

FINDINGS OF THE MAURITIUS SECOND MONEY LAUNDERING AND TERRORIST FINANCING NATIONAL RISK ASSESSMENT

Ministry of Financial Services and Economic Planning

Venue: Financial Services Commission House, Ebene

Date: 07.05.25

Mr Amit Bhushan Sunkoorah

Team Member
ML Threat Assessment Team



MONEY LAUNDERING THREATS IN MAURITIUS

MONEY LAUNDERING CASES IN MAURITIUS

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

Institutional arrangements:

ICAC and MPF – empowered to investigate Money laundering cases in Mauritius

DOMESTIC MONEY LAUNDERING THREATS

Predicate Offences identified as **HIGH** Money Laundering Threats

ILLICIT TRAFFICKING IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES

- Remained a critical threat to the national security, social stability, and financial integrity of Mauritius

- 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 offenses

- 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

- 650 ML investigations where drug trafficking was alleged to be the predicate offence.
  ML prosecutions and convictions were 98 and 30

FRAUD

- Fraud cases reported for the period under review was 3259
- Total amount of money defrauded through various schemes amounted to USD 57,365,749.44
- Embezzlement, forgery, and electronic fraud generated the most proceeds

ML Investigations

- Out of 3259 fraud case , 230 ML investigations were conducted
- Prosecution and conviction stood at 71 and 22

- Electronic fraud such bogus investment schemes and crypto scams emerged as the highest threats in terms of occurrence, the amount of money involved

    - a total of USD 11,552,274 was defrauded

ILLEGAL BOOKMAKING

- 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

- 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

- Money laundering 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

- New modes payments such as mobile payment systems

Predicate Offences identified as **MEDIUM-HIGH**

Money Laundering Threats

ROBBERY/THEFT (LARCENY)

- 41,118 cases of larceny were investigated
- Proceeds generated by these cases amounted to USD 43,869,641

ML investigations

- 317 larceny ML investigations were initiated by the MPF
- ICAC investigated 11 ML cases with a predicate offence of larceny by a person in receipt of wages.
- 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

CORRUPTION

- ICAC initiated 1,437 corruption investigations
- Total proceeds seized/attached were USD 10,171,699
- Prosecutions and convictions stood at 72 and 48
- Many of these investigations, especially post-COVID, were related to tenders allocated during the pandemic emergency.

<u>ML Investigations</u>

- ML investigations connected to corruption (29 cases during the period under review) revealed a pattern of siphoning government funds through corrupt practices
- Out of the 29 ML cases predicated on corruption, 17 cases were prosecuted

Predicate Offences identified as **MEDIUM** Money Laundering Threats

TAX CRIMES

- Lodged 171 cases at Court during FY 2016/2017 to 2021/2022
- 148 Court decisions for the same period, securing USD 500,473 as the total amount of fines imposed on the court decisions obtained.
- 20 out of 667 tax investigations were referred to prosecution for tax evasion
- Common typologies noted – involvement in drug trafficking

<u>ML Investigations</u>

- Referrals made to LEAs - Outcome of one case led to the taxpayer sentenced to pay the tax fine. Another VAT fraud case will be lodged for prosecution shortly. This case is being prosecuted for money laundering offences.

TRADE-BASED MONEY LAUNDERING (TBML)

- 5,575 cases of under-invoicing
- Additional customs duties and taxes collected were MUR 98,281,201
- cases of double invoicing - resulted in payment of additional duties, taxes and penalties amounting to MUR 3,418,507.

<u>ML Investigations</u>

- Referrals made to ICAC

TRAFFICKING IN HUMAN BEINGS AND MIGRANT SMUGGLING/SEXUAL EXPLOITATION, INCLUDING SEXUAL EXPLOITATION OF CHILDREN

- 4 cases of child exploitation
- 2 cases of human trafficking involving adults
- No ML case associated with this predicate offence

Predicate Offences identified as **MEDIUM-LOW** Money Laundering Threats

ENVIRONMENTAL CRIME- ILLEGAL FISHING

- Two categories namely those committed in the lagoon and those committed in the high seas within the Mauritian Exclusive Economic Zone
- Only one instance of illegal fishing detected

Predicate Offences identified as **LOW** Money Laundering Threats

Trading without Licence, Piracy, Illegal public collection, Extortion and Smuggling

- Small number of reported cases
- Low capacity in terms of sophistication, networks and resources
- Very reduced scope of activity
- Low criminal proceeds
- Very few money laundering cases linked to the predicate offences

EXTERNAL MONEY LAUNDERING THREATS

FRAUD

- Suspected fraud proceeds were received in Mauritius, particularly through global business companies
- 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

CORRUPTION

- 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 money laundering through their involvement in five global business companies
    - 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

TAX EVASION

- Two alleged cases of tax evasion/offences reported from open-source information

- For the period under review, 5 incoming requests having an ML component, were received for MLA which relate to tax crimes and tax evasion as predicate offence

- Several measures taken by MRA

DIRECTION OF ML 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
- 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
- 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

SUMMARY OF SECTORIAL ML THREAT ANALYSIS

High ML Threat

- Banking
- Leasing
- TCSPs
- Gambling

Medium-High ML Threat

- DPMS
- Notary

Medium ML Threat

- Real Estate
- Legal
- Securities
- Cash Dealers
- Payment Intermediary Services
- Accountancy

Medium-Low Threat

- Long-term Insurance
- Motor Insurance
- NBDTIs
- Credit Unions

Low ML Threat

- General Insurance (except Motor Class)
- Credit Finance
- Treasury Management
- Investment Banking
- CSPs
- PSPs

Mr Clifford Frichot

Team Leaders
TF Threat Assessment Team



TERRORIST FINANCING RISKS IN MAURITIUS

NATIONAL TERRORISM FINANCING THREAT

Definition of Terrorist Financing Threat and stages involved in Terrorist Financing

- *A TF threat is a person or group of people (may include both natural and legal persons) with the potential to cause harm by raising, moving, storing or using funds and other assets (whether from legitimate or illegitimate sources) for terrorist purposes. TF threats may include domestic or international terrorist organisations and their facilitators, their funds, as well as past, present and future TF activities, and individuals and populations sympathetic to terrorist organisations.* **[Source: FATF Report on Terrorist Financing Risk Assessment Guidance of July 2019]**

NATIONAL TERRORISM FINANCING THREAT

- Terrorist Threat: LOW
- Global Terrorism Index
    - 2018 to 2024 : Zero Impact of terrorism on Mauritius

- Global Peace Index
    - Year 2024: 22nd globally and 1st in Sub Saharan Africa

NATIONAL TERRORIST FINANCING THREAT

Key Findings

- No terrorist act committed in Mauritius. **However, the absence of terrorist act does not mean that Terrorist Financing activities are not taking place**;
- No known-terrorist person, group and/or organization physically or actively operating in Mauritius.
- No individual has been prosecuted or convicted for terrorist financing in Mauritius .
- No individual or entity has been designated as ‘designated party’ under The United Nations (Financial prohibitions, Arms embargo and Travel Ban) Sanctions Act 2019.
- No Mauritian national travelled to conflict zone to join any terrorist group/organization.

NATIONAL TERRORIST FINANCING THREAT

Key Findings

- There are indications that some individuals were influenced by extremist ideologies and propaganda and the **number has slightly increased during the past years**
- Two distinct modes of TF activities were identified:
  - The cross-border **inflow of funds** by suspected foreign terrorist financiers to a Mauritian embracing ISIS ideologies and
  - Raising and **outward movement of funds** to support Foreign Terrorist Fighters (FTF) through locals, and foreign intermediaries identified as terrorist financiers.

NATIONAL TERRORIST FINANCING THREAT

Key Findings

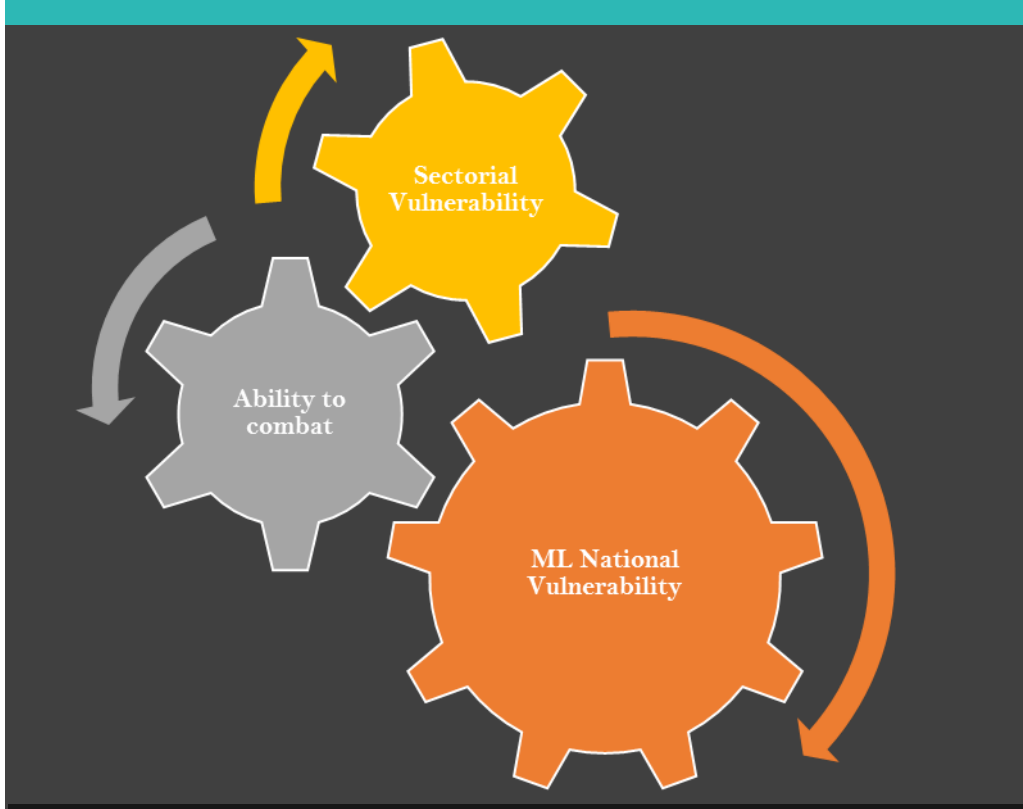
- The sources of suspected terrorist funds transferred to Mauritius to support individuals with ISIS ideologies were not traced;
- The method of raising terrorist funds transferred to Mauritius is not traced;
- The sources of funds transferred from Mauritius for suspected TF purposes were salaries, pensions and donations (Wittingly and Unwittingly);
- Use of technology for raising fund for outward financing: Social Media and crowdfunding were confirmed; Use of virtual asset
- Channels used for transferring funds:
  - Incoming terrorist funds: Money Value Transfer services (MVTS)
  - Outgoing terrorist funds: wire transfers and MVTS

NATIONAL TERRORIST FINANCING THREAT

- National Terrorism Financing Threat rating: **MEDIUM-LOW**

Mrs Preeya Raghoonundun

Team Leader
National Vulnerability Assessment Team

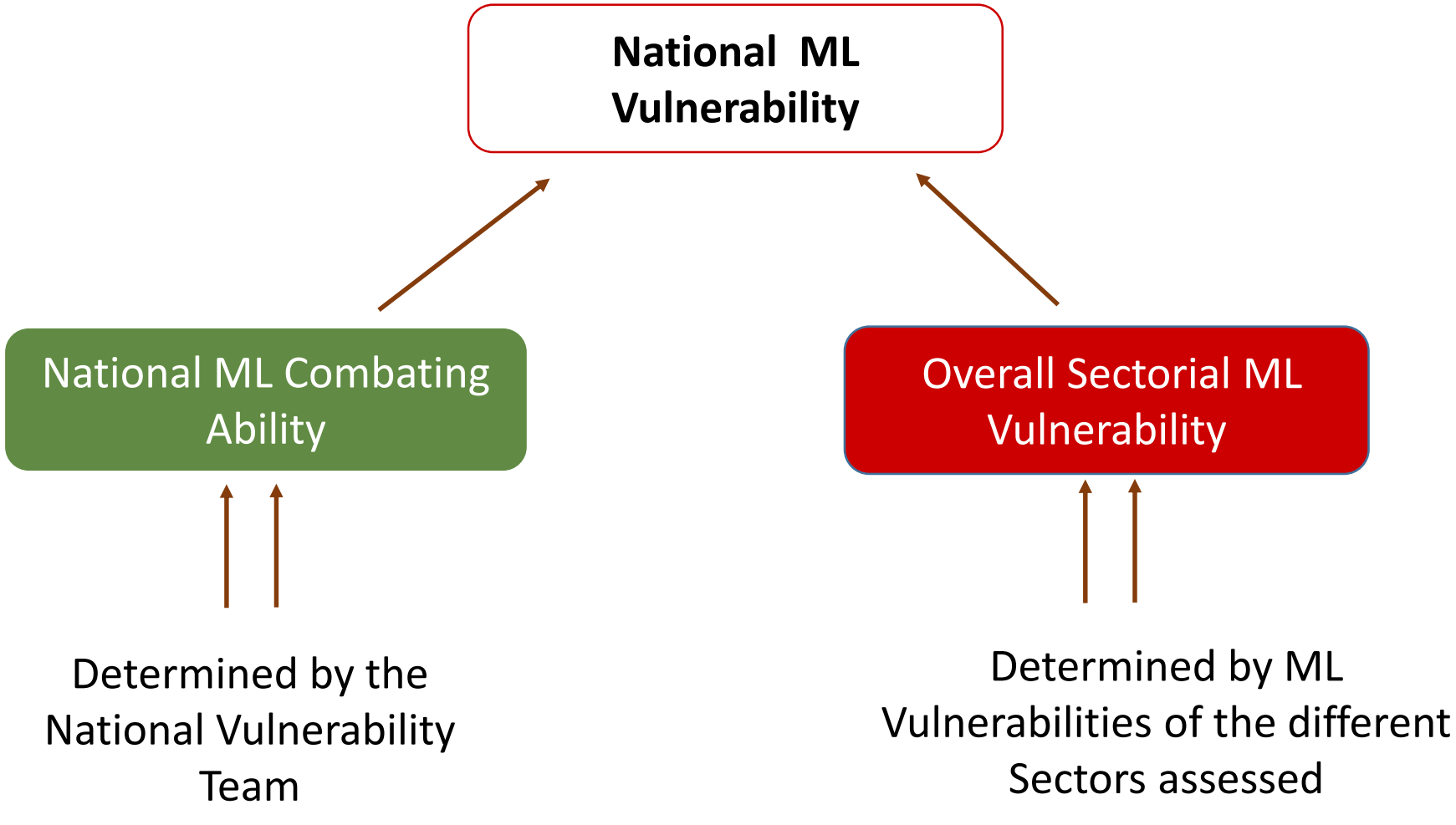


ML NATIONAL VULNERABILITY

NATIONAL ML VULNERABILITY



NATIONAL ML VULNERABILITY BREAKDOWN



NATIONAL ML COMBATTING ABILITY - METHODOLOGY

- The working group has taken into consideration the significant effort made since 2019 and the weaknesses and gaps that are affecting the country's ability to combat money laundering.

