PART III
CONCLUSION

1. OVERALL SUMMARY

1.1 Rating of the Major Money Laundering Threats

ML threat levels emanating from each major predicate offence considered in the assessment are listed below with the rating. The major changes that can be identified since 2014 are bribery and corruption moving upwards, identification of new priority areas related to customs, environmental, and tax related offences.

i. Drug trafficking - ***Medium High***
ii. Bribery and Corruption - ***Medium High***
iii. Customs related offences including laundering of trade-based proceeds - ***Medium High***
iv. Fraud (including offences in relation to fraud - scams, criminal breach of trust, cheating or criminal misappropriation, or any combination thereof) - ***Medium***
v. Robbery (includes housebreaking, extortion, and theft) - ***Medium***
vi. Environmental and natural resource (ENV-NR) crimes - ***Medium***
vii. Illegal, Unreported and Unregulated (IUU) fishing and related unlawful activities (trafficking and smuggling) - ***Medium Low***
viii. Human smuggling/ trafficking - ***Medium Low***
ix. Tax offences - ***Medium Low***
x. Counterfeiting of currency - ***Low***

1.2 Rating of the Money Laundering Vulnerability

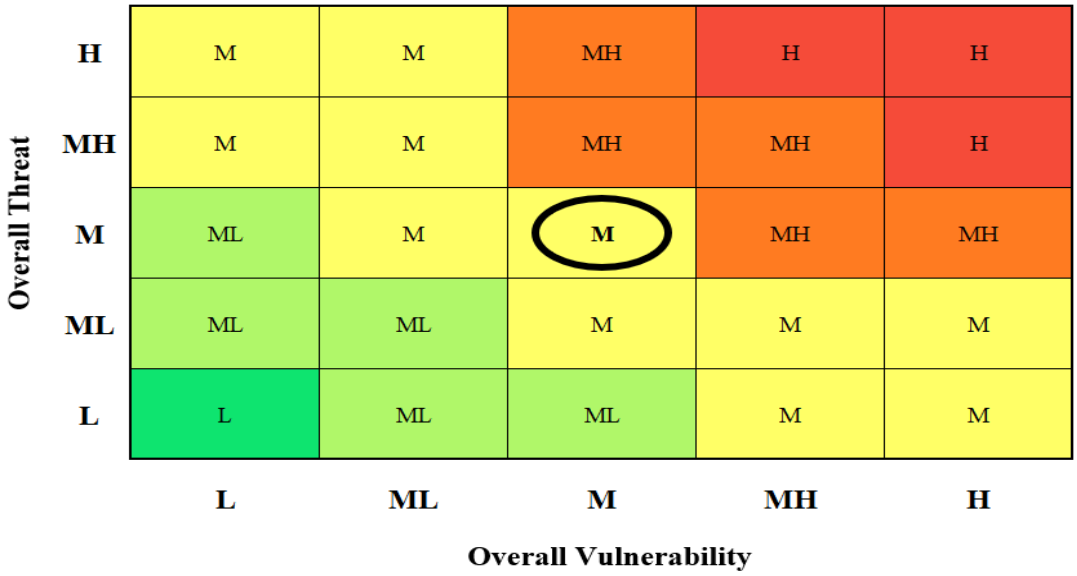
The overall national vulnerability level of Sri Lanka was determined at a ***Medium*** level. There is a slight improvement when considering the numerical values as a result of the various measures taken by authorities to address deficiencies which were identified in the previous ME. This progressive trend is also reflected in the overall sectoral vulnerability. The overall sectoral vulnerability also improved due to the initiatives of strengthening institutional compliance with the issuance of CDD Rules, Risk-Based Supervision and imposing of administrative penalties. On the other hand, the national combating ability has declined marginally when compared with the numerical values and determined at a Medium level. This marginal decline is due to the limited improvements in the law enforcement process.

1.3 National Money Laundering Risk and Terrorist Financing Risk

Accordingly, the overall ML threat and vulnerability of Sri Lanka has been assessed as ***Medium*** and the ML risk level in the country has been rated as ***Medium***.

As per the TF risk assessment, the TF threat, which is considered under four elements: the Domestic TF Threat, Outgoing TF Threat, Incoming TF Threat, and Transit TF Threat, is assessed as ***Medium***. Similarly, TF vulnerability under four specific areas, Vulnerability to Internal TF, Vulnerability to Outgoing TF, Vulnerability to Incoming TF, and Vulnerability to Transit TF is also assessed as ***Medium***. Therefore, the overall TF risk is assessed as ***Medium***.

