. Bank to bank transactions were more easily executed and this facilitated the transfer of funds across borders. Domestic cases revealed that there were only allegations that tainted funds had landed into the bank accounts of clients of TCSPs. Also, in most cases investigated, fraud and forgery were mostly used as predicate offences for ML. Thereafter, the misappropriated proceeds were transferred to both legal and natural persons in disguise of proceeds from normal business activities.

For cross border transactions, the pattern observed was through movement of funds from multiple bank accounts and thereafter moving these funds to other foreign jurisdictions. These factors, coupled with known typologies for the misuse of TCSP, indicated that the threat for the sector was High.

The level of ML threat in this sector was therefore rated **High**.

ML Vulnerability

TCSPs operating in international financial centres around the world are exposed to ML risks largely due to the complexity of their structures and the diverse nature of their clientele. In Mauritius, the contribution to the economy and the substantial turnover of the TCSP sector highlights its importance.

The large client base of Management Companies, comprising GBCs, ACs and trusts, broaden their exposure to ML risks. Trusts, commonly used for estate planning and asset management, were also vulnerable as they may be used to obscure ownership and facilitate illicit transactions.

The involvement of PEPs, particularly foreign PEPs, introduced additional challenges to the sector as a result of their influential position. Some foreign PEPs operated in regions with differing levels of regulatory oversight and varying measures to address financial crime, which may make them more complex to manage as clients.

HNWIs represented a significant portion of the sector's clientele. Their financial resources, combined with the use of complex arrangements, can create opportunities for misuse. While transactions with HNWIs are often legitimate, they may use their relationships to expedite processes that bypass necessary safeguards, thereby, increasing the sector's overall risk.

Clients with ties to jurisdictions identified as high-risk further increased the exposure of the sector. These regions often lacked adequate regulatory systems, which can make it easier to conceal the origins of funds and the identities of those involved. The cross-border nature of the sector adds another layer of complexity, as differences in regulatory environments can hinder compliance and enforcement efforts.

The use of complex ownership structures in the sector may present challenges, as they can sometimes be misused to obscure the origins of funds or make it difficult to determine ownership details. For instance, trusts, when integrated into such structures, add a layer of complexity

making the tracing of transactional records difficult and hence potentially making it more challenging to identify unusual activities. Other instances of vulnerability are where the economic rationale for creating such trusts does not have a clear stated purpose. For discretionary trusts which are part of broader structures, additional safeguards are required as beneficiary details are not always immediately available at the time of establishment. While the cross-border nature of transactions linked to such structures adds to the complexity in determining the Ultimate Beneficial Owner (UBO), ongoing efforts to enhance transparency in the sector are contributing positively to addressing potential risks. Strengthening transparency measures and oversight can help enhance clarity and ensure responsible use of these arrangements.

Though advancements in technology have improved efficiency, non-face-to-face dealings in the TCSP sector may also give rise to new risks which need to be monitored in future business relationships. Despite measures, such as document certification and independent verification, these business relationships make oversight challenging, adding to the vulnerability of this sector.

In few instances, the use of unregulated intermediaries was noted. These intermediaries can act as middlemen on behalf of clients, bypassing established controls and concealing critical information. While there are frameworks for regulated introducers, the absence of similar standards for intermediaries leaves gaps that can be exploited.

The TCSP sector is guided by the comprehensive set of AML legislation to conduct their business and are required to apply the full range of preventive measures commensurate to their size, context and business risks related to ML. TCSPs are subject to thorough entry controls by the FSC as well as being supervised under a risk-based approach for AML/CFT.

Through implementation of its AML/CFT Risk Based Supervision Framework since 2020, the FSC checks for compliance of TCSPs with AML requirements, notably during risk based onsite inspections and offsite reviews. In this respect, where the FSC identifies non-compliance, it takes a broad range of sanctions ranging from private warnings to administrative penalties, amongst others, in cases of breaches.

Furthermore, plans for outreach activities covering ML risks and AML obligations are implemented and updated on a yearly basis, taking onboard feedback from licensees whilst adapting to the evolving risk environment. Through the continuous supervisory efforts, the compliance culture of TCSPs has improved over time, specifically in terms of understanding the risks associated with the sector and the application of appropriate control measures including proper customer due diligence and monitoring of suspicious transactions.

Whilst most TCSPs have made significant progress in mitigating their ML vulnerabilities by applying stringent controls, there are areas that need further attention. Though TCSPs have established ethics-related standards to promote integrity, there were few instances where these standards were not fully upheld. Additionally, limitations in resource allocation for compliance roles influenced the overall efficiency of compliance functions.

Following the inherent vulnerability and the strength of AML controls assessment, the residual vulnerability of the TCSP sector to ML abuse was **Medium**.

Conclusion

In consideration of the assessment and analysis, the ML threat to the sector was **High**, the overall ML vulnerability of the sector was **Medium**, hence the ML risk that the TCSP sector servicing GBCs and trusts was exposed to was **Medium-High.**

TF Risk

The inherent vulnerability of the sector for TF was assessed as **Medium.** Considering the controls in the sector, the overall vulnerability of the sector was **Medium-Low**. Considering that the TF threat to the sector was **Medium-Low**, the TF risk that the sector was exposed to was **Medium-Low**.

TF Threat

With the growing and evolving level of terrorism activities in the global landscape, it is imperative to take stock of the impact and intensity of TF risks in relation to the TCSP sector of Mauritius. International typologies on the TCSP sector suggest that criminals may seek to set up opaque structures that can circumvent any restrictive measures in place. Nevertheless, there is no indication that legal entities or legal arrangements administered by the TCSP sector in Mauritius have been abused for TF purposes.

TF Vulnerability

The TCSP sector is exposed to TF risk due to the inherent nature of the business of the players of the sector. Management Companies are exposed to TF vulnerabilities through the products they administer. The nature of the global business sector which is administered by Management Companies involves a high degree of non-face-to-face dealings, cross-border transactions and layered structures. The combination of these factors together with higher client profiles such as foreign PEPs and HNWIs may make the traceability of transactions more complex. As a result, it may require enhanced scrutiny to discern genuine transactions from those intended to finance terrorism or those made to move and distribute funds to designated entities, their affiliates and potential sympathizers.

Data on inward and outward flow of funds showed the financial linkages of some management companies in the TCSP sector with jurisdictions having TF concerns for which stringent measures are applied based on risk understanding. There have been no cases concluding that the TCSP sector in Mauritius had been misused for TF purposes.

The TCSP sector may be vulnerable to TF due to the nature of some charitable trusts which are managed by QTs. As such, such legal arrangements may be abused for TF due to cross-border transactions or activities and non-face-to-face interactions with beneficiaries of charitable trusts.

Given the international exposure of these trusts, terrorist organisations may infiltrate such financial structures and divert funds in order to support terrorism.

Despite the above, there were no known cases whereby operators in the TCSP sector in Mauritius were identified for TF. The risk of cash being transferred out of Mauritius through the TSCP sector to fund terrorist groups or activities abroad was also not present as Management Companies/QTs were not involved in cash activity.

The TCSP sector is subject to a comprehensive legal and regulatory framework which is consistent with international standards in mitigating TF risk. The FIAMLA and FIAMLR have main provisions relating to CFT preventive measures including the appointment of MLRO for the reporting of suspicious transactions pertaining to TF to the FIU, the obligation to conduct a risk assessment to identify, assess and document TF risk, and the requirement to identify and verify customers as well as record keeping of transactions.

The licensing regime for the TCSP sector is further protected through mitigation controls whereby GBCs are required to be licensed, regulated, monitored and supervised. Further, Management Companies/QTs undergo thorough assessments for new appointment/change of MLROs, Deputy MLROs, Compliance Officers, Directors, Controllers including UBOs as applicable.