- It has also considered the risk and context of Mauritius and the external factors that change over time.

- There are 22 variables that are designed to capture the main drivers of vulnerability. The ratings of each variable result in the overall rating for the combatting ability.

KEY FINDINGS

National ML Combating Ability → **MEDIUM**

Strengthened AML framework

Comprehensively defined ML offences in the legislation as a separate or ancillary offence to a predicate crime

Financial Crimes Commission Act

Criminalizes a range of offences such as Fraud

Establishment of the Financial Crimes Division

Improved timeliness of case processing

OVERALL ML RISK

National ML Threat

MEDIUM HIGH

+

National ML Vulnerability

MEDIUM HIGH

=

OVERALL ML RISK

MEDIUM HIGH

NATIONAL TERRORISM FINANCING VULNERABILITY

National TF Combating Ability → **MEDIUM - LOW**

CFT framework

Comprehensively defined TF Offence in law

Prompt freezing of assets of designated persons

Continued efforts are crucial to fully addressing the challenges of TF and ensuring effective enforcement

No prosecutions or convictions for TF yet

No designated persons

OVERALL TF RISK

National TF Threat

MEDIUM LOW

+

National TF Vulnerability

MEDIUM LOW

=

OVERALL TF RISK

MEDIUM LOW

Mrs Hemlata Nundoochan
Team Leader: Banking Sector

Mrs Malini Ramdhan
Team Leader: Other Financial Institutions (Banking) Sector

Mrs Shakuntalah Ramanah
Team Leader: Payment Service Providers Sector

MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH SECTORS UNDER THE SUPERVISION OF THE BANK OF MAURITIUS

SECTORAL ML RISK RATINGS AT A GLANCE

	Residual ML Vulnerability Rating	+ ML Threat Rating	= ML Risk Rating
Banking Sector	Medium	High	Medium High
Other Financial Institutions			
Cash Dealers	Medium	Medium	Medium
NBDTIs	Medium Low	Medium Low	Medium Low
Payment Service Providers	Low	Low	Low

SECTORIAL TF RISK RATINGS AT A GLANCE

	Residual TF Vulnerability Rating	+ TF Threat Rating	= TF Risk Rating
Banking Sector	Medium Low	Medium	Medium
Other Financial Institutions			
Cash Dealers	Medium Low	Medium Low	Medium Low
NBDTIs	Low	Low	Low
Payment Service Providers	Low	Low	Low

OVERVIEW OF SECTOR(1)

- The Banking sector is a predominant pillar of the financial system in Mauritius.

- As an international financial centre, Mauritius is significantly exposed to cross-border financial flows, increasing the risks of money laundering (ML) from external 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.

- As of 30 June 2022:
  -19 licensed banks, 6 of which were domestic-owned, 10 were foreign-owned and 3 were branches of foreign banks.
  -Asset size: USD 46.3 billion
  -2.68 million customers

- As of 30 June 2024:
  -20 licensed banks (out of which 1 bank had received a licence but had not started operations), 6 of which were domestic-owned, 11 were foreign-owned, and 3 were branches of foreign banks.
  -Asset size:USD 53.4 billion
  -2.80 million customers.

OVERVIEW OF SECTOR (2)

- The ML risks facing the 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 utilizing complex financial products and structures
- The customer base comprised mostly of 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, private banking services, treasury products, custodial services, wealth management, specialised finance and safe deposit box services.
- Additionally, with the enactment of the VAITOS Act, banks may now onboard clients dealing in virtual asset-related activities or even become a Virtual Asset Service Provider themselves.

BANKING SECTOR MONEY LAUNDERING RISK

ML THREAT

- Based on local typologies, the laundering of domestic tainted money was mostly done through cash deposits, followed by several interbank transfers. 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.'

- 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.

- 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.

- The level of threat in this sector was rated as "**High**".

AML CONTROLS

- Strong control environment from the assessment of the following variables, amongst others:

i. Comprehensiveness of the AML legal/regulatory framework,
ii. Availability and effectiveness of entry controls,
iii. Effectiveness of supervision and compliance functions,
iv. Integrity and AML knowledge of banking staff, and
v. Effectiveness of Suspicious Activity Monitoring and Reporting, amongst others, for the sector.

- The AML legislative framework has been revamped to further reinforce the sector.

- From a supervisory perspective, starting in 2020, the BoM reviewed and significantly revised the off-site framework for the supervision of ML/TF 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 help them take appropriate measures to manage and mitigate the risks identified for ML and TF and have established a full-fledged compliance unction.

ML VULNERABILITIES - MAIN BANKING PRODUCTS/SERVICES

Product	Product characteristics	Final ML Vulnerability
1.Deposits	Deposit activities comprise the mobilization 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.	
i) Retail Deposits	This product comprised of demand, savings, and time deposits of individuals. Retail deposits carry ML risk inasmuch as they may be used to launder cash	MEDIUM
ii)Deposits accounts of Legal persons – Domestic	Legal entities such as 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 ML risks. 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.	MEDIUM
(iii) Deposits accounts of Legal persons – Non-Domestic and GBCs	The deposit accounts of non-domestic legal persons and GBCs were rated as 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.	MEDIUM
2.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	MEDIUM
3.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 as inherently high ML risk in view of (i) the profile 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.)	MEDIUM
4.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. Given the large volumes of funds involved in cross-border fund flows, illicit funds can readily be concealed in such transactions.	MEDIUM

ML VULNERABILITIES - MAIN BANKING PRODUCTS/SERVICES

5.Credit products for retail customers	The risk for ML could potentially be high in the event that the payment for loan instalments was made in cash. Banks, prior to granting loans, make an in-depth assessment of the customer's repayment capacity and source of funds.	LOW
6. 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. Banks, prior to granting loans, make an in-depth assessment of the customer's repayment capacity and source of funds.	LOW
7. 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.	MEDIUM
8. 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. 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, limit the risk of this product's abuse for ML. All transactions are conducted domestically.	LOW
9. 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.	MEDIUM

ML RISK ASSOCIATED WITH THE BANKING SECTOR



BANKING SECTOR TERRORIST FINANCING RISK

TF THREAT

- There is a potential risk that banks in the jurisdiction may be used as a conduit for financing of terrorism through cross-border transactions.

- TF risks 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 as **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.

CFT CONTROLS

- Similar to the robust systems and controls which banks have in place for ML risk, they have developed same for the mitigation of TF risks. 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 procedures as well as procedures manuals and circular notes which are available to members of staff regarding the implementation of TFS requirements to effectively comply with its obligations under the Sanctions Act and the Guidelines.

- Other specific internal controls include appropriate screening tools. These tools are used to screen prospective clients, existing clients and their related parties, including directors and beneficial owners, at time of onboarding and on an ongoing basis, including during file review or trigger event.

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

- Continuous training provided to staff on TF & TFS requirements.

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

TF RISK ASSOCIATED WITH THE BANKING SECTOR



BANKING OTHER FINANCIAL INSTITUTIONS (OFI) SECTOR

OVERVIEW OF BANKING (OFI) SECTOR

Other Financial Institutions under supervision of the Bank of Mauritius (BoM) consists of Non-Bank Deposit Taking Institutions (NBDTIs) and Cash Dealers.

- **NBDTIs**

Six NBDTIs operating as of end-June 2024 were authorised by the BoM to mobilize term deposits from the public. As at 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 Financial Services Commission and leasing activities have been covered 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.

- **Cash Dealers**

Cash dealers are comprised of 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 also authorised to carry out remittance businesses, including Money Value Transfer Services (MVTS) and wire transfers, as well as conducting forward exchange transactions through banks. Five of the Foreign Exchange Dealers offered MVTS through RIA, Western Union and MoneyGram.

None of the Cash Dealers conducted any transaction in virtual assets (VAs) or had virtual asset service providers (VASPs) as customers.

BANKING OFI
MONEY LAUNDERING (ML) RISK

BANKING OFI ML THREAT

	NBDTIs	Cash Dealers
Rating	Medium-Low	Medium
Reasons	Negligible cases of ML investigations with respect to term deposits and mortgage loans.	Potential unlicensed operators and the absence of ML investigations.

AML CONTROLS & RESIDUAL RISKS

	NBDTIs	Cash Dealers
AML Controls	Strong	Strong
Reasons	• They are subject to the same stringent legal and supervisory requirements as banks. • They have in place a full-fledged compliance function with adequate policies and procedures to mitigate ML risks. • They have strong monitoring systems with on-going training of staff on AML matters. • They 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. • The spectrum of products offered was also limited and carried low levels of ML vulnerability.	• Rigorous licensing requirements • Close monitoring and effective supervision by BoM particularly over the transactions reported on a daily basis. • All Cash Dealers have in place policies and procedures for mitigating ML and TF risks. • Mandatory to have in place an AML/CFT software for transaction monitoring purposes. • Compliance function exercises continuous monitoring over AML matters. • Extensive training and outreach programmes were provided to Cash Dealers and their staff to raise awareness on topical issues.
Residual risk	Given that both the ML threat and the residual ML vulnerability of the NBDTI sector was rated as **Medium-Low**, the residual ML risk was rated as **Medium-Low**.	Considering the controls in the sector, the overall ML residual vulnerability of the sector was **Medium**. Given that the ML threat to the sector was **Medium**, the residual ML risk that the sector was exposed to was **Medium**.