Figure 1: Overall Money Laundering/Terrorist Financing Risk in Sri Lanka



1.4 Rating of the Sectoral Money Laundering Risk

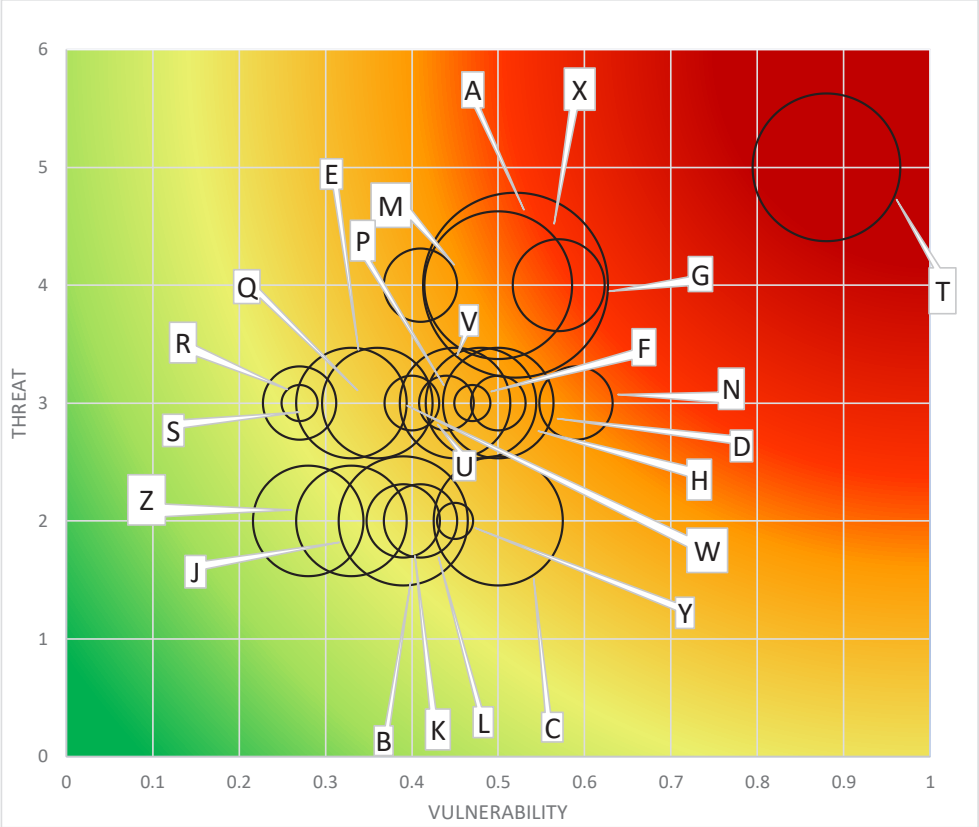
The overall ML threat, ML vulnerability and ML risk in each sector have been assessed as follows.

Table 1: Sectoral Money Laundering Threat, Vulnerability and Risks

Sector		ML Threat	ML Vulnerability	ML Risk
Banking		Medium High	Medium	Medium High
Other Financial Institutions Sector	Finance Companies	Medium High	Medium	Medium High
	Money or Value Transfer Service (MVTS) Providers	Medium	Medium	Medium
	Informal (Hawala/Hundi) Remitters	High	High	High
Securities	Stockbrokers	Medium Low	Medium	Medium
	Primary Dealers	Medium	Medium	Medium
Insurance		Medium Low	Medium Low	Medium Low
Designated Non-Finance Businesses and Professions (DNFBPs)	Casinos	Medium	Medium	Medium
	Real Estate Agents	Medium High	Medium	Medium High
	Dealers in Precious Metals and Precious Stones (DPMS)	Medium	Medium	Medium
	Lawyers	Medium Low	Medium	Medium
	Notaries	Medium		
	Accountants	Medium Low	Medium Low	Medium Low
	Trust and Company Service Providers (TCSPs)	Medium Low	Medium Low	Medium Low

When different sectors are plotted in a heat map, the Informal (Hawala/Hundi) Remitters sector stands out as the sector with highest ML risk. Similarly, Banks, Finance Companies and Real Estate Agents demonstrate a medium high ML risk. Most of the sectors are in the medium range while Insurance sector and few DNFBPs are at the medium low ML risk level.