Management Companies/QTs are subject to onsite inspection and offsite monitoring based on the yearly risk-based supervision cycle having regard to evolving risks. Depending on the outcomes of these supervision activities, Management Companies/QTs are required to submit and undertake remedial actions, as applicable. As part of the CFT controls, a wide range of administrative sanctions and criminal sanctions are available for breaches of relevant CFT laws by the TCSPs. The FSC assesses the risk exposure following inspections to determine change in risk profile.

Most staff of the TCSP sector are members of professional bodies and are thereby required to adhere to high standards of integrity. Similarly, key persons of Management Companies/QTs are mandated to be competent and proficient at all times as obliged under the Competency Standards (as amended), and other staffs are required to undergo ongoing CFT training covering typologies and TFS reporting procedures and obligations. Management Companies/QTs comply with the UNSA by having sanctions screening processes in place and implementing TFS measures relating to TF on a real time basis.

Furthermore, Management Companies/QTs monitor inward and outward transactions of their clients throughout the business relationship so as to identify any suspicious transactions. Despite having the process in place, TCSP need to strengthen their transaction monitoring systems to better identify and filter suspicious transactions linked to TF. At present, red flags and internal reporting mechanisms primarily focus on transactions associated with ML. Enhancing these systems will ensure that TF-related risks are effectively detected and addressed.

While most Management Companies/QTs have conducted independent audit review of their compliance program, CFT specific elements were not always covered.

The residual vulnerability of the TCSP Sector for TF was **Medium-Low.**

Conclusion

Based on the assessment, the TF threat to the sector was **Medium-Low**, the overall TF vulnerability of the sector was **Medium-Low**, hence the TF risk that the sector was exposed to was **Medium-Low**.

2. Company Service Providers under supervision of Registrar of Companies

Overview of the Sector

As of 2022, there were 228 CSPs under the supervision of Registrar of Companies (ROC). No natural person was registered with the ROC to act as CSP. Secretarial services are the services that were most commonly provided by CSPs to their clients. CSPs also provide formation agent and registered address services to a considerable number of clients.

ML Risk

There were a few CSPs which were linked with high risk factors such as PEPs, High-Risk Jurisdictions/Countries, HNWIs, clients with criminal records, clients operating within a complex structure and Professional Intermediaries/Agents/Introduced Business. However, generally the sector was servicing mostly domestic clients, which were deemed less risky for ML purposes.

Overall, the CSP sector might be viewed as a low revenue generator with low associated risks. There were no local typologies to demonstrate that CSPs were used for ML. The level of ML threat in this sector was thus rated **Low**.

The ML inherent vulnerability of the CSP sector was **Medium** and the quality of AML controls rating was assessed as **Medium**. The overall ML vulnerability of the CSP sector was **Medium.**

Conclusion

The ML threat associated with the CSP sector was rated **Low**. The overall ML vulnerability of the CSP sector was **Medium**. Hence, the ML risk of the CSP sector was rated as **Medium-Low**.

TF Risk

The TF threat associated with the CSP sector was rated **Low** and the TF vulnerability was assessed as **Low**. Consequently, the overall TF risk of the CSP Sector was assessed as **Low.**

12. DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

SUMMARY OF FINDINGS:

Worldwide typologies and cases in Mauritius have demonstrated that the DNFBPs can be abused for ML and TF. As such, an AML/CFT infrastructure, comprising comprehensive legislative and robust supervisory framework was put in place since May 2019 with the assistance of the German Agency for International Cooperation (GIZ) and the EU AML/CFT Global facility to regulate this sector. All DNFBPs' supervisors have put in place dedicated AML/CFT units and are conducting risk-based supervision, conducting training to AML/CFT staff, educating the reporting persons through on-going outreach and applying sanctions for non-compliance with AML/CFT requirements. The AML/CFT laws and regulation have further been strengthened since May 2019.

The DPMS, Notary, Gambling and Real Estate sectors were assessed as having the **highest ML** risk as opposed to the other DNFBPs. On the other hand, the DNFBPs witnessed **Low** TF risk ranging from **Medium-Low** to **Low.**

Overview of the Sector

As of 30 June 2023, the value added of the DNFBP to the economy was estimated at MUR 16 billion. For the purpose of this NRA, the assessed DNFBPs are Barristers, Attorneys and Law Firms, Notaries, Real Estate sector operators, Gambling sector operators, Accountants and DPMS.

Taking into consideration (i) the ML threats, information derived from investigations and other sources both at national and international levels, STRs; (ii) the vulnerability of the different entities of the DNFBP sector; and (iii) the strength of the AML/CFT controls in place in the various entities within the DNFBP sector, the ML risk faced by these different entities are summarized in Table 14.

Table 14: ML Risk Ratings for DNFBPs

Sector	ML Threat	ML Vulnerability	ML Risk
DPMS	Medium-High	Medium	Medium-High
Notary	Medium-High	Medium	Medium-High
Gambling	High	Medium	Medium-High
Real Estate	Medium	High	Medium-High
Accountancy	Medium	Medium-Low	Medium
Legal Profession (excluding Notary)	Medium	Medium	Medium

The DPMS, Notary, Gambling and Real Estate sectors were assessed as having the highest ML risk as opposed to the other DNFBP sectors.

On the other hand, the DNFBP sector witnessed **Low** TF risk ranging from **Medium-Low** to **Low** ratings as outlined in Table 15.

Table 15: TF Risk Ratings for DNFBPs

Sector	TF Threat	TF Vulnerability	TF Risk
DPMS	Low	Medium-Low	Medium-Low
Notary	Low	Medium-Low	Medium-Low
Gambling	Low	Medium-Low	Medium-Low
Real Estate	Low	Medium	Medium-Low
Accountancy	Low	Low	Low
Legal Profession (excluding Notary)	Low	Low	Low

A. DPMS Sector

SUMMARY OF FINDINGS:

The DPMS sector was rated as having a **Medium-High** ML risk, with links to lifestyle laundering and illegal money lending. While a key industry, it remains vulnerable to Trade-Based Money Laundering and over/under invoicing. Few ML cases were recorded, though some remain under investigation. AML/CFT supervision is in place, but risks persist. TF risk was assessed as **Medium-Low** with no reported cases or suspicious transactions, supported by strong safeguards and CFT controls.

ML Risk

The DPMS sector was identified as having a **Medium-High** ML risk as recent drug trafficking cases being investigated indicated possible lifestyle laundering in the jewellery sector where part of the ill-gotten gains of the traffickers was spent on expensive items to display signs of wealth/status. Investigations have also revealed that suspects were involved in the business of illegal money lender and taking properties and jewels as collateral.

As one of the most traditional industries in Mauritius, the jewellery sector initially started as a sector dominated by small-scale operators producing basic products for the local market. The sector has experienced several changes over the past decades and has grown to become the top third manufacturing sector in the country. The Jewellery sector comprised both export-oriented and domestic-oriented enterprises. The main products in the sector are pearls, precious/semi-precious stones, and jewellery, goldsmith, and silversmith wares. The average contribution to GDP of the DPMS sector was 0.4% between 2018 and 2022.

The number of dealers in the DPMS sector conducting the prescribed activities under the FIAMLA stood at 319 as of 31 August 2022 and were thus considered as reporting persons. The sector consists of approximately 30 to 45 companies considered active exporters and supplying high-end products for world-famous brands.

The Jewellery Act regulates the dealings (purchase, manufacture and sales) in precious metals, namely, gold, silver, palladium and platinum and jewellery made from these precious metals, and of precious and semi-precious stones for DPMS. Members of the DPMS sector are registered with the ROC and are duly licensed by the Assay Office. The Assay Office ensures that dealers in jewellery sector operating in Mauritius comply with the Jewellery Act 2007 and its regulations.

DPMS are categorised as reporting persons under the FIAMLA by virtue of conducting the prescribed activities under Part II of the First Schedule of the FIAMLA and are thus subject to AML/CFT supervision by the FIU. The prescribed activities relevant for the DPMS sector include dealers in jewellery, precious stones or precious metals who engage in any transaction of at least USD 12,000 in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.As per the statistics gathered, there were few ML cases in which the DPMS was involved, and they are still under investigation. There was no

case pending trial at the Court against any jeweller. Regarding external threat, in the year 2020, two foreigners were intercepted by customs, and they were found to be in possession of gold ingots which were not declared. Both have subsequently been found guilty of ML and were convicted. The court also ordered that the undeclared gold ingots be forfeited.