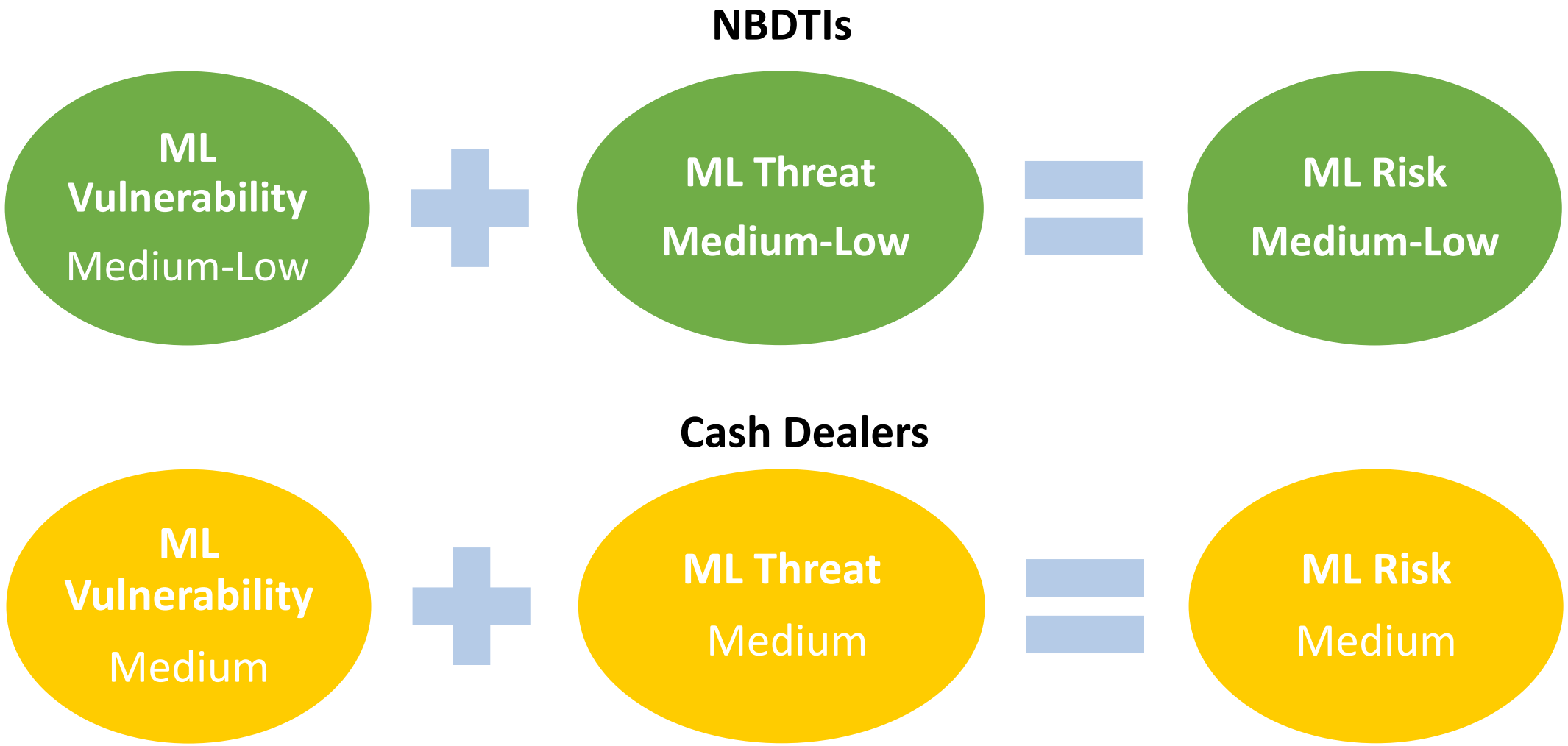
ML VULNERABILITIES - MAIN PRODUCTS/SERVICES - NBDTIs

Product	Product characteristics	Final ML Vulnerability
Term Deposits	• Majority of customers were Mauritian citizens and were onboarded face-to-face. • The level of cash activity was minimal as most term deposits were largely effected through bank transfers. • No international transaction was involved.	Medium-Low
Savings Deposits and Retirement Savings Schemes	• Only two NBDTIs offered these products. • Offered largely to retail domestic customers. • Cash transactions were not significantly involved. • Source of fund could be easily identifiable.	Savings deposits Medium-Low Retirement Savings Schemes Low
Mortgage Loans	• Only two NBDTIs offered this product. • Most credit was granted to domestic clients who were onboarded face-to-face.	Medium-Low
Other Credit Facilities	• Four NBDTIs offered this product. • 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.	Medium-Low

ML VULNERABILITIES - MAIN PRODUCTS/SERVICES – Cash Dealers

Product	Product characteristics	-Final ML Vulnerability
Over the counter purchase and sale of foreign currency notes	• Individual transactions were mostly of low value. • Cash transactions of more than MUR 500,000 were prohibited. • 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 rated as high-risk. • No cross-border exposure.	Medium
Remittance business (including spot and forward exchange transactions through wire transfers offered by Foreign Exchange Dealers only)	• Only two 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. • 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.	Medium-Low
Money Value Transfer Services (MVTS - offered by Foreign Exchange Dealers only)	• MVTS was offered exclusively to individuals, on a face-to-face basis only. • Daily limit per client/transaction, 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. • Majority of transactions were conducted in cash. • Cash transaction of more than MUR 500,000 was prohibited. • Cash intensive and cross-border exposure.	Medium-High

ML RISK ASSOCIATED WITH THE BANKING OFI SECTOR



BANKING OFI
TERRORIST FINANCING (TF) RISK

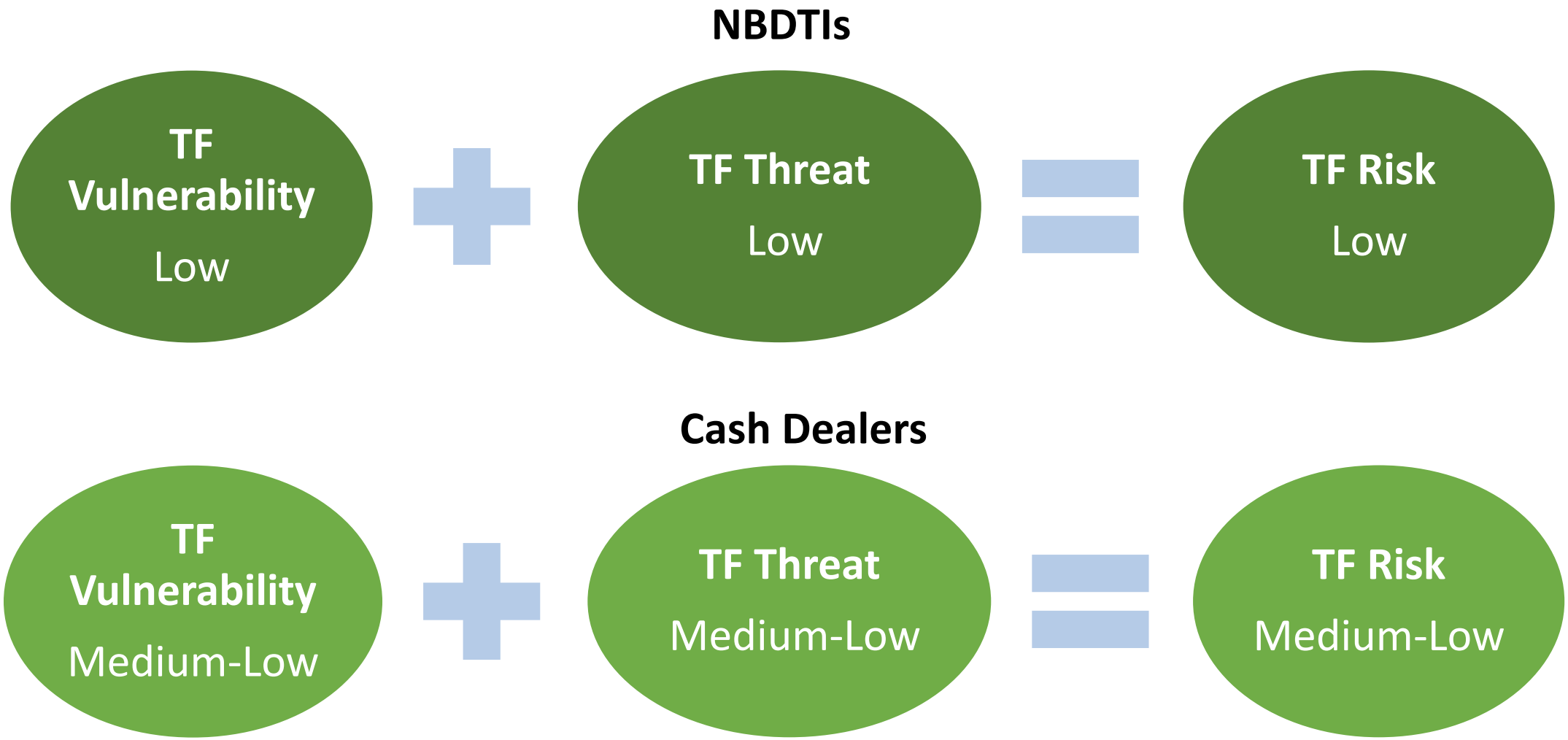
BANKING OFI TF THREAT

	NBDTIs	Cash Dealers
TF Threat	**Low**	**Medium-Low**
Reasons	➢ No intelligence suggesting misuse of this sector for TF ➢ No TF cases under investigation	➢ Cash intensive nature ➢ Risk of exploitation for cross border transfer of terrorist-related funds ➢ Limited number of intelligences received concerning TF ➢ Absence of TF cases under investigations and cases which led to conviction

CFT CONTROLS & RESIDUAL RISKS

	NBDTIs	Cash Dealers
Inherent TF Vulnerability	**Low** Reasons: • Absence of current account deposits (transactional accounts) and cross border flows. • Transfers into deposit accounts made predominantly through bank transfers. • Use of limited products. • Majority of customers were residents.	Foreign Exchange Dealers - **Medium** Money Changers - **Medium-Low** Reasons: 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.
Quality of CFT Controls	**Strong** Reasons: • Robust systems for mitigating TF risks. • Adequate policies and procedures, screening, and transactions monitoring systems for monitoring and mitigating TF risks. • Continuous training provided to staff on TF requirements.	**Strong** Reasons: • Cash Dealers have the obligation to screen all customers and transactions prior to processing same. • Transactions conducted by them were subject to close monitoring by BoM.

TF RISK ASSOCIATED WITH THE BANKING OFI SECTOR



PAYMENT SERVICE PROVIDERS MONEY LAUNDERING RISKS

OVERVIEW OF THE PSPs UNDER THE SUPERVISION OF THE BOM

- Payment Service Providers (PSPs) are entities which provide payment services, other than entities licensed by the FSC to conduct payment intermediary services exclusively outside Mauritius

- Three PSPs licensed by the Bank of Mauritius (in 2021 and 2022) at end June 2024, to offer mobile payment services, card services and e-money services

- Only one PSP allowed over-the-counter cash transactions, but stopped cash transactions in last quarter of 2024

- Total sector assets (USD 605 million) represented 1 % of total banking sector assets as of June 2024 (low side)

ML THREAT

Factors for rating of ML Threat for the period under review:

- No STRs reported by PSPs
- PSPs have not been subject to any ML investigations
- ML threat rating for this sector is therefore assessed as '**Low**'.

ML VULNERABILITY

ML Vulnerability assessed as **Low** based on:

- Size of PSP sector *(only 1% of Banking sector whose ML risk rating is medium high)*
- Size of Transactions *(small when compared to Banking sector)*
- Only one PSP deals in cards *(includes cross-border transactions)*
- The other two PSPs deal in domestic transactions only
- Generally low thresholds on transactions *(in line with customer profile)*
- Customer base mostly individuals *(mitigates customer risk)*
- PSP sector no longer has any cash activity

AML CONTROLS & RESIDUAL ML VULNERABILITY

AML CONTROLS

- Compliance with legal AML requirements *(AML Procedures, Compliance Officer, MLRO, Training Programme)*
- AML compliance reviews & AML audits
- AML oversight by board of directors
- Audits include AML reviews
- Suspicious Transaction Monitoring and Reporting procedures
- Fit & Proper Person Test to directors & senior officers

Residual ML vulnerability is Low.

ML RISK ASSOCIATED WITH PSPs



Residual ML Vulnerability =

Inherent Vulnerabilities + AML Controls

PAYMENT SERVICE PROVIDERS TF RISK

TF THREAT

Factors for rating of TF Threat for the period under review:

- No STRs reported by PSPs
- PSPs have not been subject to any TF investigations
- TF threat rating for this sector is therefore assessed as ‘Low’

Overall TF threat is **Low**

TF VULNERABILITY

TF Vulnerability assessed as **Low** based on:

- Size of PSP sector *(only 1% of Banking sector whose TF risk rating is medium)*
- Size of Transactions *(small when compared to Banking sector)*
- Low level of Outward International transactions *(only one PSP deals in cards- online purchase of goods & services from countries with acceptable risk ratings- low card limits)*
- The other two PSPs deal in domestic transactions only
- Inward international transactions non-existent
- Client base profile of PSP sector is low risk
- PSP sector no longer has any cash activity

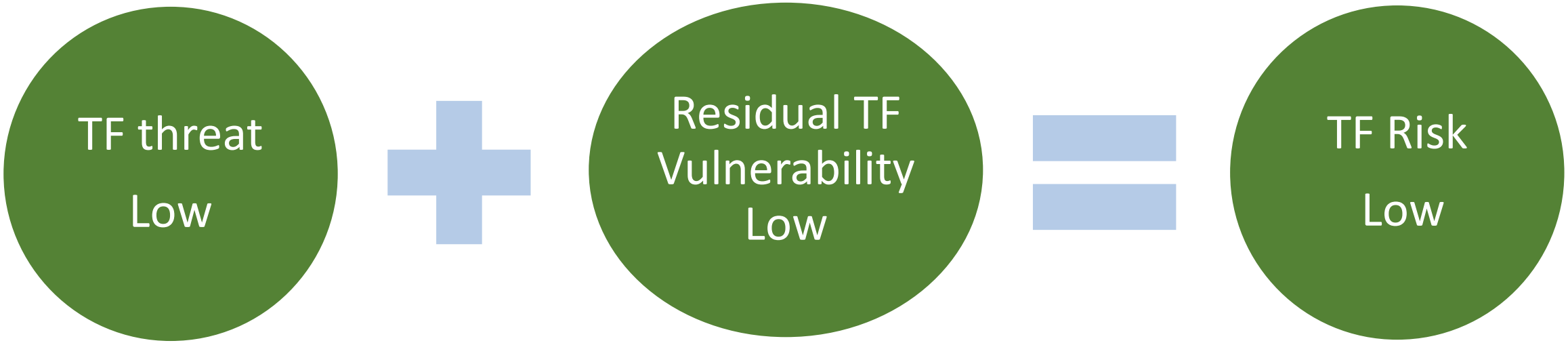
TF CONTROLS & RESIDUAL TF VULNERABILITY

TF CONTROLS

- Compliance with legal CFT requirements *(TFS Procedures, Compliance Officer, MLRO, CFT Training Programme)*
- Compliance reviews & audits
- Oversight by board of directors
- Suspicious Transaction Monitoring and Reporting procedures