Figure 2: Sectoral Money Laundering Risk



Sector	Short Form	Sector	Short Form
Banking	A	Other FIs - MVTS providers	N
Insurance	B	Other FIs - RDs	P
Securities - SBs	C	Other FIs - SLCs	Q
Securities - PDs	D	Other FIs - CSs	R
Securities - UTs and IMs	E	Other FIs - Samurdhi Banks	S
DNFBPs - Casinos	F	Other FIs - Hawala	T
DNFBPs - Real Estate	G	Other FIs - IPBs	U
DNFBPs - Gem and Jewellery	H	Other FIs - IMLs	V
DNFBPs - Accountants and Auditors	J	Other FIs - EMS	W
DNFBPs - TCSPs	K	Other FIs - LFCs	X
DNFBPs - Lawyers	L	Other FIs - UMFIs	Y
DNFBPs - Notaries Public	M	Other FIs - MFIs	Z

1.5 Risk Ratings of the Other Sectors

i. Financial Inclusion Products

With respect to the financial inclusion, for 8 categories of products which are Micro Loans, Small and Medium Enterprises (SME) Loans, Group Lending/Self Help Groups, Regular Savings/Fixed Deposits, Microinsurance, Deposit Backed Loan Products, Finance Leasing, and Pawning, initial and final risk assessment arrived as low risk. For MVTS and Remittances and Sale/Purchase of Foreign Currency, initial product risk assessment was medium and final risk assessment after considering risk mitigants, arrived at low risk.

ii. Newly Assessed Modules

- Overall threat of ENV-NR sector is assessed as ***Medium***. Hence, overall ENV-NR sector risk is also arrived as ***Medium***.
- National Level NPOs are sub-categorized into 6 main categories based on their nature of objectives/functions as Health and Sanitization, Training and Education, Relief Work, Poverty Alleviation and Entrepreneur Development, Human Rights and Environmental and Other NPOs and all of them are in the ***Low*** to ***Medium*** level of risk. As the majority of TF related STRs are reported on the suspicion of the abuse of NPOs in the Training and Education category, the risk of only that category is assessed as ***Medium***.
- As per the assessment, overall ML threat of the legal structures created in Sri Lanka is at ***Medium*** level and vulnerability of legal structures has been assessed as ***Medium High*** with medium attractiveness and low level strength of mitigation measures. Further, the entity risk remains at medium level for the Private Limited Liability Companies, Public Limited Liability Companies, Companies Limited by Guarantee, and Foreign Companies.
- The assessment of VASPs was conducted across 6 categories: Non-Custodial Wallet Providers, Custodial Wallet Providers, P2P Transfer Services, Virtual to Fiat Conversion Services, and V2V Conversion Services. All categories received ratings in the ***Low*** to ***Medium*** level of risk range, except for V2V Conversion Services, which was not assigned a rating.

2. LIMITATIONS OF THE ASSESSMENT

The assessment faced a number of limitations as outlined below:

- Since the entire NRA process took almost two years, it was challenging to keep the teams intact throughout the NRA process, especially, given staff transfers/rotations and turnover in stakeholder institutions.
- Lack of available and adequate data from the targeted sources in some instances. This was common among even in some formal financial sectors. However, this was more prominent in the informal financial sector, DNFBPs, Legal Structures, NPOs, VA/VASPs and ENV-NR Crimes. The data provided was not sufficient to come up with a proper ML risk rating for certain areas. This resulted in dependence on expert judgments for assessing particular areas of certain sectors.
- Where the data was available, some institutions were, however, not forthcoming with the information. This was applicable to some government institutions where they had to obtain official clearance before releasing the data. Some institutions were less cooperative during the assessment in providing information they possessed. At the same time, information from the informal sector was also held back due to the fear of the informal sector participants that they would have to face adverse repercussions as a result of divulged information related to their businesses.
- As the understanding of AML/CFT measures and ML/TF risk is still at a developing stage in the country, specifically, for some sectors, assessing the impact of ML/TF was challenging.
- Proceeds generated from criminal activities are usually not captured in some cases, as the templates used by LEAs for their usual reports do not demand data on proceeds generated. It was therefore difficult to obtain data on proceeds of crimes as the major focus is on the number of investigations, prosecutions, and convictions.
- Many government institutions are still maintaining data manually, and even in instances where data is maintained digitally, for some information there is no centralized databases from which information could easily be accessed.
- Some institutions faced the problem of retrieving data from their existing system to suit with the module requirements within the limited time allocated.
- The data collection was undertaken amidst the COVID-19 pandemic, and the economic crisis prevailed in the country. Therefore, most of the meetings conducted by the WGs were non face-to-face. This might have adversely affected the NRA process.
- The assessment was undertaken by individuals from various institutions who had other demanding institutional assignments during the same period. This caused issues with data collection and finalization of the draft report.