For the purpose of the assessment, international typologies as well as the different ML techniques including Trade Based Money Laundering and over/under invoicing in international trade of diamonds was considered.

Conclusion

Considering the ML threat, which was rated **Medium-High** and ML vulnerability level, which was rated **Medium**, the ML risk was rated **Medium-High**.

TF Risk

Despite the inherent risk of using the DPMS sector as a mode of transferring/moving value for TF, several safeguards against the abuse/misuse of the sector have been established in Mauritius. These include, amongst others, cross border controls and CFT obligations that are to be undertaken by reporting persons. It is also to be noted that during the period under review, there were no reported case suggesting the use of the jewellery sector for TF purposes. Likewise, there also were no STRs filed by the supervisory body and/or operators in this sector.

Hence, the TF Threat level in this sector was rated **Low.**

Based on the inherent TF vulnerability assessment and on the strength of CFT controls, the residual vulnerability of the DPMS sector to terrorism financing was **Medium-Low**.

Conclusion

Considering TF threat, which was rated **Low** and vulnerability level, which was rated **Medium-Low,** the TF risk was **Medium-Low.**

B. Notary

SUMMARY OF FINDINGS:

Notaries, acting as gatekeepers, handle transactions highly vulnerable to ML, particularly in real estate. Governed by the Notaries Act 2008, 59 notaries are subject to AML/CFT regulations under FIAMLA. Despite safeguards, notaries have been linked to ML cases, where illicit funds were used for property acquisitions or fraudulently transferred. Investigations are ongoing, highlighting the sector's exposure to financial crime risks.

The ML risk for notaries was rated **Medium-High**, with a **Medium-High** threat and **Medium** vulnerability based on recent trends and cases. In contrast, TF risk was assessed as **Medium-Low**, with no reported involvement and strong CFT controls mitigating vulnerabilities.

ML Risk

As gatekeepers, notaries are exposed to tremendous amounts of information, and act on behalf of their customers in many transactions. Some of these transactions are highly vulnerable to ML due to the nature of the products or services that are offered.

The Notaries are registered with the Chamber of Notaries and are normally governed by the Notaries Act 2008 and the code of ethics ("code de deontologie"). The sector consists of 59 Notaries who are regulated for AML/CFT purposes as they have confirmed to be conducting the prescribed services under FIAMLA, mainly through buying and selling real estate and involvement in real estate transactions. Other services provided by Notaries include Quittance, Procuration/Power of Attorney Notoriété/deed of Notoriety, Notification de la revocation de procuration, Testament/Will, Prêt/Loan, amongst others.

Despite being in the legal sector, Notaries have a very distinct role as compared with other professionals in the sector. More specifically, they are the only ones within that sector to be engaged in buying and selling real estate, namely in the finalisation of the real estate transactions by providing a duly signed notarial deed. Since the real estate sector is vulnerable to ML risk, it also has an incidence on the vulnerability of the Notary to ML risk.

Following the legislative amendments brought through the AML/CFT (Miscellaneous Provisions) Act 2020, though notaries can still accept cash for the legal services they provide, cash consideration is no longer acceptable for acquisition of immovable property and same should be carried out by way of bankers' cheque.

Several typologies published by international bodies demonstrated that the legal profession, including notaries, was tagged as professional enablers to ML offences given that they acted as gatekeepers to the international financial system and could play a key role in facilitating illicit financial flows by lending their expertise. The cases involving Notaries were mostly

linked to the real estate sector where the services of the Notaries were hired for the acquisition of immovable properties. It was found that the sources of funds used by their clients emanated mainly from illicit activities which the Notaries failed to detect. In some cases, it was also noted that the funds were fraudulently transferred to the personal bank accounts of the clients or that of their close relatives and the funds were subsequently used to acquire properties. Investigations into these cases are still in progress.

Conclusion

Based on the trends in recent years and ongoing cases, the ML threat associated to the profession of Notary was rated **Medium-High,** while the ML Vulnerability level was rated as **Medium**. Consequently, the ML Risk of the sector was rated as **Medium-High**.

TF Risks

During the period under review, there were no reported instances where Notaries have been personally involved or found in facilitating TF. Hence, the TF threat level in this sector was rated **Low**.

Based on the inherent TF vulnerability assessment and on the strength of CFT controls, the residual vulnerability of the Notaries sector to terrorism financing was **Medium-Low**.

Conclusion

Considering TF threat, which was rated **Low** and vulnerability level, which was rated **Medium-Low**, the TF risk was rated as **Medium-Low**.

C. Legal Profession (excluding Notary) Sector

SUMMARY OF FINDINGS:

The Legal Professions (excluding Notary) Sector includes law firms, barristers, and attorneys, with AML/CFT-related activities such as trust account management, company formation, and securities transactions. Clients often include PEPs, high-risk businesses, and individuals with criminal backgrounds. The legal sector faces a **Medium** ML risk, with vulnerabilities due to their diverse client base. While AML obligations apply, most legal professionals focus on litigation and advisory services, limiting exposure. The sector's TF risk was rated **Low**, with no reported cases of TF facilitation by legal professionals.

The legal professions sector comprises Law Firms, Barristers and Attorneys. The fields of expertise of legal professionals in relation to AML/CFT prescribed activities encompasses establishing trust accounts, forming corporations and legal trusts, and securities-related transactions, amongst others. The clients' profile in this sector generally includes Politically Exposed Persons, clients in vulnerable businesses and professions, clients with criminal backgrounds, and clients whose activities are conducted in high-risk jurisdictions. The FIU is the AML/CFT supervisory body for the legal professions sector.

ML Risk

Given the diverse client base with different risk profiles, the legal sector is deemed vulnerable to being exploited for ML. In order to mitigate this risk and in line with Recommendation 22 of the of the FATF, legal professionals are now also subject to AML obligations, depending on the services being offered. During the period under review, the sector had 77 legal professionals who were considered as reporting persons, i.e., 16 Attorneys, 39 Barristers, and 22 Law Firms. The difference arising between the professionals in the sector and the ones being supervised is due to the fact that most legal professionals in Mauritius provide litigation and advisory services and were thus not under the AML/CFT regulatory purview.

The average contribution to GDP of the Legal Profession sector as a whole (including Notaries), was 0.2% between 2019 and 2022. Data obtained for the assessed period indicated that the average turnover and assets managed was USD 15 million and USD 25,000, respectively.

All the practitioners in the legal profession sector, whether self-employed or part of an organisation or law firm have their specific association namely the Mauritius Law Society (for Attorneys) and the Mauritius Bar Association (for Barristers). Besides adhering to their respective Code of Ethics, legal professionals are also required to comply with the AML regime as stipulated under the FIAMLA, and POCA, amongst others, and their subsequent regulation.

Inspection findings have shown that even though the legal professionals do have international clients in their portfolio, the amount being dealt do not appear to constitute a significant part of their work.

Conclusion

Based on the trends since the past years and ongoing cases, the ML threat associated with the legal profession (excluding Notary) sector was rated **Medium**. The ML Vulnerability level was rated as **Medium.** The ML risk was therefore rated as **Medium**.

TF Risk

The proficiency of legal practitioners may also be exploited knowingly or unknowingly for terrorism/TF purposes. Terrorist groups or terrorist financiers may avail of the services offered by professionals in this sector for disguising, storing, moving and using terrorism related funds (Government of Canada, 2015)[35].However, during the period under review, there were no reported instances where members of the legal profession (excluding notary) had personally been involved or found in facilitating TF.

Conclusion

Considering TF threat which was rated **Low**, and vulnerability level also rated as **Low**, the TF risk was therefore assessed as **Low**.