Residual TF vulnerability is Low

TF RISK ASSOCIATED WITH PSPs



Residual TF Vulnerability =

Inherent Vulnerabilities + AML Controls

Mrs Komalavadi Narrainen and Mrs Meenakshi Bappoo-Soobhug

Team Leaders: Securities Sector

Ms Teenoosha Boyjoo and Mr Dharmanand Poyroo

Team Leaders: Insurance Sector

Mrs Sarojini Sumputh-Veeramah and Mrs Shamala Mooroogen

Team Leaders: Other Financial Institutions (Non-Banking) Sector

Mrs Anjali Seedoyal and Ms Tanvi Keerodhur

Team Leaders: Trust and Company Service Providers Sector

MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH SECTORS UNDER THE SUPERVISION OF THE FINANCIAL SERVICES COMMISSION

SECTORIAL ML RISK RATINGS AT A GLANCE

	Residual ML Vulnerability Rating	+ **ML Threat Rating**	= **ML Risk Rating**
Securities Sector	Medium	Medium	Medium
Insurance Sector	Medium	Ranges from Medium Low to Low	Medium
Other Financial Institutions (non-banking)	Medium	Ranges from High to Low	Medium
Trust and Company Service Providers	Medium	High	Medium High

SECTORIAL TF RISK RATINGS AT A GLANCE

	Residual TF Vulnerability Rating	+ **TF Threat Rating**	= **TF Risk Rating**
Securities Sector	Low	Low	Low
Insurance Sector	Medium Low	Low	Medium Low
Other Financial Institutions (non-banking)	Medium Low	Ranges from Medium Low to Low	Medium Low
Trust and Company Service Providers	Medium Low	Medium Low	Medium Low

AML CONTROLS APPLIED ACROSS THE SECTORS

- Comprehensive AML framework applicable across the FSC sectors
- Clear and Comprehensive framework for the licensing requirements

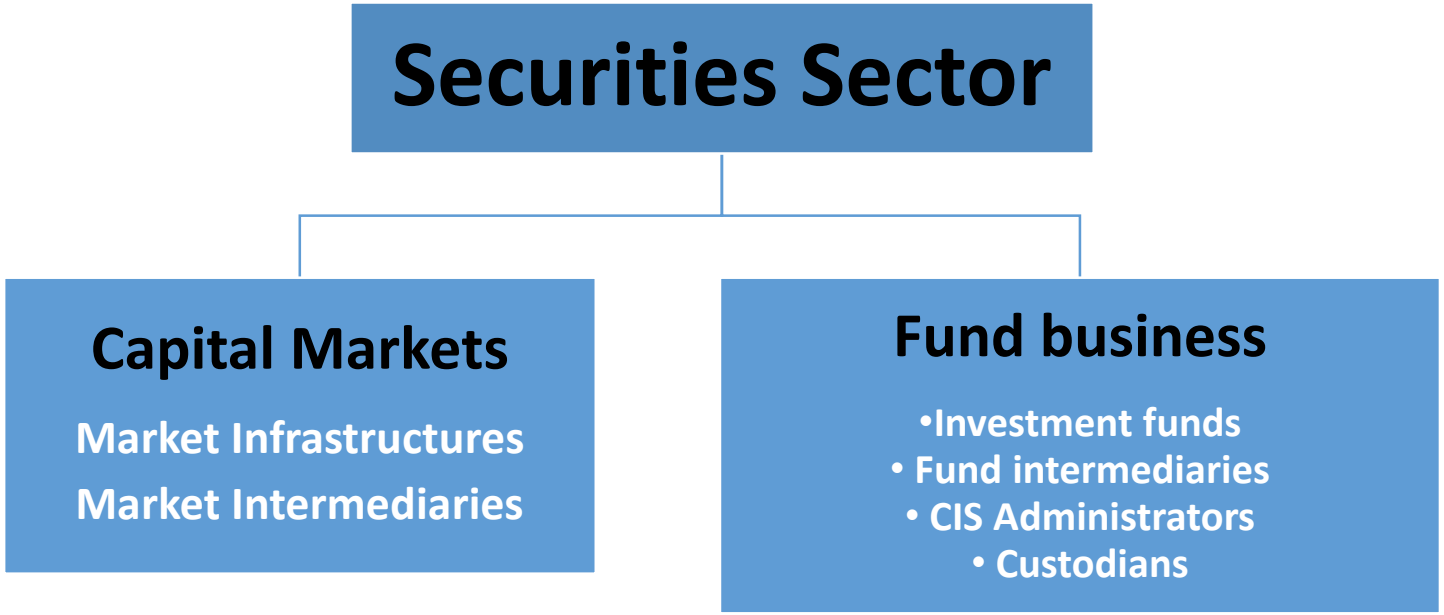
  Entry controls –fit and proper test/assessment on directors, shareholders, members of senior management and beneficial owners
- Adherence to Code of Business Conduct / Appointment of MLRO / Regular training
- Application of AML/CFT risk-based approach for supervision : onsite, offsite and follow-up
- Power to impose administrative sanctions

CFT CONTROLS APPLIED ACROSS THE SECTORS

- Comprehensive legal framework – FIAMLA and UN Sanctions Act
- For onsite inspections, there is one parameter on Targeted Financial Sanctions which is assessed for TF purposes.
- Effectively implementing TFS
- All transactions subject to Sanction screening
- Existing account are screened regularly and as and when the UNSC list is updated

SECURITIES SECTOR MONEY LAUNDERING RISK

OVERVIEW OF SECURITIES SECTOR



- Include domestic and GB players. There is a single legal and AML regime overseeing both types of entities.
- As of 30 June 2024, the sector comprised 2,185 licensees (142 domestic entities and 2,043 GB players).

The securities institution types assessed for NRA:

- Market Infrastructure [Securities Exchanges and Clearing and Settlement Facilities]
- Market Intermediaries [Different categories of Investment Dealers and Investment Advisers]
- Funds business [CIS Managers and Custodians]

SECURITIES SECTOR ML THREAT

- The sector was not subject to any enquiry by the LEAs
- No case under investigation, prosecution or conviction
- No local typology for the Securities sector
- 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.
- The FATF typologies - perception 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.

SECURITIES SECTOR ML VULNERABILITY

Overall ML Vulnerability for the Sector: **MEDIUM**

The main activities which are more vulnerable to ML are Collective Investment Schemes (CIS), Closed-end Funds (CEF) and Investment Advisers (Unrestricted)

SECURITIES SECTOR ML VULNERABILITY (CONT.)

Activities	Characteristics	Inherent ML Vulnerability
Market Infrastructure	- Provide trading and settlement platform for members to trade and settle securities on behalf of investors - Securities exchange, Securities trading systems & Clearing and Settlement facilities	**LOW** - Do not deal with clients' monies

Activities	Characteristics	Inherent ML Vulnerability
Investment Advisers	▪ Core activity - provision of investment advice to clients ▪ Different categories of investment advisers: ▪ Investment Adviser (Unrestricted) ▪ Investment Adviser (Restricted) ▪ Investment Adviser (Corporate Finance Advisory)	**LOW:** Investment Adviser (Restricted) & Investment Adviser (Corporate Finance Advisory) ▪ Provide advice on securities to clients ▪ Do not deal with clients' funds **MEDIUM:** Investment Advisers (Unrestricted) ▪ Management of clients' portfolio of securities under a discretionary or non-discretionary mandate in addition to providing advice; • *Discretionary mandate: can invest in securities without the prior consent of clients, thus elevating the vulnerability to ML.* ▪ Include complex products depending on risk appetite and clients' investment objectives.

SECURITIES SECTOR ML VULNERABILITY (CONT.)

Activities	Characteristics	Inherent ML Vulnerability
Investment Dealers	▪ Core Activity: The execution of trade orders on behalf of clients ▪ Do not hold clients' funds ▪ Large number of domestic and global business retail clients' accounts ▪ Different Categories of Investment Dealers: - Investment Dealer (Discount Broker) - Investment Dealer (Broker) - Investment Dealer (Full-Service Dealer including Underwriting) - Investment Dealer (Full-Service Dealer excluding Underwriting)	▪ Main risk is the source of funds used by investors to trade in securities products. ▪ Complex products rather than traditional equity-based products – transactions more difficult to red-flag and trace ▪ Potential abuse of ML is higher when dealing with certain types of clients such as PEPs and clients from high-risk jurisdictions. ❑ **MEDIUM:** Investment Dealer (Full Service Dealer excluding Underwriting) & Investment Dealer (Broker) ❑ **MEDIUM-LOW:** Investment Dealer (Full Service Dealer including Underwriting & Investment Dealer (Discount Broker)

SECURITIES SECTOR ML VULNERABILITY (CONT.)

Activities	Characteristics	Inherent ML Vulnerability
CIS Manager - Collective Investment Schemes (CIS) - Closed-end Funds (CEF) CIS Managers are licensed by the FSC to manage CIS and CEF.	Domestic market - retail funds, attractive to the public and retail clients. Global Business - Expert Funds or Professional CIS with expert investors, sophisticated investors, and high net worth individuals.	**MEDIUM-HIGH** (risk factors present but to a lesser extent than the previous NRA) - Client base: • PEPs • Clients from high-risk jurisdictions • High Net Worth individuals • International clients and institutional investors - Use of legal persons and legal arrangements to structure investments - Non-face-to-face dealings with clients

SECURITIES SECTOR ML VULNERABILITY (CONT.)

Activities	Characteristics	Inherent ML Vulnerability
Custodians (CIS) - a bank or a bank subsidiary - responsible for the safekeeping of the assets of a CIS or a CEF	- Custodial services provided as part of broader banking services - Custody business segment is insignificant when compared to their overall banking activities.	**MEDIUM-LOW** - Size of assets under custody quite low and most of those assets are under sub-custody and held outside Mauritius - Clients mainly GB entities and hence non-face-to-face business

AML CONTROLS

1.Comprehensive legal framework – FIAMLA and Regulations

Clear and comprehensive framework for the licensing and registration

Entry controls – fit and proper test/assessment on directors, shareholders, members of senior management and beneficial owners

Adherence to Code of Business Conduct / Appointment of MLRO / Regular training provided by Securities institutions

Supervision: risk based onsite and offsite inspections

Powers to impose administrative sanctions

ML RISK ASSOCIATED WITH SECURITIES SECTOR



Residual ML Vulnerability =

Inherent Vulnerabilities + AML Controls

SECURITIES SECTOR TERRORISM FINANCING RISK

SECURITIES SECTOR TF THREAT

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 has not observed the misuse of this sector.

No known TF case emanating from the Securities sector either on the domestic front or in the global business sector & No terrorist group/organisation in Mauritius

The threat associated with the securities sector was considered as **LOW**

SECURITIES SECTOR TF VULNERABILITY

The TF vulnerability of the Securities sector was rated Low.

- Outward international transaction - 22%.
- Inward international transactions - 23%

Inward and Outward international transactions to higher risk geographical locations < 1 % of total value of transactions

Number of clients from high-risk jurisdictions and the clients having business links with high-risk jurisdictions < 10%

CFT CONTROLS & RESIDUAL TF VULNERABILITY

- Comprehensive legal framework – FIAMLA and UN Sanctions Act
- For onsite inspections, there is one parameter on Targeted Financial Sanctions which is assessed for TF purposes. The compliance rate for this parameter was on average 83% over the 3 cycles.
- No TF cases were reported for the sector. Inadequate understanding and detection of TF risks.

  For the period under review, there were no cases where criminal sanctions have been taken for the Securities sector.
- Staff of securities firms have benefitted from outreach activities however was on ML aspects rather than TF.

  For the period under review, no STR was filed for TF purposes.
- 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**

TF RISK ASSOCIATED WITH SECURITIES SECTOR



Residual TF Vulnerability =

Inherent Vulnerabilities + TF Controls

INSURANCE SECTOR MONEY LAUNDERING RISK

OVERVIEW OF INSURANCE 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.

Long-term insurance	General Insurance
• Linked Long-Term Insurance • Life Insurance Plans with a Cash Value • Investment/Savings component, Pure Protection Life Insurance Plans • Other Life Insurance Plans • Annuities and Pensions	• Motor, • Accident & Health • Property, • Miscellaneous • Liability, • Transportation • Engineering, and • Guarantee classes.

OVERVIEW OF INSURANCE SECTOR (continued)

The contribution of the Insurance, Reinsurance and Pensions sector to GDP amounted to 1.9% in 2024 with an annual growth rate of 3.9%.

Gross Premium for Long-Term Insurance Business amounted to MUR 11.7 bn in 2023 compared to MUR 12.6 bn in 2022 (- 7%).
The Long-Term Insurance sector saw an increased in Total Assets, which amounted to MUR 117.4 bn in 2023 compared to MUR 109.6 in 2022 (a growth of 7%).

For General Insurance Business, gross premium stood at MUR 16.3 bn in 2023 compared to MUR 14.4bn in 2022 (+14%). For companies in the General Insurance sector.

Total Assets amounted to MUR 28.7 bn in 2023 compared to MUR 27.7 bn in 2022 (+4%).

INSURANCE SECTOR ML THREAT

Long-Term Insurance
ML Threat Rating: Medium-Low
One domestic typology reported – fraud committed by employee of LT insurer
International typologies indicate potential criminal exploitation.
General Insurance
ML Threat Rating: Low, except Motor Insurance (Medium-Low)
One domestic typology involving motor insurance
Risks exist due to potential fraud, where proceeds could be used for ML.

INSURANCE SECTOR ML VULNERABILITY

The final vulnerability level of the insurance sector is rated as Medium.

INSURANCE SECTOR ML VULNERABILITY (CONT.)