Nonetheless, the data limitations do not in any way invalidate the results of this assessment.

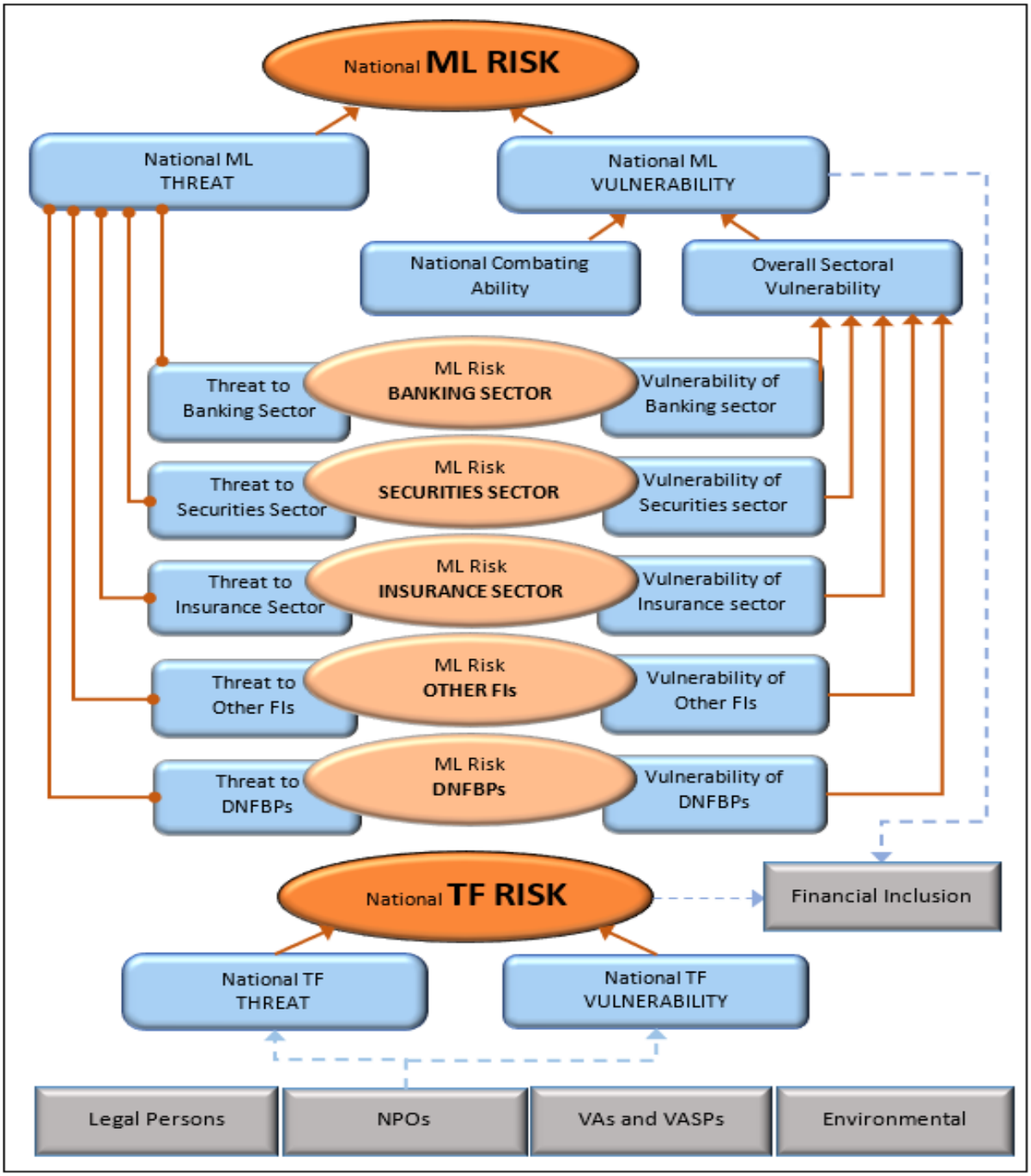
3. MAIN RECOMMENDATIONS OF THE NATIONAL RISK ASSESSMENT

Strengthening Legislative Framework
1) Amend/introduce relevant legislations to meet international standards and best practices (E.g., Proceeds of Crimes, NPO, Companies Act, Trust Ordinance, CIABOC, etc.)
2) Enhance the transparency of legal persons and arrangements on beneficial ownership requirements.
3) Develop regulatory mechanism on VA/VASPs, Real Estate Sector, informal money remitters.
ML/TF Investigations, Prosecution and Asset Recovery
4) Increase ML/TF investigations and prosecutions, especially, in relation to areas identified as generating higher proceeds of crime.
5) Develop policy guidelines to enhance the confiscation of proceeds of crime.
6) Build the capacity of the Investigators, Prosecutors, Judiciary, and the FIU on AML/CFT.
7) Establish a proper mechanism and an Asset Management Authority for asset recovery.
Risk-Based AML/CFT Supervision
8) Strengthen risk-based AML/CFT supervision and monitoring on FIs and DNFBPs.
9) Improve risk-based supervision capacity of Regulatory and Supervisory Bodies.
10) Establish a feedback and collaboration mechanism between the FIU, regulators, and RIs.
11) Impose proportionate and dissuasive sanctions for non-compliances observed and introduce necessary amendments to legislations where necessary.
12) Introduce fit and proper criteria for shareholders, beneficial owners and key management personnel across FIs and DNFBPs.
13) Increase the number of institutions covered for AML/CFT supervision in FIs and DNFBPs sectors.
Strengthen Domestic and International Cooperation
14) Promote formal international cooperation through MLA, counterpart agreements (Sri Lanka Police, Sri Lanka Customs, NSNGO, CIABOC, Regulators, etc.) as well as informal cooperation.
15) Promote domestic coordination and cooperation among relevant stakeholders to share information, intelligence, and experience.
16) Promote exchange of information and intelligence to support ML/TF investigations and prosecution among LEAs.