[35] Government of Canada, 2015. *Assessment of Inherent Risks of ML and TF in Canada*. [Online] *Available at*: *https://www.canada.ca/en/department-finance/services/publications/assessment-inherent-risks-money-laundering-terrorist-financing.html*

D. Gambling Sector

SUMMARY OF FINDINGS:

Drug traffickers commonly use the gambling sector to justify illicit funds, with 75% of cases involving betting gains as a defence. Criminals exploit horseracing, casinos, and illegal betting, often using split transactions and credit betting to launder proceeds. The ML threat in the sector was rated **High**, with unlicensed bookmakers increasing illegal activities; however, the ML risk in the gambling sector was rated **Medium-High**, with a **Medium** vulnerability. TF risk was assessed as **Medium-Low**, as no cases of misuse for TF were reported.

ML Risk

Based on investigations carried out, it was revealed that drug traffickers were using the Gambling Sector to justify funds which were suspected of being derived from illicit activities. This has become a common trend of defence provided to LEAs whenever these persons are questioned about the source of funds for the acquisitions of properties or money secured from their house. Several cases were detected relating to drug traffickers. In 75% of the cases involving drug traffickers, they used the defence that the funds represented gains from betting.

Criminals also used the horseracing sector to justify their source of funds when providing defence to LEAs.

One of the preferred methods used by criminals to link tainted funds to gambling activities in casinos was through the use of split transactions. Moreover, the proceeds generated from fraud and drug related offences were often placed in betting activities. There were also instances where perpetrators laundered their proceeds through illegal betting to circumvent the vigilance of authorities. Credit betting has become the new modus operandi of illegal bookmakers thus rendering their activities opaquer. The MPF has conducted investigations into several cases of illegal betting for horseracing with the predicate offence as carrying on activity without licence in breach of the GRA Act. This trend indicated an increase in such illegal activities by unlicensed bookmakers where credit betting was placed through mobile phone. In light thereof, the associated ML threat was rated as **High**.

The GRA was established in December 2007 following the enactment of the GRA Act. The GRA is administered and managed by the Gambling Regulatory Board as per section 5 of the GRA Act. The mandate of the GRA encompasses the regulation of gambling activities as well as ensuring that gambling is conducted in a fair and transparent manner.

Pursuant to Part II of the First Schedule of the FIAMLA, 80 operators of the gambling industry have an obligation to comply with the Act as well as any regulations made, or any guidelines issued under the Act. However, inclusive of the 80 operators, there are only 4 casinos and 21 Gaming House 'A' operators which conduct activities as prescribed under the FATF

requirements; hence they are considered as reporting persons, falling under the AML/CFT regulatory and supervisory purview of GRA.

Conclusion

Considering ML threat which was rated as **High** and ML vulnerability level, which was rated as **Medium**, the ML risk was assessed as **Medium-High**.

TF Risks

Casinos and Gaming House 'A' operators perform UN Sanctions screening of punters at entry (of the premises) and at cashier level. Although, gambling/betting may be an attractive means for raising funds for TF purposes by sympathisers or persons embracing terrorist ideologies, to date, there have been no reported instances where the Mauritian gambling sector has been misused/abused for TF purposes.

There also was no information that individuals from Mauritius had tried to use online gaming platforms/websites in other jurisdictions for TF purposes.

Conclusion

Given that the TF Threat associated with the gambling sector was considered as **Low** and the vulnerability level of the sector to TF was rated as **Medium-Low**, the TF risk for the gambling sector was therefore assessed as **Medium-Low**.

E. Real Estate Sector

SUMMARY OF FINDINGS:

The real estate sector of Mauritius is globally attractive but poses risks of illicit property acquisitions by criminals and terrorists through intermediaries.

The real estate sector faces a **Medium-High** ML risk, with criminals using fraud, embezzlement, and drug proceeds to acquire properties and obscure illicit funds. Investigations revealed cases of investment fraud funds being channelled into Mauritian real estate. The TF risk was rated **Medium-Low**, with no evidence of the sector being exploited for terrorism financing.

Mauritius has a dynamic real estate sector, which is attractive to clients worldwide. There is a threat that criminals from high-risk countries, including terrorists, may acquire property through third parties/intermediaries, to move and store terrorism related funds. However, the sector is subject to a host of control measures. For instance, notaries have obligations under FIAMLA, requiring them to perform their risk assessments, CDD and EDD, and monitor their transactions, amongst others. Records of the transaction are also required to be maintained and screening under the UN sanctions list is, therefore, mandatory. Likewise, high-value transactions and high-risk customers should be closely monitored. The Real Estate sector's contribution to Mauritius GDP was on average 5.2% from the years 2019 to 2022.

ML Risk

Real Estate Agents, Land Promoters and Property Developers are regulated for AML purposes under the FIAMLA, and the FIU is the AML/CFT supervisor for this sector. The services provided in the Real Estate Sector have not materially changed since the NRA (2019).

There are around 418 Real Estate Operators which fall under the AML/CFT requirements in terms of the prescribed activities.

In most investigations, it was revealed that the most common modus operandi used in the real estate activity by perpetrators was through proceeds derived from offences like swindling, forgery, embezzlement, larceny, making use of forged documents, and drug dealing as predicate offences to ML. Cases investigated highlighted that the perpetrators lured their victims through social media or impersonate themselves as a real estate dealer or businessman by employing fraudulent pretences to establish the belief of the existence of a fictitious operation and subsequently, obtained the remittance of funds.

Another common typology noted was that the suspects embezzled funds from companies where they were working and transferred funds to their personal bank accounts as well as that of their close relatives. These funds were then used to acquire properties. These properties were mainly land and then construction was initiated using the tainted funds.

It was revealed from investigations that drug traffickers may finance the acquisition of bare land through loans from banks and thereafter finance the construction of luxury buildings. These loans were serviced from cash intensive business proceeds, where illegal proceeds were comingled with legitimate proceeds in order to obfuscate the trail.

It was further observed that the real estate sector deals a lot with foreign clients and that the big players were those involved with clients carrying higher risks. With the advent of the AML/CFT (Miscellaneous Provisions) Act in July 2020, real estate transactions in cash were no longer allowed (previously cash transactions below USD 12,000 were allowed). Additionally, transactions "Hors Vue du Notaire" were no longer allowed. As a result, all buying and selling transactions related to real estate have to be done through the account of a notary, who is a reporting person. However, investigation also revealed that foreigners had, in the past, acquired properties in Mauritius, which were allegedly financed by proceeds of criminal activity (which was investment fraud committed abroad), and the proceeds channelled to Mauritius in the bank account of legal person as investment.

Conclusion

Given that the threat in this sector is existent, both at national and international levels, the level of ML threat in this sector was assessed as **Medium,** while the ML Vulnerability level of the Real Estate sector was determined as **High**. Consequently, the ML risk was rated as **Medium-High**.

TF Risk

As at date, there were no domestic or international intelligence pointing towards the use of the Mauritian real estate sector for TF purposes. There was also no evidence linking the real estate sector investments with any terrorist groups/financiers.

Conclusion

The TF Threat associated with the real estate sector was rated as **Low** while the TF vulnerability level was assessed as **Medium**. Hence the TF risk was rated as **Medium-Low**.

F. Accountancy Sector

SUMMARY OF FINDINGS:

The ML risk in the accountancy sector was rated **Medium**, with TCSP services posing the highest risk, enabling money laundering, asset concealment, and fund movement to secrecy jurisdictions. Accountants were found to set up complex structures, act as nominees, and manage cash-intensive businesses linked to drug traffickers. While ML cases involving accountants have decreased since 2019, risks remain, particularly in fraud, corruption, and tax evasion. TF risk was rated **Low**, with no reported cases or suspicious transactions.