Products – Long Term Insurance	Characteristics	Inherent ML Vulnerability
1. Linked Long-Term Insurance (LLTI)	• The ML risks in LLTI arise from its investment flexibility, liquidity, and ability to handle large fund volumes. • LLTI holds a significant market share and features a high level of single premium policies. • Higher cash usage.	Medium-High
2. Life Insurance Plans with Cash Value and Investment/Saving	▪ Life insurance plans with cash value and an investment or savings component combine protection with long-term wealth creation. ▪ Low size, client base, use of agents and its availability of cross-border use were present	Medium-Low
3. Annuities and Pensions	• Contracts involving liabilities related to human life or annuities, excluding health and accident insurance. • Mostly involved regular premium payments. • 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.	Medium-Low

INSURANCE SECTOR ML VULNERABILITY (CONT.)

Products – Long Term Insurance	Characteristics	Inherent ML Vulnerability
4. Pure Protection Life Insurance Plan	▪ A Pure Protection Life Insurance Plan provides financial security to the insured's family upon death, typically with regular premium payments. ▪ Use of agent involvement and level of cash activity ▪ ML typologies included fraud and tax evasion risks. Cross-border use was rated medium, while anonymous use was unavailable.	Medium-Low

INSURANCE SECTOR ML VULNERABILITY (CONT.)

Products – General Insurance	Characteristics	Inherent ML Vulnerability
Motor	▪ Motor insurance provides financial protection against losses or damages involving motor vehicles. ▪ Premium payments were primarily made via bank transfer followed by cheque and cash, with the use of cash transactions was notably higher than other insurance segments. ▪ Domestic typology involving staged accidents and fraudulent claims was reported.	Medium
Property	• Provides benefits for risks related to the use, ownership, loss, or damage of property. • Moderate market share, use of agents, client base, and cash activity. ML typologies and evidence of its use in fraud or tax evasion schemes	Medium
Engineering	▪ Provides coverage with risks associated with machinery, equipment, construction, or machinery breakdowns. ▪ Low market share and 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.	Medium-Low

INSURANCE SECTOR ML VULNERABILITY (CONT.)

Products – General Insurance	Characteristics	Inherent ML Vulnerability
Liability	• Provides protection against claims resulting from injuries and damage to other people or property. • 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.	Medium-Low
Transportation	▪ Provides coverage for the insured's property while it is in transit from one location to another, using any necessary mode of transport. ▪ 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.	Medium-Low

INSURANCE SECTOR ML VULNERABILITY (CONT.)

Products – General Insurance	Characteristics	Inherent ML Vulnerability
Guarantee	• 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. • 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 and the market share was minimal.	Medium-Low
Miscellaneous	▪ Cover a wide range of risks not specifically addressed by other specialized types of insurance. ▪ 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.	Medium-Low

AML CONTROLS & RESIDUAL ML VULNERABILITY

Existence of strong AML legal framework and FSC's risk-based supervision.

FSC maintains ML/TF risk understanding through offsite monitoring, onsite inspections, and follow-ups.

Onsite inspections revealed that insurance companies have improved AML/CFT compliance by implementing:

- AML systems to identify high-risk transactions (PEPs, clients from non-equivalent jurisdictions, watch-listed clients) and mitigate associated risks.
- Customer acceptance policies for risk profiling and periodic reviews of high-risk clients.

Most insurers:

- Screen clients and transactions against Sanctions Lists and adverse media.
- Identify PEPs, their controlled entities, and individuals on the UN Sanctions List.

While strong regulatory frameworks mitigate risks, products like Linked Long-Term and Motor insurance remain vulnerable.

ML RISK ASSOCIATED WITH INSURANCE SECTOR

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

For General insurance, motor insurance was found to be **Medium**, primarily due to fraudulent claims to launder money.

Property, Liability, A & H are rated **Medium Low**, while Miscellaneous, Transportation, Guarantee and Engineering are rated **Low**.

INSURANCE SECTOR TERRORISM FINANCING RISK

INSURANCE SECTOR TF THREAT

TF threat is rated **Low.**

No domestic TF case was reported for the period under assessment.

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.

Terrorists may attempt to file fraudulent insurance claims to generate funds through early cancellation, using fraudulent or suspicious claims as a means of extracting funds from insurance companies.

INSURANCE SECTOR TF VULNERABILITY

The TF vulnerability of the Insurance sector was rated **Medium-Low**.

Insurance products with and without investment component which were all rated **Medium-Low** for TF Risk.

Level of outward international transactions and operations of business entities was a factor as significant outwards transactions were conducted from within Mauritius.

Low level of total outward transactions was carried out with high-risk jurisdictions.

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.

Level of cash activity ranged from **Medium** to **Medium-Low** across all classes of insurance business.

CFT CONTROLS & RESIDUAL TF VULNERABILITY

The Insurance sector indicated having in place the following CFT measures:

- internal controls and procedures in their compliance programmes to comply with targeted financial sanctions obligations.
- majority of the insurance entities have adequate policies and procedures, systems and controls in place to meet TFS requirements:
  - screening systems that had been effectively designed and tested;
  - sufficient and quality data about the customer to identify whether the customer was sanctioned; and
  - documented sanctions screening searches.

Considering the TF vulnerability is **Medium-Low**, and TF threat **Low**, the TF risk of the Insurance Sector is **Medium-Low**.

TF RISK ASSOCIATED WITH INSURANCE SECTOR

Inherent vulnerability - **Medium-Low**.

Final TF vulnerability - **Medium-Low**.

TF threat – **Low**:

Overall TF risk of the sector **Medium-Low**.

OFI SECTOR MONEY LAUNDERING RISK

OVERVIEW OF OFI 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.

The activities falls under Section 14 (Second Schedule), Section 77A and 79A of Financial Services Act, Section 12 of Private Pension Schemes Act 2012, and Financial Services Rules 2008

1. Asset Management	**11. Payment Intermediary Services**
2. Registrars and Transfer Agents	**12. Pension Scheme Administrators**
3. Family Office (Single)	**13. Peer to Peer Lending**
4. Family Office (Multiple)	**14. Factoring**
5. Credit Rating	**15. Credit Finance**
6. Investment Banking	**16. Actuarial Services**
7. Distribution of Financial Products	**17. Representative Office**
8. Treasury Management	**18. External Pension Scheme**
9. Global Legal Advisory Services	**19. Funeral Scheme Management**
10. Leasing	

No Licensees for following OFI activities
Compliance Services
Crowdfunding
Fintech Service Provider
Robotic and Artificial Intelligence Enabled Advisory Services
Representative Office

OFI SECTOR ML THREAT

Out of all the activities falling under the OFI sector, Leasing companies and PIS were the most exposed to ML Threat.

Leasing

High ML Threat

- Local typologies
- Drug traffickers acquiring vehicles under the name of their relatives or using “prêtes noms”

Payment Intermediary Services (PIS)

Medium ML Threat

- Complaints received- Ongoing case
- Facilitator for the transfer of funds between two or more parties

OFI SECTOR ML VULNERABILITY

- The overall ML vulnerability of all the activities under the OFI sector ranged from **Low** to **Medium**, considering the controls in the sector.

- The 5 most vulnerable activities to ML in the OFI sector:

ML: 5 most risky activities	Leasing
	Payment Intermediary Services
	Investment Banking
	Treasury Management
	Credit Finance

LEASING

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

Leasing activity provides an alternative means to raise money other than debt or term loan financing

The main ML vulnerability arises mostly from the lessee who may be laundering the proceeds.

The total assets and turnover for leasing were relatively significant when compared to other activities within the OFI Sector.

PAYMENT INTERMEDIARY SERVICES

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

PIS is related to the processing and execution of payment transactions

Most of the transactions are carried out through wire transfers and online systems with a relatively high frequency of international transactions

Holders of a PIS licence can only conduct business exclusively outside Mauritius.

INVESTMENT BANKING

The residual vulnerability for Investment Banking was assessed as **Medium.**

The Investment Banking activity regroups activities like

1. Investment advisory
2. Investment dealer
3. Distribution of financial products
4. Asset management

under a single umbrella licence in Mauritius.

Products offering are vast and may be complex

The frequency and value of international transactions was assessed as significant.

TREASURY MANAGEMENT

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

Treasury Management involves the process of managing the cash and investments of the business, mostly within group entities

Main ML risk resides with the payments resulting from foreign trade business

Large volume of international transactions

CREDIT FINANCE

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

Credit Finance provides alternative sources of financing (generally short-term) to household and corporates

Credit Finance providers are internationally recognised as being vulnerable to ML as loans could be repaid with illicit funds.

AML CONTROLS

- Applying CDD Checks
- Reported suspicious transactions
- Transactions recorded and easily retrievable

ML RISKS ASSOCIATED WITH OFI SECTOR

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

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

OFI SECTOR TERRORISM FINANCING RISK

OFI SECTOR TF THREAT

The TF threat rating for the activities in the OFI sector was assessed as Low except for PIS which was Medium-Low.

No existence of local cases related to the activities in the OFI Sector

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

OFI SECTOR TF VULNERABILITY

- The overall TF vulnerability of all the activities under the OFI sector ranged from **Low** to **Medium-Low**, considering the controls in the sector.

- The 5 most vulnerable activities to TF in the OFI section under the supervision of the FSC are:

TF:	Payment Intermediary Services
5	Custodian services (Non-CIS)
most	Credit finance
risky	Treasury Management
activities	Investment Banking

CFT CONTROLS & RESIDUAL TF VULNERABILITY

- Effectively implementing TFS
- All transactions subject to Sanction screening
- Existing account are screened regularly and as and when the UNSC list is changed

TF RISKS ASSOCIATED WITH OFI SECTOR

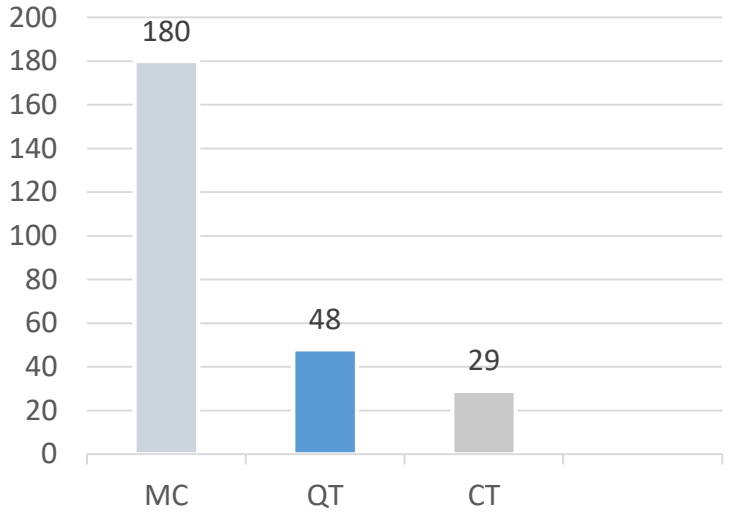
The TF risk assessment showed that potential channels for TF activities are PIS, Custodian (Non-CIS), Credit Finance, Treasury Management, and Investment Banking and they were assessed as **Medium-Low.**

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

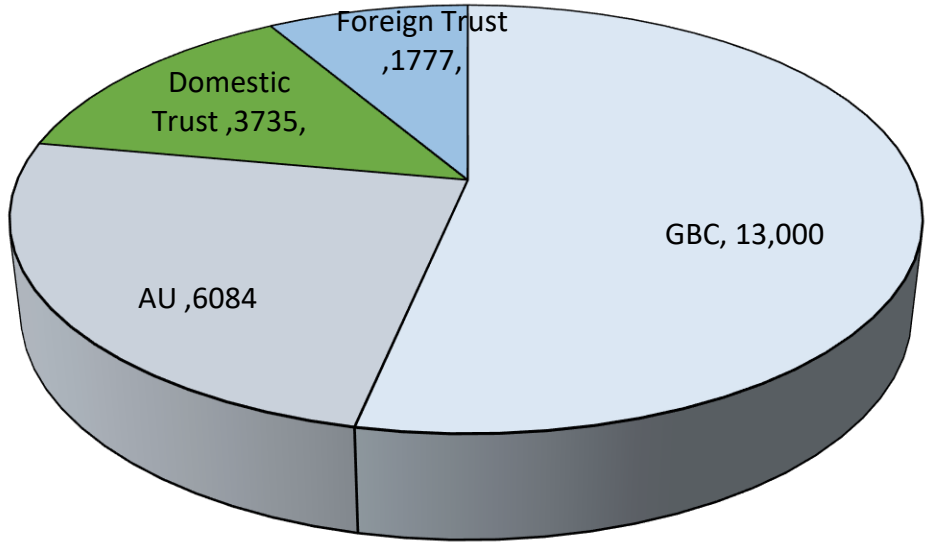
TCSPs SECTOR MONEY LAUNDERING RISK

OVERVIEW OF TCSPs SECTOR

Breakdown of TCSPs



Breakdown of entities managed



- MCs: Licensed under Section 77 of the FSA
- QTs: Licensed and supervised
- Both regulated as Financial Institutions
- Formation & management of GBCs, AUs, and Trusts and AML/CFT compliance

Economic impact

- Employment: ~5,600 people (Dec 2023)
- Contribution to GDP: 8.4% (2023)
- Aggregate Assets: USD 705 billion
- Annual Growth Rate: 3.9% (2023)