17) Strengthen feedback and case monitoring mechanism among LEAs in order to enhance information sharing on ML/TF investigations and prosecution.
18) Launch a regular consultative forum/mechanism to facilitate communication between supervisors and the private sector.

Strengthen Capacity and Enhance Awareness
19) Provide adequate human, financial and technological resources to where required.
20) Enhance awareness of all stakeholders on the ML/TF risk and vulnerabilities faced by the country.
21) Strengthen the independence, autonomy and integrity of all stakeholders involved in the AML/CFT framework.
22) Introduce advanced technologies into basic infrastructure such as Biometric NIC, integrated databases, online access to databases, shared KYC, etc.
23) Deepen AML/CFT awareness among public and private sector stakeholders including the general public.
24) Include AML/CFT as a subject in degree programmes in Universities, Law College, other private and public educational institutions.
25) Enhance the identification and reporting of ML/TF related STRs within FIs and DNFBPs.
Develop and Maintain Databases/Statistics
26) Develop a methodology for all LEAs and Competent Authorities to collect and maintain accurate statistics, electronically or in a promptly accessible manner on their operations.
27) Ensure that the databases maintained by competent authorities are accessible to LEAs and other competent authorities and even FIs and DNFBPs where necessary (E.g., Criminal record, Personal identification, Passport, Motor Vehicle, Land Registry, Company Registry, Trust Registry, etc.) free of charge or at a minimum cost.
28) Ensure information security and confidentiality of all statistics and databases.
Facilitate the Implementation of the National Financial Inclusion Strategy
29) Promote sustainable financial inclusion and increase financial literacy.
30) Increase the availability and usage of innovative financial products and services.
31) Identify low risk financial inclusion products and target groups.
32) Encourage launching financial inclusion products to low risk groups.
33) Introduce simplified CDD framework for financial inclusion products/low risk groups.