The MIPA acts as an umbrella professional body for Professional and Public Accountants who are members of Professional Accountancy Institutes and Associations specified in or contemplated by the Financial Reporting Act 2004. There were around 71 accountancy firms which conducted prescribed activities as defined by FIAMLA and were hence under the AML/CFT regulatory purview of MIPA. Based on the recent questionnaires sent to its licensees in September 2024, the number of reported persons increased to 114 and were risk rated as follows in **Table 16**:

Table 16: Accountancy Sector

Risk Category	No of firms
High Risk	2
Medium Risk	7
Low Risk	105

ML Risk

TCSPs, Company formation and associated TCSP services[36] continue to be the ML highest risk services provided by accountants. These can enable the laundering of millions of funds, conceal the ownership of criminal assets, and facilitate the movement of money to secrecy jurisdictions. Company formation as a standalone service offers less exposure to potential abuse and it is therefore considered lower risk. However, when coupled with other high-risk services provided by them or when dealing with high-risk factors, such as dealing with a third party outside Mauritius, the level of risk increases. However, this section relates solely to the accountancy sector without TCSP, which are licensed by FSC and assessed under TCSP sector.

[36] TSCP as a firm or sole practitioner which by way of business, forms companies or other legal persons; acts as or arranges for someone else to act as a company director, partner or nominee shareholder; provides a registered office or business address or similar; and/or acts as or arranges for someone else to act as a trustee for a trust or similar arrangement. The provision of TCSP services involves various professional service sectors including reporting persons, many of which provide these services as add on services to their core business activity.

The client base of the accountancy sector in Mauritius was diverse. The major groups were domestic clients and companies. A minority of the clients were international PEPs, HNWI, non-resident clients, clients with foreign business, clients that were legal entities and clients obtained through introduced business.

Based on intelligence and cases investigated, it was noted that there were professional accountants who were responsible for setting up complex structures on behalf of their clients. In other cases, professional accountants were reported to act as nominees and as tax representatives. Such services may increase the threat of ML. In most drug related cases, it was observed that drug traffickers had set up several domestic companies to launder their money and they employed accountants to maintain their accounts. The nature of business of these companies was mostly cash intensive businesses such as night clubs, restaurants, and fast-food outlets, among others. The STRs received from professional accountants related mainly to corruption, fraud and tax evasion cases. Further, the trend noted in the number of cases investigated is decreasing and the prosecution and conviction was also low. As such the ML Threat associated with accountants was deemed to be **Medium**.

Conclusion

Considering ML threat, which was rated **Medium** and ML vulnerability level, which was rated **Medium-Low**, the ML risk for accountancy sector was rated **Medium**.

TF Risks

According to international trends, TF Threat associated with the accountancy sector is **Low** as the accountancy services are not attractive to terrorist financiers because of the CDD and KYC requirements[37].

Business associated with accountancy services is mainly domestic. Further, accountants are under the obligation to conduct CDD. During the period under review, there were no STR relating to TF which were filed by professionals in this particular sector. Likewise, there were no TF investigation involving professionals in the accountancy sector or evidence that the sector has been misused for TF purposes. Therefore, the TF Threat associated with the accountancy sector was considered as **Low.**

Conclusion

The TF Threat associated with the accountancy sector was therefore assessed as **Low**. The TF vulnerability level was also as rated **Low** and hence the TF risk for accountants was rated **Low**.

[37] HMT 2020.

13. Looking Ahead: Forthcoming Key Measures

Key Measures

Based on the findings of the second NRA, Mauritius will embark on the development of a comprehensive National AML/CFT strategy with the aim of addressing the identified ML/TF threats and vulnerabilities to safeguard the integrity of the financial system.

The National Action Plan, which will subsequently result from the National Strategy will, where relevant, be adopted at the level of all competent authorities and be supported by the necessary resources to ensure implementation of the risk mitigation measures.

Furthermore, to provide a regular update to both the private sector and the public regarding ML and TF risks, committees will be set up to ensure a more regular and dynamic process of assessing ML and TF risks including emerging risks.

Forthcoming Initiatives and Measures

The anticipated initiatives and measures that will shape the AML/CFT landscape in Mauritius are as follows:

(i) Establishing a Centralised Database

Mauritius is in the process of implementing a Centralised Information Management System for AML/CFT/CPF at national level. The system will assist Mauritius in maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of its AML/CFT/CPF regime.

The systematic collection, compilation and maintenance of quantitative data will ensure that comprehensive statistics/data related to AML/CFT/CPF are readily available at national level for the swift conduct of risk assessments. Further, this database will also benefit stakeholders when reporting progress to international and regional bodies as well as for the next mutual evaluation exercise for Mauritius.

(ii) Mid-Term Independent Assessment

Mauritius is currently undertaking a mid-term independent assessment to evaluate the technical compliance and effectiveness of its AML/CFT/CPF Framework with respect to the revised FATF Methodology. This proactive review aims at identifying deficiencies and implementing corrective measures ahead of the next Mutual Evaluation exercise.

(iii) Conducting other Risk Assessment exercises

In order to complement this NRA, Mauritius is also undertaking the Risk Assessment of Legal persons and Legal Arrangements using the World Bank Methodology. To further strengthen its AML/CFT regime, Mauritius will embark on a number of risk assessments, including: its first PF risk assessment, as well as the review of ML/TF Risk related to the misuse of VAs/VASPs, and TF risks linked to NPOs.

Annex 1: Establishment of the NRAWG

In accordance with the World Bank model, Mauritius established an NRAWG composed of all AML/CFT related stakeholders in Mauritius. The different teams forming part of the NRAWG is outlined in Table 17.

Table 17: Composition of the NRAWG

SN	Team	Sub- Team	Team Leader(s)	Participants by Institutions
1.	Threat Assessment Team	ML Threat Assessment Team	▪ Ex- Independent Commission Against Corruption ▪ University of Mauritius	▪ National Security Services ▪ Mauritius Police Force ▪ Financial Intelligence Unit ▪ Office of Director of Public Prosecutions ▪ Attorney General's Office ▪ Mauritius Revenue Authority – Tax ▪ Mauritius Revenue Authority – Customs ▪ Ex- Integrity Reporting Services Agency ▪ Ex- Asset Recovery Investigation Division ▪ Ministry of Foreign Affairs, Regional Integration and International Trade ▪ Bank of Mauritius
		TF Threat Assessment Team	▪ Counter Terrorism Unit ▪ Mauritius Police Force ▪ Financial Intelligence Unit	▪ Office of Director of Public Prosecutions ▪ Attorney General's Office ▪ Mauritius Revenue Authority – Customs ▪ Bank of Mauritius ▪ National Security Services ▪ CFT Cell (Mauritius Police Force) ▪ Registrar of Associations ▪ National Sanctions Secretariat

				▪ Financial Services Commission ▪ Registrar of Companies
2.	National Vulnerability Team (Both ML/TF)		▪ Ex-Integrity Services Reporting Agency ▪ Office of Director of Public Prosecutions	▪ Ex- Independent Commission Against Corruption ▪ Mauritius Police Force ▪ Financial Intelligence Unit ▪ Attorney General's Office ▪ Mauritius Revenue Authority – Tax ▪ Mauritius Revenue Authority – Customs ▪ University of Mauritius ▪ Registrar of Companies ▪ National Sanctions Secretariat ▪ Financial Services Commission ▪ National Security Service ▪ CFT Cell (Mauritius Police Force) ▪ National Audit Office ▪ Registrar of Associations ▪ Ex- Asset Recovery Investigation Division ▪ Counter Terrorism Unit ▪ Passport and Immigration Office
3.	Banking Sector vulnerability assessment Team (Both ML/TF)		▪ Bank of Mauritius	▪ Financial Intelligence Unit ▪ Private sector representatives