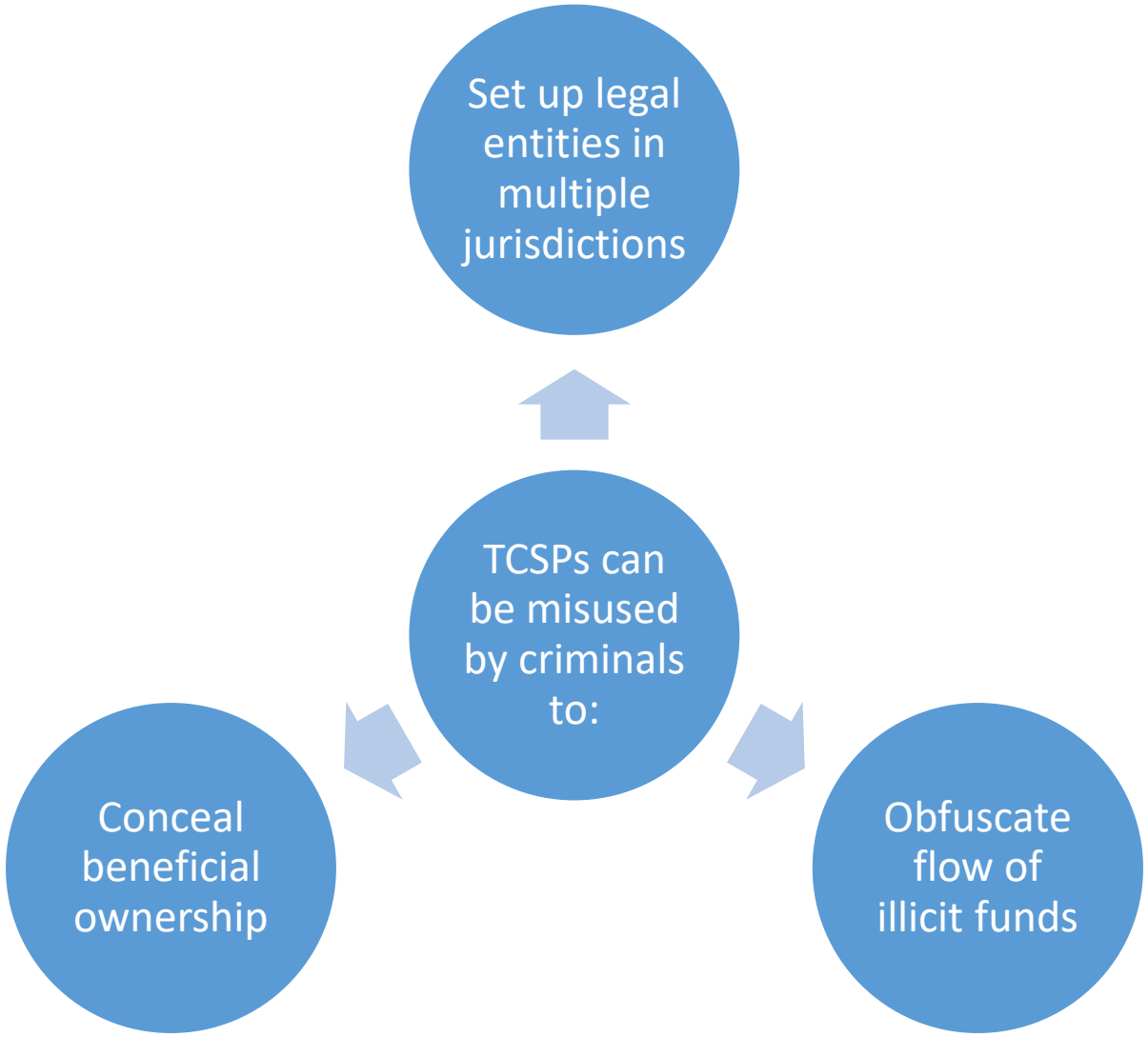
TCSPs SECTOR ML THREAT

Common Typologies

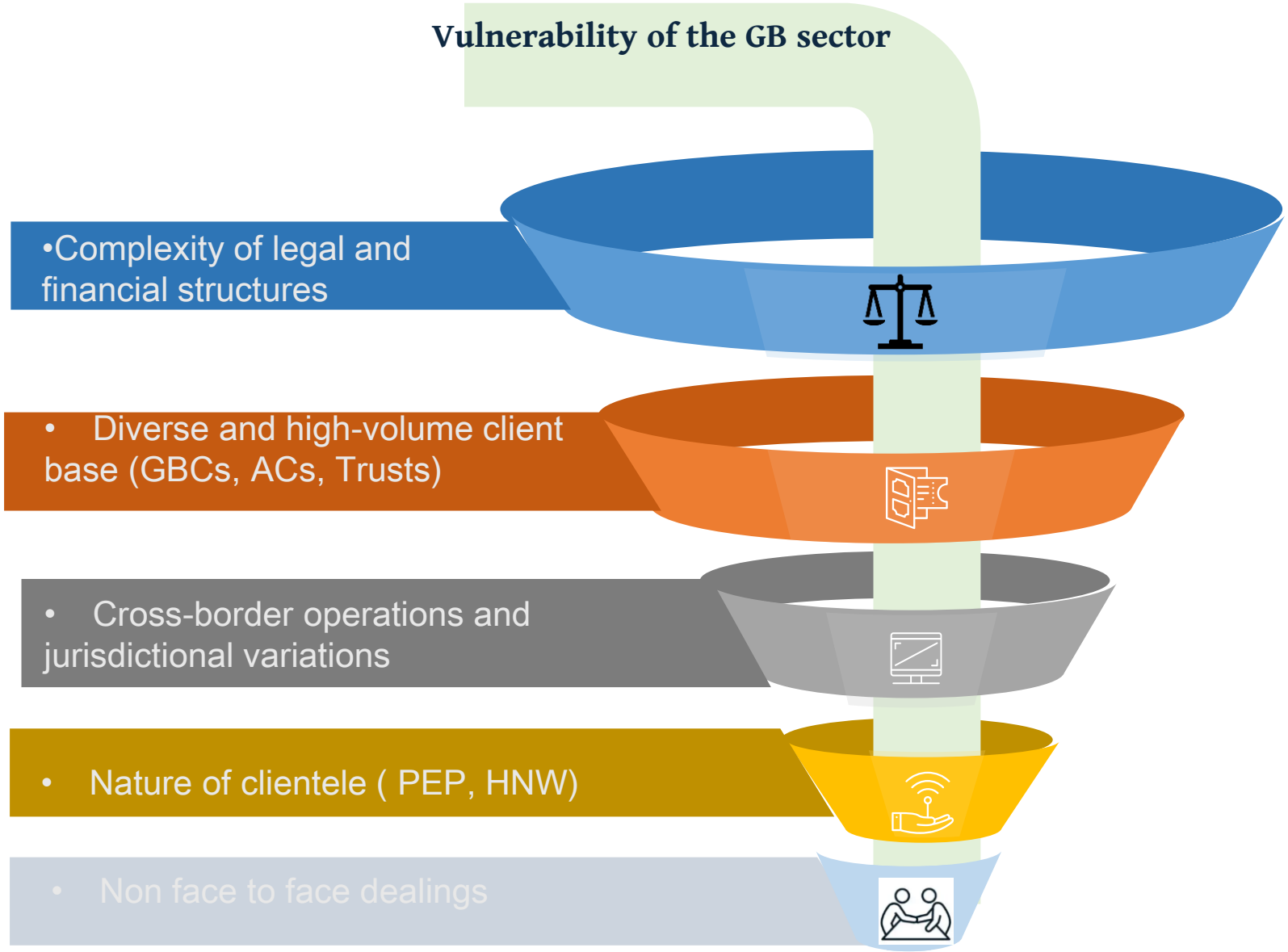
Reduce traceability of illicit funds

Create **complex, multi-layered structures**

Facilitate **cross-border fund transfers**



TCSPs SECTOR ML VULNERABILITY



The entities managed by TCSPs include higher risk client profiles, non-face to-face dealings, complex legal structures and cross border transactions, dealings with high risk jurisdictions

These factors may contribute in making the sector vulnerable to ML by presenting opportunities for illicit funds to move across borders undetected while concealing the identities of those involved

TCSPs SECTOR ML VULNERABILITY

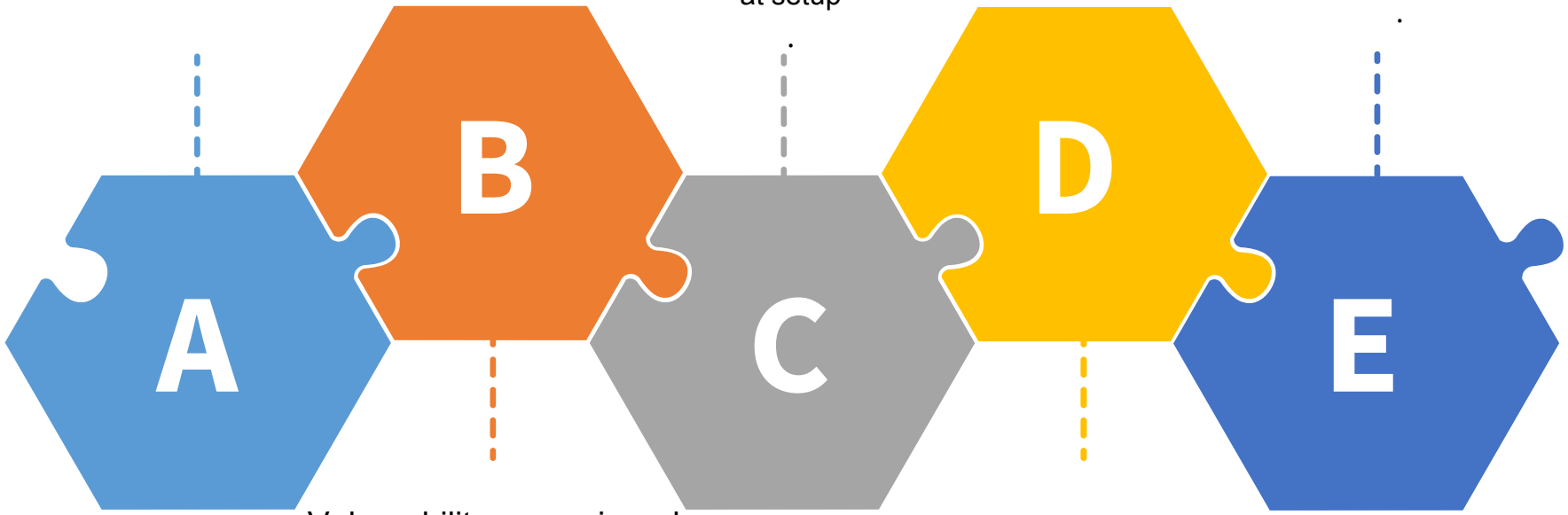
Vulnerability of Trusts

Layering Complex ownership structures

Can be used to obscure fund origins

Discretionary trusts do not provide beneficiary details at setup

Cross-border transactions further complicate:
•Determining the Ultimate Beneficial Owner



•Vulnerability may arise when there is no clear economic rationale for setting up the trust

Complex layering make it difficult to identify true ownership

AML CONTROLS

- Comprehensive AML framework applicable to TCSPs
- Comprehensive framework for the licensing and registration requirements, Entry controls –fit and proper test/assessment on directors, shareholders, and beneficial owners of TCSPs
- Application of AML/CFT risk-based approach for supervision of TCSPS
- Supervision: risk-based onsite and offsite
- Powers to impose administrative sanctions

ML RISKS ASSOCIATED WITH TCSPs SECTOR



TCSPs SECTOR TERRORISM FINANCING RISK

TCSPs SECTOR TF THREAT

- International cases on the TCSP sector suggest that criminals may seek to set up opaque structures that can circumvent any restrictive measures in place.

TF Threat Rating: **MEDIUM-LOW**

TCSPs SECTOR TF VULNERABILITY and CONTROLS

Inherent TF vulnerability

- Non face to face dealings
- Large cross border transaction
- Use of complex structures
- Linkage and dealings with Jurisdictions of concern

TF Controls

- No cash transactions
- Comprehensive legal and regulatory framework
- CFT preventive measures including the appointment of MLRO for the reporting of suspicious transactions
- Obligation to conduct a risk assessment to identify, assess and document TF risk
- MCs/QTs required monitor inward and outward transactions

TCSPs SECTOR TF VULNERABILITY and CONTROLS

Trust Service Providers

Vulnerability	Mitigating factors
Cross-border transactions	No known cases of TF involving TCSP operators in Mauritius.
Non-face-to-face interactions with beneficiaries.	No involvement in cash transactions by MCs or QTs.
International exposure to Jurisdictions of concern	Low risk of funds being transferred out of Mauritius via TCSPs for terrorism

TF RISKS ASSOCIATED WITH TCSPs SECTOR



Mrs. Sulakshna GIGABHOY SAUHOBOA
Team leader for DNFBP Vulnerability Assessment Team

MONEY LAUNDERING AND TERRORISM FINANCING RISK ASSOCIATED WITH DESIGNATED NON-FINANCIAL BUSINESS PROFESSIONS (DNFBPs)

SECTORIAL ML RISK RATINGS AT A GLANCE

DNFBP Sub sector	Residual ML Vulnerability	ML Threat	ML Risk
Gambling	Medium	High	Medium High
Real estate	High	Medium	Medium High
DPMS	Medium	Medium High	Medium High
Legal	Medium	Medium	Medium
Notaries	Medium	Medium High	Medium High
Accountancy	Medium low	Medium	Medium

SECTORIAL TF RISK RATINGS AT A GLANCE

DNFBP Sub sector	TF Vulnerability Rating	TF Threats Rating	TF Risk Rating
Gambling	Medium Low	Low	Medium Low
Real estate	Medium	Low	Medium Low
Jewellery	Medium-Low	Low	Medium-Low
Legal	Low	Low	Low
Notaries	Medium-Low	Low	Medium-Low
Accountancy	Low	Low	Low

LEGAL SECTOR MONEY LAUNDERING RISK

OVERVIEW OF THE LEGAL SECTOR

The legal sector includes law firms, barristers and attorneys.