ANNEX I

Structure of the National Risk Assessment Tool



ANNEX II

Stakeholders of the National Risk Assessment Working Group

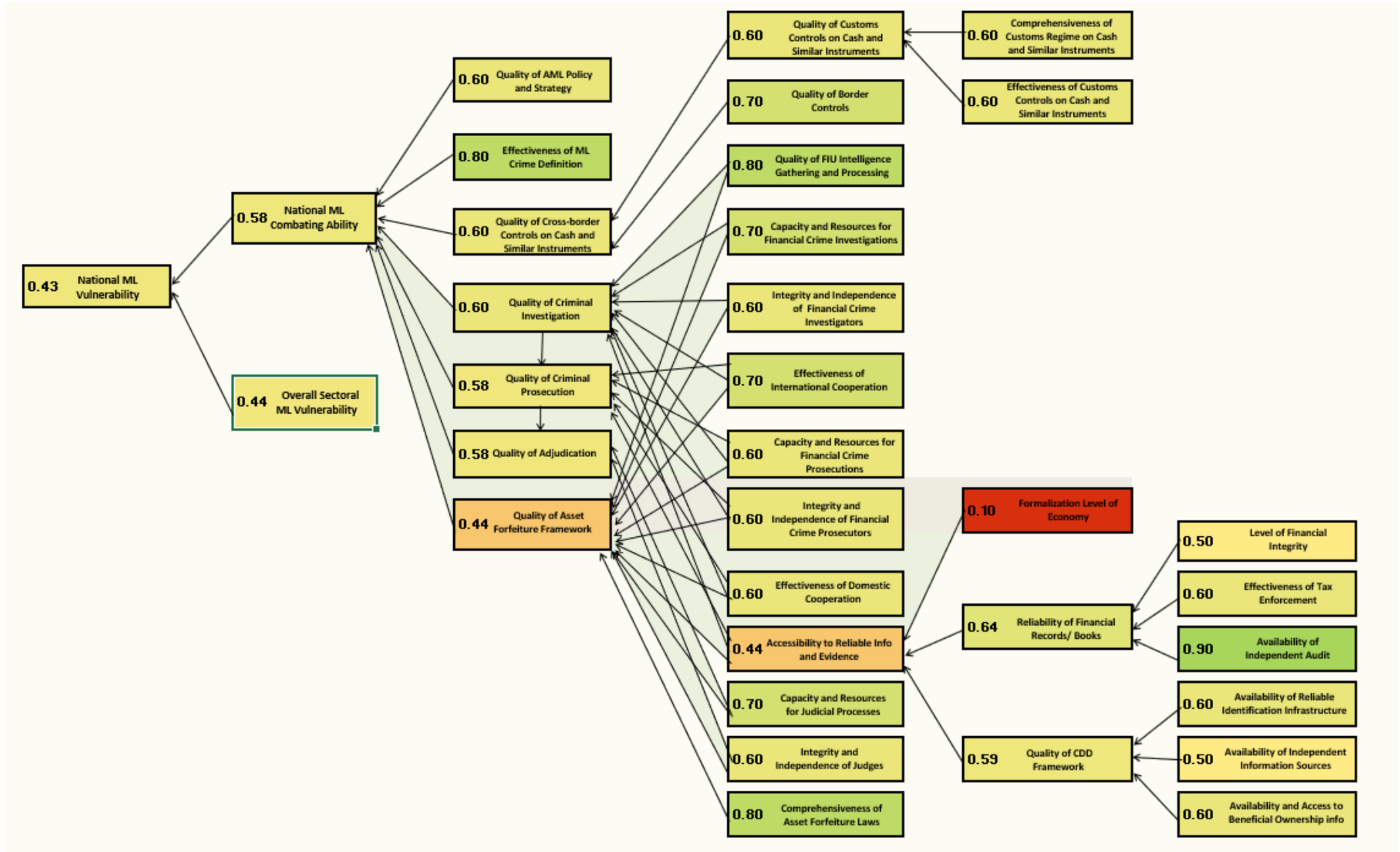
No	Stakeholder	Module
1	Attorney General's Department	ML Threat, National Vulnerability and TF Risk
2	Ministry of Justice, Prison Affairs and Constitutional Reforms	ML Threat, National Vulnerability and TF Risk
3	Ministry of Finance, Economic Stabilization and National Policies	ML Threat, National Vulnerability and DNFBPs Vulnerability
4	Ministry of Foreign Affairs	ML Threat, National Vulnerability and TF Risk
5	Ministry of Defence	ML Threat, National Vulnerability and TF Risk
6	Auditor General's Department	ML Threat and National Vulnerability
7	Commission to Investigate Allegations of Bribery or Corruption	ML Threat and National Vulnerability
8	Sri Lanka Police	ML Threat, National Vulnerability and TF Risk
9	Sri Lanka Customs	ML Threat and National Vulnerability
10	Department of Inland Revenue (Revenue Authority)	ML Threat, National Vulnerability and DNFBPs Vulnerability
11	Department of Immigration and Emigration	ML Threat and National Vulnerability
12	Registrar of Companies	DNFBPs Vulnerability and Legal Persons, Legal Arrangements and Beneficial Ownership-related Risk
13	Registrar General's Department	DNFBPs Vulnerability
14	National Dangerous Drugs Control Board	ML Threat and National Vulnerability
15	Ceylon Chamber of Commerce	DNFBPs Vulnerability
16	National Gem and Jewellery Authority	DNFBPs Vulnerability
17	Condominium Management Authority	DNFBPs Vulnerability
18	Department of Co-operative Development	Financial Inclusion Product Risk
19	Department of Samurdhi Development	Other Financial Institutions Vulnerability and Financial Inclusion Product Risk
20	Institute of Chartered Accountants of Sri Lanka	DNFBPs Vulnerability
21	National Secretariat for Non-Governmental Organizations	ML Threat, National Vulnerability, NPOs Risk and TF Risk
22	Securities and Exchange Commission of Sri Lanka	Securities Sector Vulnerability
23	Colombo Stock Exchange	Securities Sector Vulnerability
24	Insurance Regulatory Commission of Sri Lanka	Insurance Sector Vulnerability
25	Bar Association of Sri Lanka	DNFBPs Vulnerability
26	Condominium Developers' Association of Sri Lanka	DNFBPs Vulnerability
27	Sri Lanka Gem and Jewellery Association	DNFBPs Vulnerability
28	Sri Lanka Jewellery Association	DNFBPs Vulnerability