4.	Insurance Sector vulnerability assessment Team (Both ML/TF)		▪ Financial Services Commission	▪ Financial Intelligence Unit ▪ Private Sector Representatives
5.	Securities Sector vulnerability assessment Team (Both ML/TF)		▪ Financial Services Commission	▪ Financial Intelligence Unit ▪ Private sector representatives
6.	Other Financial Institution (OFI) Sector Vulnerability assessment team (Both ML/TF)	OFIs under Supervision of BoM	▪ Bank of Mauritius	▪ Financial Intelligence Unit ▪ Private sector representatives
		Payment Service Providers	▪ Bank of Mauritius	▪ Financial Intelligence Unit ▪ Private sector representatives
		OFIs under FSC Supervision	▪ Financial Services Commission	▪ Financial Intelligence Unit ▪ Private sector representatives
		Cooperative Credit Unions	▪ Registrar of Cooperatives	▪ Financial Intelligence Unit ▪ Private sector representatives
7.	Trust and Company Service Providers Vulnerability Assessment Team (Both ML/TF)		▪ Financial Services Commission	▪ Financial Intelligence Unit ▪ Private Sector representatives
8.	Company Service Providers Vulnerability Assessment Team (Both ML/TF)		▪ Registrar of Companies	▪ Financial Intelligence Unit ▪ Private Sector representatives

9.	Designated Non-Financial Businesses and Professions Sector Vulnerability Assessment Team (Both ML/TF)		▪ Attorney General's Office ▪ Mauritius Institute of Professional Accountants	▪ Financial Intelligence Unit ▪ Assay Office ▪ Gambling Regulatory Authority ▪ Mauritius Revenue Authority ▪ University of Mauritius ▪ Financial Reporting Council ▪ Private sector representatives

Annex 2: Measures taken by Mauritius

1. AML/CFT Measures implemented by Mauritius since 2019

Over the last 5 years, Mauritius has revamped its AML/CFT infrastructure to adhere to the highest international standards in the combat against ML and TF. This has resulted in enormous strides in addressing the technical compliance deficiencies and improving the level of effectiveness of the regime.

In its Mutual Evaluation 2018, Mauritius was rated 'Compliant' or 'Largely Compliant' with only 14 out of 40 recommendations and showed low to moderate effectiveness across all 11 Immediate Outcomes. In response, Mauritius brought significant changes to its AML/CFT/CPF framework.

Furthermore, based on the findings of the first NRA, Mauritius developed a National AML/CFT Strategy 2019-2022 to address the ML/TF risks as well as the feedback received from the Mutual Evaluation Report 2018. It also contained a strategy for maintaining an ongoing dialogue with relevant private sector stakeholders to ensure effective implementation of AML/CFT requirements. The National Strategy comprised of eight core themes which aimed at enhancing the ability of Mauritius to detect and deter ML and TF. A snapshot of the eight core strategic themes and progress made to date with respect in each area are set out in Table 18.

Table 18: Eight Core Strategic Themes

SN	Strategic Theme	Details	Status
1	Strengthening the AML/CFT Legal and Regulatory Framework	The AML/CFT Framework was revamped since May 2019, through the enactment of several pieces of legislation such that Mauritius is currently rated 'Compliant' or 'Largely Compliance' with all the 40 FATF Recommendations. The Anti- Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Acts 2019 and 2020 were enacted to address various gaps identified in the Mutual Evaluation Report and the NRA.	Addressed
2	Implementing a comprehensive risk-based supervision framework	All supervisors have developed and implemented a risk-based supervisory framework to supervise their respective sectors.	Addressed

		A comprehensive legislative framework and supervisory infrastructure for AML/CFT was established for DNFBPs since May 2019 and August 2020, respectively. The DNFBPs supervisors are also conducting numerous outreach activities to convey supervisory expectations to their reporting persons and to educate them on their AML/CFT obligations, including on obligations to file STRs. TFS are factored in on a regular basis in supervisory outreach programmes and are continuously integrated in the scope of AML/CFT on-site inspections.	
3	Strengthening the process by which the ML/TF threats are detected and disrupted, criminals are prosecuted, and illegal proceeds are confiscated	Parallel financial investigations are being conducted and a framework for confiscation of illicit assets has been established.	Addressed
4	Enhancing national co-ordination and cooperation	Several committees such as the Core Group which has been entrenched in the law, 11 Immediate Outcome Sub-Committee, National Sanctions Committee, ICC and AML/CFT Coordination Task Force were established/ enhanced since 2018 while the mandate of the National Committee on AML/CFT was reinforced	Addressed
5	Consolidating capacity building, training and awareness raising programs	From January 2020 to June 2022, around 61 capacity building and training were provided to competent authorities involved in AML/CFT matters.	Addressed
6	Enhancing transparency of legal persons and arrangements	A Registry for Beneficial Ownership information has been put in place by the Corporate Business Registration	Addressed

		Department and has been made available to competent authorities in real time A process has been established which includes a range of controls devised to ensure that beneficial ownership information remains accurate and up to date.	
7	Implementing an effective AML/CFT data collection system	Up to date statistic using the ESAAMLG format is requested from competent authority and kept at the Ministry of Financial Services and Economic Planning level. However, this is being done on a manual basis. The Ministry of Financial Services and Economic Planning is in the process of implementing a Centralised Information Management System for AML/CFT/CPF at national level. The system will assist Mauritius in maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of its AML/CFT/CPF regime.	In progress
8	Enhancing regional and international cooperation	There has been the implementation of a structured system to ensure timely processing of MLA extradition requests and amendments have been brought to legislations to enable supervisory and other competent authorities to share AML/CFT related information with their foreign counterparts.	Addressed

Within a year of implementing the National Strategy and National Action Plan, Mauritius improved its compliance to 35 out of 40 FATF Recommendations and addressed the majority of the Recommended Actions outlined in its MER. Despite this progress, due to remaining strategic deficiencies, in February 2020 the FATF placed Mauritius on its list of 'Jurisdictions under Increased Monitoring,' and was conferred with a two-year action plan to address same in its AML/CFT regime under the International Co-operation Review Group (ICRG) process.

Following progress made at its October 2021 Plenary, the FATF concluded that Mauritius would no longer be subject to increased monitoring by the FATF. The FATF concluded that Mauritius had made significant progress in improving its AML/CFT regime. Mauritius had strengthened its AML/CFT regime and addressed the strategic deficiencies that the FATF identified in February 2020. Mauritius was therefore no longer subject to the FATF's increased monitoring process.

In 2021, with the enactment of the VAITOS Act, an Addendum to the National Strategy was undertaken to incorporate strategies that address the identified risks associated with VAs and VASPs following a risk assessment exercise.

In order to sustain and further reinforce the jurisdiction's AML/CFT/CPF framework, recent reforms undertaken by the Government are as follows:

(i) Establishing the Financial Crimes Commission

On 29th March 2024, the FCC Act 2023 was proclaimed. Accordingly, the FCC was established which is now the apex agency in Mauritius to detect, investigate, and prosecute financial crimes and any other ancillary offence connected thereto. The FCC is responsible for asset recovery in Mauritius. It also targets unexplained wealth and is the depository of all declarations made under the Declaration of Assets Act. More details are at item 6-(Establishment of the FCC).

(ii) Enacting the AML/CFT Miscellaneous Provision Act 2024

On 25 July 2024, the AML/CFT (Miscellaneous Provisions) Act was enacted, which brought changes to 16 pieces of existing legislation with a view to meet international standards on AML/CFT/CPF by ensuring the laws reflect revisions made to FATF recommendations and reinforcing the AML/CFT framework so as it remains resilient against evolving ML/TF risks.

(iii) Conduct of an in-person Assessors Training

From 27 to 31 May 2024, an in-person Assessor Training was conducted by the ESAAMLG in Mauritius. The aim of the training was to empower our officers involved in AML/CFT matters with an in-depth understanding of the FATF Recommendations and the FATF methodology for assessing compliance and effectiveness.

2. Our ICRG Journey

To address the deficiencies in the MER 2018, Mauritius has undertaken significant reforms, including the adoption of a comprehensive National AML/CFT Strategy and Action Plan, which improved its compliance rating to 'Compliant' or 'Largely Compliant' with 35 of the 40 FATF Recommendations and addressing 53 of the 58 recommended actions from the MER.