During the review period, 77 legal professionals were classified as reporting persons, including 16 Attorneys, 39 Barristers, and 22 Law Firms.

It is to be noted that most legal professionals focused on litigation and advisory services, limiting exposure to prescribed activities.

Clients 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

ML THREAT ASSOCIATED WITH THE LEGAL SECTOR

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.

Therefore, ML threat associated with the Legal sector was rated **Medium**

RESIDUAL ML VULNERABILITY RATINGS

Legal professionals are subject to professional oversight through associations like the Mauritius Law Society and the Mauritius Bar Association and they are also bound by Codes of Ethic and AML obligations under FIAMLA.

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.

However, the nature of legal services still presents inherent ML risk justifying a rating of **Medium** residual ML vulnerability.

ML RISK ASSOCIATED WITH THE LEGAL SECTOR

Legal professionals have widened their services from conventional drafting of contracts, legal advice to providing trusteeship services and management of corporate entities.

Given the diverse client base with different risk profiles, the legal sector is deemed vulnerable to being exploited for money laundering offences.

The ML Risk of the legal sector is rated as **Medium**

LEGAL SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE LEGAL SECTOR

The proficiency of legal practitioners may be exploited knowingly or unknowingly for terrorism/TF purposes.

However, the absence of any known or reported TF activity involving legal practitioners indicates a **Low** TF threat.

RESIDUAL TF VULNERABILITY

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.

However, no such cases have been found domestically, so the residual TF vulnerability for the legal profession is considered **Low**

TF RISK ASSOCIATED WITH THE LEGAL SECTOR

For the period under review, there were no reported case for TF.

The TF risk in this sector is rated as **Low**

NOTARIES SECTOR MONEY LAUNDERING RISK

OVERVIEW OF THE NOTARIES SECTOR

- Notaries are registered with the Chamber of Notaries and are normally governed by the Notaries Act 2008 and their code of ethics (“code de deontologie”).

- Notaries have a very distinct role as compared to other professionals in the legal profession sector. More specifically, they are the only one within that sector to be engaged in the buying and selling of real estate namely in the finalisation of the real estate transactions by providing a duly signed notarial deed.

- They have to interact with key stakeholders in the Real Estate Sector and given exposure of Real Estate Sector to money laundering, it would be expected that same has an incidence on the vulnerability of the Notary’s profession.

ML THREAT ASSOCIATED WITH THE NOTARIES SECTOR

- 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 product or service that are offered.
- Following the legislative amendments of the Anti-money laundering and combatting the financing of terrorism (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.
- 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.
- In some cases, 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. Due to these, the ML threat was rated **Medium-High.**

RESIDUAL ML VULNERABILITY RATINGS

Based on the trends in recent years and ongoing cases, the ML Vulnerability level was rated as **Medium**.

ML RISK ASSOCIATED WITH THE NOTARIES SECTOR

- 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.

- It was found in some cases where Notaries were engaged for property acquisitions, they failed to detect that the source of their clients' funds which originated from illicit activities.

- Overall, the ML risk associated to this sector was rated as **Medium-High.**

NOTARIES SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE NOTARIES SECTOR

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

RESIDUAL TF VULNERABILITY

There was no domestic cases, but international exposure and typologies highlight the sector's potential susceptibility.

The residual TF Vulnerability level was rated **Medium-Low.**

TF RISK ASSOCIATED WITH THE NOTARIES SECTOR

On an international landscape, there exists cases for TF where Notaries were involved. However, on the domestic front, no such cases have been identified for Notaries during the assessed period.

As a result, the TF risk for the Notaries sector was rated **Medium-Low.**

REAL ESTATE SECTOR MONEY LAUNDERING RISK

OVERVIEW OF THE REAL ESTATE SECTOR

- Since May 2019, the real estate sector has been regulated for AML/CFT purposes under the FIAMLA, with the FIU as its supervisory body.
- 418 Real Estate Agents, Land Promoters and Property Developers were under the purview of the FIU for AML/CFT purposes.
- The real estate sector remain susceptible to unlawful property purchases through intermediaries.
- It faces a **Medium-High ML risk**, with offenders utilizing fraud, embezzlement and drug profits to conceal illicit wealth.

ML THREAT ASSOCIATED WITH THE REAL ESTATE SECTOR

Real estate is a popular choice for investment, but it also attracts criminals who use real estate in their illicit activities or to launder their criminal profits.

Perpetrators often deceive victims:-

- through social media or pose as real estate dealers
- By using fraudulent pretenses to create fictitious operations and obtain funds.

The ML threat in the real estate sector exists both nationally and internationally and is assessed as **Medium**.

RESIDUAL ML VULNERABILITY RATINGS

Following legislative improvements, "Hors Vue du Notaire" transactions are no longer permitted, and all real estate sales must go through a notary's account.

However, gaps and vulnerabilities persist within the sector.

The residual ML vulnerability level was rated as **High**, highlighting the significant risk of illicit financial activities through real estate transactions.

ML RISK ASSOCIATED WITH THE REAL ESTATE SECTOR

Investigation revealed that:-

- drug traffickers used bank loans to purchase bare land and build luxury properties, repaying loans with mixed illicit and legitimate proceeds to obscure the financial trail.

- Foreigners, including high risk clients have acquired properties in Mauritius.

Since July 2020, cash transactions for real estate are banned and all transactions must go through notaries, who are reporting persons.

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

REAL ESTATE SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE REAL ESTATE SECTOR

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

Hence, the TF threat in this sector is rated **Low.**

RESIDUAL TF VULNERABILITY

Although no direct evidence of TF cases was observed during the review period, vulnerabilities exist primarily due to:-

- the attractiveness to global investors,
- use of intermediaries,
- high-value transactions, and
- the existence of TF threats at national and international levels.

The residual TF vulnerability of the Real Estate Sector to terrorism financing was rated **Medium.**

TF RISK ASSOCIATED WITH THE REAL ESTATE SECTOR

For the period 2018-2022, no TF cases were identified for the Real Estate Sector.

The sector has been subject to regular and intensive outreach between 2020-2022.

Considering that the TF Threat associated with the Real Estate Sector was rated as **Low** while the residual TF vulnerability level was assessed as **Medium**.

The TF risk was rated as **Medium-Low.**

DPMS (JEWELLERY SECTOR) MONEY LAUNDERING RISK

OVERVIEW OF THE JEWELLERY SECTOR

- The sector has grown to become the top third manufacturing sector in the country and has a direct contribution to Mauritius GDP on an average of 0.4% for the period 2018-2022.

- The sector includes around **319** reporting persons as of August 2022.

- 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.

- It faces a **Medium-High ML risk.**

ML THREAT ASSOCIATED WITH THE JEWELLERY SECTOR

- Recent drug trafficking cases being investigated by LEAs, indicated possible lifestyle laundering in the jewellery sector whereby they were in possession of jewellery and precious stones up.

- Part of the ill-gotten gains of the traffickers was spent on expensive items to display signs of wealth/status.

- Investigation have also revealed that suspects were involved in the business of illegal money lender and taking properties and jewels as collateral.

- It faces a **Medium-High** ML threat**.**

RESIDUAL ML VULNERABILITY RATINGS

As per statistics gathered, there were few ML cases in which the DPMS was involved, and they are still under investigation. The DPMS remains vulnerable to Trade-Based Money Laundering and over/under invoicing justifying the residual ML vulnerability level of **Medium.**

ML RISK ASSOCIATED WITH THE JEWELLERY SECTOR

- 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.
- Overall, the ML risk in the DPMS sector was rated as **Medium-High.**

JEWELLERY SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE JEWELLERY SECTOR

While there is inherent potential for the sector to be misused for moving value for TF (as it's cash-based and deals with high-value portable goods), there were no reported cases suggesting the use of the jewellery sector for TF purposes during the review period.

Hence, the level in this sector is rated **Low**.

RESIDUAL TF VULNERABILITY

Mauritius has implemented several safeguards to prevent the abuse or misuse of the sector for terrorism financing purposes. These measures include, among others, cross-border controls and CFT obligations imposed on reporting persons.

Such controls help to mitigate the sector's exposure to TF risks, resulting in a **Medium-Low** rating for residual TF vulnerability

TF RISK ASSOCIATED WITH THE JEWELLERY SECTOR

The combination of low threat and safeguards in place, results in a **Medium-Low** TF risk for the DPMS sector.

ACCOUNTANCY SECTOR MONEY LAUNDERING RISK

OVERVIEW OF THE ACCOUNTANCY SECTOR

The accountancy sector in Mauritius operates under the regulatory oversight of the Mauritius Institute of Professional Accountants (MIPA), which acts as the umbrella body for professional and public accountants. MIPA regulates firms and individuals engaged in prescribed activities under the FIAMLA

The sector provides a broad range of services primarily to domestic clients and companies, with a minority of clients being Politically Exposed Persons (PEPs), High-Net-Worth Individuals (HNWIs), non-residents, or entities with foreign business interests. Some of the services offered by professional accountants include tax representation, acting as nominees, and establishing complex company structures.

As of September 2024, the number of accountancy firms conducting prescribed activities under FIAMLA and regulated by MIPA increased from 71 to 114. Based on risk assessments, 2 firms were classified as high risk, 7 as medium risk, and 105 as low risk.

There remain Mauritius-based accounting firms that are not within the AML supervisory scope, although accountants are licensed by the MIPA

ML THREAT ASSOCIATED WITH THE ACCOUNTANCY SECTOR

- Diverse clientele including domestic clients, international PEPs, High Net-Worth individuals and non-resident clients.
- Accountants were found to set up complex structures, act as nominees, and manage cash-intensive businesses linked to drug trafficker.
- Accountants acted as nominees and tax representatives for their clients..
- Auditors had certified figures for the assets of their clients that were incorrect, in a willfully blind manner.
- The services provided by professional accountants make them vulnerable to be unwittingly involved to ML activities by disguising the nature of the funds and creating complex layers.
- Threat was rated as **Medium**.

RESIDUAL ML VULNERABILITY RATINGS

- 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.

- However, the number of cases investigated has shown a declining trend, both prosecution and conviction rates were low.

- The residual ML vulnerability of the sector was rated as **Medium-Low.**

ML RISK ASSOCIATED WITH THE ACCOUNTANCY SECTOR

The ML risk rating for the accountancy sector is based on the following considerations:

- The sector services a diverse client base, including higher-risk categories such as Politically Exposed Persons (PEPs) and foreign legal entities.
- The presence of accountants in roles such as nominees or tax representatives, particularly in arrangements involving complex structures or cash-intensive businesses.
- While company formation and TCSP-related services are among the highest ML risk offerings by accountants, these fall under the separate regulatory oversight of the Financial Services Commission (FSC) and are assessed under the TCSP sector.
- Dealing with third parties outside Mauritius increased the level of risk

Taken together, these factors support the assessment of the sector's overall ML risk as **Medium.**

ACCOUNTANCY SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE ACCOUNTANCY SECTOR

- Business associated with accountancy services is mainly domestic. Further, accountants are under the obligation to conduct CDD.
- According to international trends, TF Threat associated with is low as the accountancy services are not attractive to terrorist financiers because of the CDD and KYC requirements.
- Therefore, the TF Threat associated to the sector was **Low.**

RESIDUAL TF VULNERABILITY

- There were no TF investigation involving professionals in the accountancy sector or evidence that the sector has been misused for TF purposes.

- The residual TF Vulnerability level was rated as **Low.**

TF RISK ASSOCIATED WITH THE ACCOUNTANCY SECTOR

- Business associated with accountancy services is mainly domestic.

- Likewise, there is no TF investigation involving professionals in the accountancy sector or disclosing the misuse of the sector for TF purposes. As a result. The TF risk associated to this sector was rated as **Low.**

GAMBLING SECTOR MONEY LAUNDERING RISK

OVERVIEW OF THE GAMBLING SECTOR

- The gambling sector presents a high (**ML**) threat, with 75% of cases citing betting gains to justify illicit funds.

- Criminals commonly exploit
  - casinos,
  - illegal betting, using methods such as split transactions and credit betting
  - horseracing

- The Gambling Regulatory Authority (GRA) oversees the sector, but
  - Only 80 operators are defined as reporting persons under FIAMLA; and
  - out of 80 reporting persons, as defined by FIAMLA, only 4 casinos and 21 gaming houses are under the purview of AML/CFT Supervision.

ML THREAT ASSOCIATED WITH THE GAMBLING SECTOR

Investigations revealed that criminals:-

- used casinos, gambling houses and racecourses to justify illicit funds as betting gain.
- used split transactions in casinos as a preferred method to link tainted funds to gambling activities.
- used proceeds from fraud and drug-related offences and placed them into betting activities to disguise their illicit origin.
- used illegal betting operations to launder money and evade detection by authorities

- Credit betting (*through mobile phone and huge amount of cash*) was observed as the new modus operandi of illegal bookmakers thus rendering their activities opaque.
- Due to the rise in these activities, the ML threat was rated **High**.