29	Ministry of Environment	ENV-NR Crimes
30	Department of Forest Conservation	ENV-NR Crimes
31	Department of Wildlife Conservation	ENV-NR Crimes
32	Central Environmental Authority	ENV-NR Crimes
33	Ministry of Fisheries	ENV-NR Crimes
34	Geological Survey and Mines Bureau	ENV-NR Crimes
35	Casino Marina	DNFBPs Vulnerability
36	Casino Bellagio	DNFBPs Vulnerability
37	Casino Bally's	DNFBPs Vulnerability
38	Bank of Ceylon	Banking Sector Vulnerability
39	Peoples Bank	Banking Sector Vulnerability
40	Sampath Bank	Banking Sector Vulnerability
41	HSBC Bank	Banking Sector Vulnerability
42	National Savings Bank	Banking Sector Vulnerability
43	Dialog Axiata PLC	Other Financial Institutions Vulnerability and Financial Inclusion Product Risk
44	Berendina Micro Investments Company Limited	Other Financial Institutions Vulnerability and Financial Inclusion Product Risk
45	MMBL Money Transfer (Pvt.) Ltd	Other Financial Institutions Vulnerability
46	SLT Mobitel PLC	Other Financial Institutions Vulnerability
47	LOLC Finance PLC	Other Financial Institutions Vulnerability
48	Singer Finance (Lanka) PLC	Other Financial Institutions Vulnerability
49	Assetline Leasing Company Limited	Other Financial Institutions Vulnerability
50	Candor Equities Limited	Securities Sector Vulnerability
51	First Capital Treasuries PLC	Securities Sector Vulnerability
52	NDB Wealth Management Limited	Securities Sector Vulnerability
53	Lynear Wealth Management (Pvt) Ltd	Securities Sector Vulnerability
54	Sri Lanka Insurance Corporation Limited	Insurance Sector Vulnerability
55	Ceylinco General Insurance Ltd	Insurance Sector Vulnerability
56	Ceylinco Life Insurance Ltd	Insurance Sector Vulnerability
57	Softlogic Life Insurance PLC	Insurance Sector Vulnerability
58	Senaratne Insurance Brokers (Pvt) Ltd	Insurance Sector Vulnerability
59	CBSL - Bank Supervision Department	Banking Sector Vulnerability and Financial Inclusion Product Risk
60	CBSL - Department of Supervision of Non-Bank Financial Institutions	Other Financial Institutions Vulnerability and Financial Inclusion Product Risk
61	CBSL - Department of Foreign Exchange	Other Financial Institutions Vulnerability
62	CBSL - Payments and Settlements Department	Other Financial Institutions Vulnerability and VAs and VASPs Risk

63	CBSL - Regional Development Department	Financial Inclusion Product Risk
64	CBSL - Public Debt Department	Securities Sector Vulnerability
65	CBSL - Economic Research Department	ML Threat and National Vulnerability
66	CBSL - Statistics Department	National Vulnerability and Other Financial Institutions Vulnerability
67	CBSL – Financial Intelligence Unit	All Modules

ANNEX III

Vulnerability Map



ANNEX IV

Typology 1: Trade-Based Money Laundering

The ongoing NRA coordinated by the FIU identifies Trade-Based Money Laundering (TBML) as an emerging ML/TF risk in the financial system of Sri Lanka.

The FIU received an STR from a bank about Company Z, a private limited company, established recently and based in Sri Lanka. The company is said to be engaged in importing different types of products such as apparel, electric items, yarn, solar panels, tyres, etc. All payments of Company Z are handled by its agent, Company Y located in Country A, at a nominal fee. Further, Company Z imports solar panels from Country B, a zero-tax product in Sri Lanka and imports tyres from Country C, a highly taxed product in Sri Lanka. Commercial invoices from Country B are overvalued because of zero tax and the commercial invoices from Country C are undervalued due to high tax.