As noted previously, in February 2020, despite significant progress, Mauritius was placed on the FATF's list of "Jurisdictions under Increased Monitoring" due to strategic shortcomings.

The FATF highlighted that since the completion of its MER in 2018, Mauritius has made progress on a number of its MER Recommended Actions to improve technical compliance and effectiveness, including amending the legal framework to require legal persons and legal arrangements to disclose of beneficial ownership information and improving the processes of identifying and confiscating proceeds of crimes.

The FATF identified 5 priority areas where Mauritius had to develop action plans, namely: (1) demonstrating that the supervisors of its global business sector and DNFBPs implement risk-based supervision; (2) ensuring the access to accurate basic and beneficial ownership information by competent authorities in a timely manner; (3) demonstrating that LEAs have capacity to conduct ML investigations, including parallel financial investigations and complex cases; (4) implementing a risk based approach for supervision of its NPO sector to prevent abuse for TF purposes; and (5) demonstrating the adequate implementation of TFS through outreach and supervision.

In February 2020, Mauritius made a high-level political commitment to work with the FATF and ESAAMLG to strengthen the effectiveness of its AML/CFT regime.

Over several FATF Plenary meetings, Mauritius submitted four progress reports detailing its actions taken to address those strategic deficiencies. These actions related to changes in its legislative, institutional, and regulatory and supervisory framework, amongst others. By June 2021, the FATF determined that Mauritius had substantially completed its action plan.

In October 2021, the FATF removed Mauritius from the grey list, acknowledging its significant progress in enhancing its AML/CFT regime. Consequently, Mauritius exited the UK's and EU's lists of high-risk third countries in November 2021 and March 2022, respectively.

Since its delisting, Mauritius has continued to improve its AML/CFT framework, particularly in regulating VAs and initial token offerings, in alignment with international standards. These efforts resulted in a 'Largely Compliant' rating for FATF Recommendation 15 on New Technologies in the September 2022 ESAAMLG meetings, placing Mauritius among the top-tier jurisdictions 'Compliant' or 'Largely Compliant' with all 40 FATF Recommendations.

3. Reinforcing AML/CFT Coordination Mechanism

In order to ensure effective implementation and oversight of AML/CFT matters and to enhance Coordination of AML/CFT measures, Mauritius established several committees as follows:

(a) Inter- Ministerial Committee

An Inter-Ministerial Committee chaired by the Prime Minister was set up which considers the recommendations of the Core Group and fosters effective implementation of strategic priorities. The members are the Honourable Prime Minister, the Minister of Finance, the Minister of Financial Services and Economic Planning, and the Attorney General.

(b) Core Group

A Core Group for AML/CFT/CPF was set up and conferred with legal status under the FIAMLA through the Finance (Miscellaneous Provisions) Act. The Core Group is chaired by the Financial Secretary and co-chaired by the Director General of the ICAC (now FCC) and the Governor of the BoM. The functions of the Core Group are, inter-alia, as follows:

- ensure the effective implementation, by the relevant competent authorities, of the FATF international standards on AML/CFT;
- make recommendations to the Prime Minister on matters, including implementation, strategy and international developments, pertaining to AML/CFT;

- decide on matters pertaining to the implementation of AML/CFT standards which a relevant competent authority may refer to it; and
- ensure effective coordination and cooperation with the National Committee and among all competent authorities.

(c) National Committee for AML/CFT

The National Committee coordinates the development, regular review and implementation of national policies and activities to combat ML, TF and PF.

(d) IO Sub-Committees set up under the National Committee for AML/CFT

11 IO Sub-Committees were set up to enhance institutional, technical and operational coordination in order to ensure Mauritius implemented an effective AML/CFT system which met international standards. The IO Sub-Committees meet on a regular basis and also report to the National Committee on the progress made under different IOs.

(e) AML/CFT Coordination Task Force

The Task Force is headed by the Office of Director of Public Prosecutions (ODPP) and ensure that both ML and TF cases are comprehensively investigated (including through parallel financial investigation). Investigations are now 'prosecution-led' providing investigators with timely access to legal advice and guidance in ML and TF cases.

(f) Interagency Coordination Committee (ICC)

Following the signature of a MOC in August 2020, an Interagency Coordination Committee (ICC), regrouping all AML/CFT supervisors and regulators, was established. This has proven to be an effective platform to continuously improve the AML/CFT supervisory effectiveness in different areas, notably, in pulling resources together to conduct joint training for the benefit of supervisors and outreach sessions for the industry.

(g) Other Committees include:

(i) AML/CFT Statistics Committee to coordinate and harmonise collection of AML/CFT Statistics by all relevant authorities;

(ii) Observatory Committee of Virtual Assets Activities to identify trends and patterns of VA transactions/activities, track unlicensed VASPs, and detect illegal activities within the VA ecosystem of Mauritius; and

(iii) National Sanctions Committee to promote and coordinate the implementation of UNSCR.

4. Increase in International Cooperation

Mauritius has, in various instances, also provided assistance to other jurisdictions for investigation of illicit funds. Mauritius participates in the global effort to combat ML and TF, and mechanisms are in place for providing assistance to other jurisdictions, including MLA, financial intelligence exchange, and co-operation amongst law enforcement and supervisors.

More specifically, in order to promote international cooperation, the following measures have been implemented:

- Introduction of a database in 2019 by the AGO, which tracks detailed information on incoming and outgoing MLA and extradition requests, such as dates, types of offences, assistance sought, and case progress which ensures timely updates and urgent processing of MLA requests;
- Introduction of feedback forms by the AGO in 2020 to help in evaluating the outcomes of MLA assistance provided and received. The Ministry of Foreign Affairs also processes requests within 48 hours, coordinating closely with the AGO and maintaining an Excel database to track requests; and
- Amendments of legislations to enable supervisory and other competent authorities to share AML/CFT related information with their foreign counterparts.

Legislative amendments have enabled competent authorities to take a proactive approach to both formal and informal international cooperation and are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes. The measures undertaken have led to an increase in information exchanges with foreign counterparts, as well as an increase in the number of outgoing and incoming MLAs requests. Furthermore, Mauritius has a central register of beneficial ownership which enables it to share information with other authorities.

Moreover, Mauritius has been assigned an overall rating of 'Compliant' by the Global Forum on Transparency and Exchange of Information for Tax Purposes during the second round of Exchange of Information on Request reviews which reflects its commitment to the highest standards of tax transparency and information exchange.

5. Beneficial Ownership Registry

As of 15 May 2020, the Registrar of Companies maintains registers of beneficial ownership information for legal persons.

In addition to establishment of a beneficial ownership register, Mauritius has implemented several legislative reforms to enhance transparency and disclosure of beneficial ownership.

These amendments include, amongst others, redefining beneficial ownership and UBOs as natural persons with direct or indirect control and mandated the ROC to disclose beneficial ownership information to competent authorities in specific circumstances, such as during investigations.

Furthermore, basic information about legal persons has always been public.

Revisions were also made to the laws to impose sanctions for non-disclosure of beneficial ownership information.

6. Establishment of the FCC

The FCC was established under the FCC Act 2023 which came into operation on 29 March 2024. Consequently, the POCA, the Asset Recovery Act, the Good Governance and Integrity Reporting Act and Part II of the FIAMLA were repealed.

In line with the object of the FCC Act, the FCC is now the apex agency in Mauritius to detect, investigate and prosecute financial crimes such as corruption, ML, fraud, the financing of drug dealing and any other ancillary offence connected thereto. The FCC is responsible for asset recovery in Mauritius. It also targets unexplained wealth and is the depository of all declarations made under the Declaration of Assets Act.

The new legal framework enables a holistic approach to fight financial crimes, including through coordination mechanisms between relevant agencies as well as the conduct of parallel investigations. In addition, the range of sanctions under the FCC Act has been expanded such that a convicted person may be subject not only to the penalty for the said offence but also to other sanctions.