RESIDUAL ML VULNERABILITY RATINGS

The presence of unlicensed operators, mobile-based betting platforms coupled with other risk factors justify the residual ML vulnerability level of the gambling sector as **Medium.**

ML RISK ASSOCIATED WITH THE GAMBLING SECTOR

- Casinos and horseracing bookmakers are highly cash-intensive, making them vulnerable to ML risks.
- Criminals often claim gambling winnings to explain the origin of illicit cash, especially in drug trafficking or corruption cases.
- Illegal betting is another significant concern. The use of credit betting (especially via mobile phones) by unlicensed bookmakers has created an opaquer environment, where transactions can easily be hidden or disguised.
- Overall, the ML risk in the gambling sector was assessed as **Medium-High**

GAMBLING SECTOR TERRORISM FINANCING RISK

TF THREAT ASSOCIATED WITH THE SECTOR

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.

The TF Threat associated with the gambling sector was considered as **Low.**

RESIDUAL TF VULNERABILITY

Casinos and Gaming House 'A' operators conduct UN Sanctions screening of punters both upon entry to the premises and at the cashier level. These measures help to reduce the sector's vulnerability.

However, due to the inherently cash-intensive nature of the industry, certain structural vulnerabilities remain, which could expose it to potential misuse for terrorism financing purposes.

That said, there was no available information indicating that individuals in Mauritius had attempted to use online gaming platforms or websites in other jurisdictions for TF activities..

The TF residual vulnerability level is rated **Medium-Low.**

TF RISK ASSOCIATED WITH THE SECTOR

Although gambling may appeal to terrorist sympathisers as a fundraising method, there have been no reported cases of its misuse for terrorist financing (TF) in Mauritius, including through foreign online platforms.

As a result, the TF risk for the gambling sector is rated **Medium-Low.**

Mr Mahendra Raj Goorvadoo
Team Member: Other Financial Sector (Cooperatives Credit Union)

MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH COOPERATIVES CREDIT UNIONS (CCUs)

OTHER FINANCIAL INSTITUTIONS
CO-OPERATIVE CREDIT UNION (CCU) SECTOR
ML RISK

OVERVIEW OF CCU SECTOR

- Co-operative Credit Unions (CCUs) in Mauritius are member-owned financial cooperatives whose objects are to promote thrift among, and provide credit/ other financial services to its members. They operate on the principles of mutual assistance, democratic governance (one member, one vote), and financial inclusion, particularly for low- to middle-income individuals.
- The sector is primarily governed by the Co-operatives Act, the FIAMLA and the UNSA.
- The Registrar of Co-operative Societies as the Supervisory Authority oversees the registration, supervision and compliance process.
- CCUs in Mauritius operate only at domestic level.

OVERVIEW OF SECTOR – cont'd

For the purpose of the NRA exercise, CCUs are categorised as hereunder:

- Industrial based credit unions wherein membership is restricted by common bond to government employees, parastatals, hotels, educational institutions and private organizations among others; and
- Community based Credit union which is registered by members of a specific community.

For the assessment year under review, there were 164 CCUs with a turnover of around USD 22 million.

The contribution of the CCU sector to GDP is below 1% which is relatively low as compared to other financial sectors.

OFI – Co-operative Credit Union
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 Mauritius Police Force, 3 cases of predicate offence were registered where CCUs were involved- Embezzlement through misappropriation of funds.

As such, the **ML threat** associated to credit unions is considered **Medium Low.**

AML CONTROLS & RESIDUAL RISKS

As part of the CDD process, CCUs have established customer acceptance policies.

Ongoing training and awareness programs on AML/CFT concepts are conducted for licensees and staff with the assistance of designated authorities.

Clear and comprehensive framework for the registration of a credit union and issuance of a Certificate of Registration by the Registrar of Co-operative Societies.

Compliance with the UN Sanctions list screening requirements is ensured, with Nil Returns filed accordingly with relevant authorities.

Amendments to the Co-operatives Act are currently underway to address AML/CFT concerns, including enhancing the supervisory and enforcement powers of the Registrar

While amendments to the legal framework aim at mitigating risks, the Community Based CCU remain vulnerable as compared to an Industrial Based CCU

CCU SECTOR- ML VULNERABILITY

- Use of agents and the frequency of international transactions are non-existent in the CCU sector.

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

ML VULNERABILITIES - MAIN PRODUCTS/SERVICES

Product	Product characteristics	Inherent ML Vulnerability
Loans	Loans require approval at Credit Committee with scrutiny on repayment ability and purpose Face-to-face transactions are conducted- reduces risk of identity fraud Simple financial products offered as specified in the Rules of the society Only approved members with a known history and verified identity are eligible for loan application	Low
Deposits	Most transactions mainly effected through banks If cash deposit above required threshold or if the amount does not match the customer's profile, source of fund is required. No complex deposit products (foreign currency or anonymous accounts). CUUs do not offer remote or online deposit services- limits opportunity for layering of funds Third party deposits do not exist- policies restrict deposit from individuals	Low

ML RISK ASSOCIATED WITH THE OFI SECTOR



OFI- CCU SECTOR TERRORIST FINANCING RISK

CCU- TF THREAT

- During the review period, 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 organization/group/person was funded through funds obtained from credit unions.

Hence the **TF Threat** associated with the CCU sector is considered **Low.**

CCU- TF VULNERABILITY

The **TF Vulnerability** is rated **Low** based on the following factors:

- Outward/Inward international transactions/operations to countries/high risk geographical locations do not exist in the CCU sector.
- Client based profile- Mauritian Nationals
- Level of cash activity- Low; most of the transactions are channeled through banks
- Use of agents/intermediaries- does not exist

CFT CONTROLS & RESIDUAL RISKS

Comprehensive legal and regulatory framework- the FIAMLA and the UNSA.

Regular training and Outreach for staff and licensees on TF and CFT measures with the assistance of designated authorities.

Screening against UN Sanctions List for positive match and a Nil Return is submitted.

TF RISK ASSOCIATED WITH THE CO-OPERATIVE CREDIT UNION SECTOR



Mr A. Rughoobur
Team Leader: Company Service Providers

MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH COMPANY SERVICE PROVIDERS

OVERVIEW OF CSPs SECTOR

- CSPs are reporting persons as from 2019
- Population: 228 CSPs (as of 2022) under Supervision of ROC
- Includes those under Section 164 (company Secretary) and 167(A) of the Companies Act
- Servicing around 8000 Clients
- Provides mostly secretarial, formation agent and registered office address
- Only a few provide nominee shareholder services and some act as Bank Signatory for their clients

ML RISK ASSOCIATED WITH THE CSP SECTOR



CSPs SECTOR ML THREAT

- ML Threat –has been assessed by the Threat Team, as LOW

Main Factor: There was no local typologies to demonstrate that CSPs were used for money laundering.

CSPs SECTOR ML VULNERABILITY

- ML Inherent Vulnerability for the CSP sector : Medium

(i) Size / Volume: Medium Low

- 228 CSPs- Some 8000 Clients
- Turnover- relatively small size. 65% CSPs have turnover less than Rs 5 Million (USD 110,000)

(ii) Client Profile: Medium

- Mostly Private Domestic Companies
- Around 20 % of CSPs had clients with risk factors such as PEPs, High Risk Jurisdictions / countries, High Net-worth Individuals, Clients with criminal records, clients with complex structure, making use Professional Intermediaries .

(iii) Other factors such as Professional Secrecy, Use of Agents, Non-Face to Face Clients were considered

AML CONTROLS & RESIDUAL ML VULNERABILITY

- AML Controls: Medium Residual ML Vulnerability: Medium

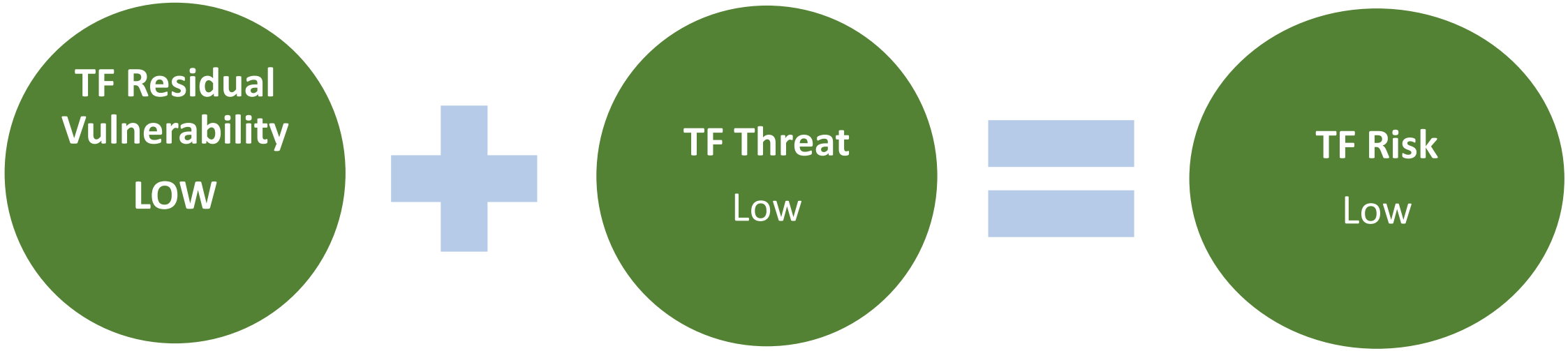
Variables	Ratings	
(1) Comprehensiveness of AML Legal Framework	Close to Excellent	
(10) Availability and Access to Beneficial Ownership information	Very High	
(3) Availability and Enforcement of Administrative Sanctions	High	
(6) Integrity of Business/ Profession Staff	High	
(11) Availability of Reliable Identification Infrastructure	High	
(7) AML Knowledge of Business/ Profession Staff	High	
(2) Effectiveness of Supervision/Oversight Activities	Medium High	ROC
(4) Availability and Enforcement of Criminal Sanctions	Medium High	
(5) Availability and Effectiveness of Entry Controls	Medium High	ROC
(8) Effectiveness of Compliance Function (Organization)	Medium High	CSPs
(9) Effectiveness of Suspicious Activity Monitoring and Reporting	Medium High	CSPs
(12) Availability of Independent Information Sources	Medium High	

ML RISKS ASSOCIATED WITH CSPs SECTOR

- ML Risk: Medium Low
  - The nature of the services that CSPs provide (Secretarial, Formation agent, Registered address)
  - The majority of CSPs are not bank signatories and they are less involved in processing payments and bank transfers for their clients
  - There is less exposure to foreign jurisdictions and cross border activities, as the CSP Sector service mostly domestic clients
  - There are local no typologies to demonstrate CSP have been abused for ML
  - 20 % of CSPs have some clients with high risk factors
  - Some AML Controls can be strengthened by ROC (Supervision and Entry Controls)
  - Effectiveness of Compliance function can be improved (eg independent audit and client risk assessment)

CSPs SECTOR TERRORISM FINANCING RISK

TF RISK ASSOCIATED WITH THE CSP SECTOR



CSPs SECTOR TF THREAT

- TF Threat – LOW
- There was no local typologies to demonstrate that CSPs were used for TF

CSPs SECTOR TF VULNERABILITY

- Inherent Vulnerability was assessed as LOW
- Inward and outward Transactions were mostly with Medium and low geographical locations (GTI 2023). 9 CSPs, as per the survey, were involved.

INHERENT VULNERABILITY FACTORS	ASSESSMENT RATINGS
Total size/volume of the business/profession	Medium Low
Outward International Transactions/Operations	At moderate level
Outward Transactions/Operations to higher risk geographical locations	At limited level
Inward International Transactions/Operations	At limited level
Inward International Transactions/Operations to higher risk geographical locations	At limited level
Client Base Profile	Medium Risk
Level of Cash Activity	Does not exist
Use of Agents, Vendors, other Intermediaries	Low
Suitability/utility for TF	Does not exist
Other Inherent Vulnerability Factors	Does not exist

CFT CONTROLS & RESIDUAL TF VULNERABILITY

- CFT Control: MEDIUM Residual TF Vulnerability: LOW

Variables	Ratings	
(1) Comprehensiveness of AML Legal Framework	Close to Excellent	
(10) Availability and Access to Beneficial Ownership information	Very High	
(3) Availability and Enforcement of Administrative Sanctions	High	
(6) Integrity of Business/ Profession Staff	High	
(11) Availability of Reliable Identification Infrastructure	High	
(13) Effectiveness of TFS implementation	High	
(7) CFT Knowledge and awareness of staff in the Sector	Medium High	
(2) Effectiveness of Supervision/Oversight Activities	Medium High	ROC
(4) Availability and Enforcement of Criminal Sanctions	Medium High	
(5) Availability and Effectiveness of Entry Controls	Medium High	ROC
(8) Effectiveness of Compliance Function (Organization)	Medium High	CSPs
(9) Effectiveness of Suspicious Activity Monitoring and Reporting	Medium High	
(12) Availability of Independent Information Sources	Medium High	

TF RISKS ASSOCIATED WITH CSPs SECTOR

- TF Risk: Assessed as LOW
- (i) No local typologies available
- (ii) Very few CSPs had international transactions –mostly with medium and low risk jurisdictions
- (iii) Nature of services provided by the CSPs
- (iv) CSPs Service mostly Domestic Clients
- (v) TF controls are Medium

Thank You