The local bank account of Company Z receives large cash deposits which are immediately remitted as advance payments under outward telegraphic transfers to Country D for the purchase of apparel and yarn. Shipments of advance payments made one year ago have not yet reached Sri Lanka since no Customs Declarations were submitted to the bank for endorsement.

Additional information requested by the FIU from the STR reporting bank revealed that Company Z recently submitted a set of commercial invoices to the bank to facilitate payments to import electric items. However, the commercial invoices appear to be forged and a search of importers in the public domain revealed that they are not engaged in the said business. At the same time, as per the agency agreement provided by Company Z, a large fee is paid to Company Y as support service fees monthly where there is a minimal difference between the value of the import payment and the monthly support service fee.

Based on the unusual nature of account transactions, the bank made inquiries from Company Z. However, the given contact numbers were not reachable. Later, the bank visited the given address of Company Z but could not find any physical business therein.

The FIU analysed the case based on threshold reports, financial data, and beneficial owners with the support of the goAML system and Egmont Secure Web. Accordingly, information of the beneficial owners was obtained from countries A, B, and C through the Egmont Secure Web. The analysis revealed indications of a clear attempt at TBML by an organised group. The findings were forwarded to Sri Lanka Customs to initiate further investigations in this regard.

Above scenarios show that the financial sector has a key responsibility to prevent and detect TBML. For this purpose, the financial sector must be smart enough to identify possible red flags and indicators and some of them are given below.

- Undervalued or overvalued commercial invoices.
- Supplier/importer payments are made through third parties.
- Unusually large support service fees paid.
- Frequent advance payments followed by outward telegraphic transfers.
- Non-submission of Customs Declarations to confirm the physical movement of goods for the relevant advance payments made.
- Absence of a place of business.

ANNEX V

Typology 2: Misuse of Corporate Vehicles for Money Laundering Purposes and Beneficial Ownership

Misuse of corporate vehicles such as companies, trusts, foundations, and other types of legal arrangements for ML/TF purposes is a global paradigm, where criminals use complex corporate structures like special purpose vehicles spread across the globe, to launder money that they earn from illicit sources. In this regard, the FATF Recommendations require countries to ensure that adequate, accurate and timely information on the BO of corporate vehicles is available and can be accessed by the competent authorities in a timely manner.

The FIU received an STR from one of the LCBs, which elaborated on a recently incorporated Sri Lankan company, Company A and it had received a significant amount of IFTs from a different jurisdiction, to make a strategic investment in Sri Lanka. The Company A had received the said funds by way of a loan from a foreign company, Company B which is a fully owned subsidiary of another foreign company, Company C incorporated in a Tax Haven.

When scrutinized the ownership of the Company C by the FIU, it was revealed that a trust formed in another jurisdiction owns total shares of Company C and the specific trust was created by Mrs. Y for the benefit of Mr. X and his children. Mr. X is a citizen and a PEP of Country Z and his business ventures are spanning across the entire region. Some of the business ventures owned by Mr. X are allegedly engaged in illegal activities and are being investigated by the LEAs of those countries.

Apart from the information available domestically, the FIU in its analysis had gathered information about BO of aforesaid legal persons and arrangements from different foreign FIU counterparts through ESW and identified that the funds ultimately remitted to Sri Lanka for strategic investment purpose had been originated from the business ventures of Mr. X which are under investigation in Country Z and other foreign jurisdictions. The aforesaid complex corporate structures were apparently used by the offenders to conceal the origin and flow of the said funds.

Afterward, the FIU referred its analysis and the information gathered from foreign FIU counterparts about BO of the concerned legal persons and arrangements to the CID of Sri Lanka Police to assist their further investigations.

Accordingly in this case, the availability and the accessibility of adequate, accurate and timely information on BO of aforesaid companies and trusts were vital to identify the illegitimate origin of the funds flowed to Sri Lanka and to detect possible money laundering efforts.

Furthermore, the following have been identified as some general ML red flag indicators relating to misuse of corporate vehicles to disguise BO which the FIs should be vigilant.

- Customers provide insufficient or incomplete information about the BO of their institutions.
- Transactions that involve sender or beneficiary companies in offshore locations typically Tax Havens or high-risk jurisdictions.

- Institutions engage in transactions irregularly, occasionally, or that seems unusual for their industry.
- Transactions are in amounts that do not match with the company's business profile.
- Institutional customers produce fabricated documents to support significant amounts of remittances received or sent out.