National Coordination Committee

The FCC Act provides for the establishment of a National Coordination Committee which is chaired by the Director-General of the FCC and comprises the Solicitor-General, Director of Public Prosecutions, the Commissioner of Police, the Governor of the BoM, the Chief Executive of the FSC, the Chief Executive Officer of the GRA, and the Director of the FIU as members.

The National Coordination Committee shall, for the purpose of combatting financial crimes, inter alia:

(a) ensure effective coordination and collaboration regarding criminal investigations with investigatory authorities and supervisory authorities in relation to parallel and complex cases, and assist in overcoming any challenges;

(b) harness intelligence and capabilities from across different sectors, including the private sector, to tackle financial crimes;

(c) develop strategic oversight to enable agencies involved in the fight against financial crimes to prioritise activity better, drive performance and align funding and capability;

(d) jointly identify and prioritise the most appropriate type of enquiries, whether criminal or regulatory, to ensure maximum impact; and

(e) organise and coordinate training needs for its members, the investigatory authorities or any other relevant authorities.

Public-Private Partnership Task Force

The FCC Act further provides for the establishment of a Public-Private Partnership Task Force which consist of the Director-General of the FCC as chairperson, the Director of the Investigation Division, the Director of the Asset Recovery and Management Division, a representative from the MPF, FIU, BoM, FSC, Business Mauritius, MRA, Mauritius Bankers' Association, a relevant insurance company, and 3 other members from the private sector, to be appointed by the Prime Minister.

The Public-Private Partnership Task Force shall:

(a) be responsible to develop and promote cooperation between the public and private sector in combatting financial crimes;

(b) strengthen the fight against financial crimes with the collaboration and partnership of the public and private sectors; and

(c) enhance collaboration and sharing of information by its members to assist the FCC in financial crimes investigation and prosecution.

Membership of International Organisations and participation in Regional Projects

Mauritius is a member of several regional and international bodies such as the UN, the Commonwealth of Nations, AU, COMESA, SADC, ARINSA, Egmont Group of FIUs, IOSCO, OECD Bribery Working Group, and ESAAMLG.

Following the progress made by Mauritius, the jurisdiction has moved from a recipient of technical assistance to a privileged partner in sharing its experience gained and lessons learned to tackle illicit financial flows. To this end, assistance was provided amongst others to Panama, Madagascar, Bangladesh, Tunisia, Jordan, South Africa, Seychelles, Zambia, the Democratic Republic of Congo, Djibouti, Namibia, UAE, Angola, Cote D'Ivoire, and Uganda.

Additionally, Mauritius has actively participated in ESAAMLG Projects, including, amongst others, the development of a toolkit for assessing ML and TF risks by legal entities, a project on Regional TF Risk Assessment, and a survey on the impact of Fintech products like VAs on inclusive financial integrity in the ESAAMLG Region.

Annex 3: Prescribed Activities under the Financial Intelligence and Anti-Money Laundering Act

Table 19: Activities under the FIAMLA

Designated Non-Financial Businesses and Professions	Transactions	AML/CFT Supervisory Authority
Law firm, foreign law firm, joint law venture, foreign lawyer, under the Law Practitioners Act Attorney Barrister Notary	A barrister, an attorney, a notary, a law firm, a foreign law firm, a joint law venture, a foreign lawyer under the Law Practitioners Act, and a professional accountant, a public accountant and a member firm licensed under the Financial Reporting Act, who prepares for, or carries out, transactions for his client concerning the following activities – (i) buying, selling or rental of real estate; (ii) managing of client money, securities or other assets; (iii) management of bank, savings or securities accounts; (iv) organisation of contributions for the creation, operation or management of legal persons such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; (v) creating, operating or management of legal persons such as a company, a foundation, an association, a limited liability partnership or such other entity as may be prescribed, or legal arrangements, and buying and selling of business entities; (vi) the business activities of VASPs and issuers of initial token offerings under the VAITOS Act; or	Financial Intelligence Unit
Professional accountant, and public accountant under the Financial Reporting Act only where they are sole practitioners, partners or employed professionals within member firms. Member firms under the FIAMLA, namely, a person registered under section 54 of the Financial Reporting Act, other than an audit firm registered under section 35 of the Act.		Mauritius Institute of Professional Accountants

	(vii) preparing, or carrying out, transactions for a client concerning the following activities – a. acting as a formation agent of a legal person with a view to assisting another person to incorporate, register or set up, as the case may be, a company, a foundation, a limited liability partnership or such other entity as may be prescribed; b. acting, or causing another person to act, as a director, as a secretary, as a partner or in any other similar position, as the case may be, of a legal person such as a company, foundation, a limited liability partnership or such other entity as may be prescribed; c. providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; or d. acting, or causing for another person to act, as a nominee shareholder for another person.	

-

Dealer in jewellery, precious stones or precious metals, namely (a) a person who deals in jewellery, precious stones or precious metals; and (b) including a person who – (i) manufactures, processes, buys, sells, imports or exports jewellery, or supplies jewellery for sale; (ii) processes, buys, sells or imports precious metals, or exports melted precious metals; or (iii) processes, buys, sells or imports precious stones.	A dealer in jewellery, precious stones or precious metals who engages in any transaction of at least 500,000 rupees in total, whether the transaction is executed in a single operation or in several operations which appear to be linked.	Financial Intelligence Unit
Real Estate Agents, including Land Promoters and Property Developers (in so far as it relates to AML/CFT under the FIAMLA or under any other relevant enactment)	(a) a real estate agent where he is involved in real estate transactions concerning the sale, exchange, purchase or lease of real estate for a client; (b) a land promoter and property developer who, in the course of a business, is involved in real estate transactions concerning the sale, exchange, purchase or lease of real estate.	Financial Intelligence Unit

Person licensed to operate a casino, a hotel casino, as a horse racing organiser, the Mauritius National Lottery, a limited payout machine, a sweepstake, as a local pool promoter, as the agent of a local pool promoter, a gaming house, a gaming machine, as a totalisator, as a bookmaker and interactive gambling under the Gambling Regulatory Authority Act.	(a) a person licensed, under the Gambling Regulatory Authority Act, to operate a casino, hotel casino, limited payout machine, sweepstake, gaming house, gaming machine, where any of his customers engages in, on any given date, a total cumulative financial transaction equal to or above 20,000 rupees or an equivalent amount in foreign currency; (b) a totalisator, a bookmaker, a local pool promoter, the agent of a foreign pool promoter and pool collector, under the Gambling Regulatory Authority Act, where any of his customers engages in, on any given date, a total cumulative financial transaction equal to or above 20,000 rupees or an equivalent amount in foreign currency.	Gambling Regulatory Authority
Company Service Providers (a) a person, registered under section 164 or 167A of the Companies Act, that provides any of the services specified in section 167A of that Act; but (b) does not include – (i) a barrister, an attorney or a notary, or a law firm, foreign law firm, joint venture or foreign lawyer under the Law Practitioners Act;	A company service provider who prepares, or carries out, transactions for a client concerning the following activities – (i) acting as a formation agent of a legal person with a view to assisting another person to incorporate, register or set up, as the case may be, a company, a foundation, a limited liability partnership or such other entity as may be prescribed; (ii) acting, or causing another person to act, as a director, as a secretary, as a partner or in any other similar position, as the case may be, of a legal person such as a company, foundation, a limited liability partnership or such other entity as may be prescribed;	Registrar of Companies

(ii) a professional accountant, public accountant and member firm under the Financial Reporting Act; and (iii) the holder of a management licence under section 77 of the Financial Services Act.	(iii) providing a registered office, a business address or an accommodation, a correspondence or an administrative address for a legal person such as a company, a foundation, a limited liability partnership or such other entity as may be prescribed; or (iv) acting, or causing for another person to act, as a nominee shareholder for another person.	

Ministry of Financial Services and Economic Planning
Level 14, SICOM Tower
Wall Street, Cybercity, Ebene
Republic of Mauritius
Tel: 404-2400
E-mail: financialservices@govmu.org
Website: https://financialservices.govmu.org