
REPUBLIC OF NAMIBIA

# UPDATE TO THE 2020/21 NATIONAL MONEY LAUNDERING, TERRORIST AND PROLIFERATION FINANCING RISK ASSESSMENT

ISSUED: 30 JUNE 2023

FIRST UPDATE: 31 AUGUST 2023

SECOND UPDATE: 17 NOVEMBER 2023

***DISCLAIMER***

*The National Money Laundering, Terrorist and Proliferation Financing (ML/TF/PF) Risk Assessment of Namibia has been conducted as a self-assessment by Namibia, via stakeholders (NRA Project Team) involved in the combatting of such risks. Similar to the 2020 NRA, this exercise made use of some guidance, methodologies and other aspects in the risk assessment solutions and tools developed by the World Bank Group and the Royal United Services Institute (RUSI) to the extent possible. Such were amended or aligned to the extent possible to address challenges encountered. The said bodies did not in any way influence, nor participate in conducting the risk assessment. Data, statistics and information used in completing the risk assessment was independently sourced by the NRA project team. The findings and conclusions reflected herein are informed by the NRA Project Team's analysis and assessments of data, statistics and other qualitative information, after consulting as widely as possible.*

**ACRONYMS**

| | |
|---|---|
| AI | Accountable Institution as per Schedule 3 of the FIA |
| ACC | Anti-Corruption Commission |
| ADLA | Authorized Dealers in Foreign Exchange with Limited Authority |
| AML | Anti Money Laundering |
| AMLCFTCPF | Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation |
| AMLCFTCPF Council | Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Council |
| BIA | Banking Institutions Act, 1998 (Act No 2 of 1998) as amended |
| BIPA | Business and Intellectual Property Authority (Registrar of companies) |
| BoN | Bank of Namibia |
| CA | Companies Act, 2004 (Act No. 28 of 2004) as amended |
| CBFERTS | Cross Border Foreign Exchange Transaction Reporting System |
| CCs | Close Corporations |
| CCFAs | Customs Clearing and Forwarding Agents |
| CDD | Client/Customer Due Diligence |
| CID | Criminal Investigations Directorate |
| CTF | Combatting Terrorist Financing |
| CPA | Criminal Procedure Act, 1977 (Act No 51 of 1977) as amended |
| CPF | Combatting Proliferation Financing |
| CTRs | Cash Threshold Reports |
| DNFBPs | Designated Non-Financial Institutions and Businesses and Professions |
| EFT | Electronic Fund Transfer |
| ESAAMLG | Eastern and Southern African Anti Money Laundering Group, of which the Government of the Republic of Namibia is a founding Member |
| FATF | Financial Action Task Force |
| FBOs | Faith Based Organisations |
| FIA | Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended |
| FIC | Financial Intelligence Centre |

| | |
|---|---|
| FTFs | Foreign Terrorist Fighters |
| LEAs | Law Enforcement Authorities |
| ME | Mutual Evaluation |
| MHISS | Ministry of Home Affairs, Immigration Safety and Security |
| MME | Ministry of Mines and Energy |
| ML | Money Laundering |
| NAD | Namibian Dollars |
| NAMFISA | Namibia Financial Institutions Supervisory Authority |
| NamPol | Namibian Police |
| NBFIs | Non-Banking Financial Institutions |
| NPO | Non-Profit Organisation |
| NRA | National Risk Assessment |
| OPG | Office of the Prosecutor General |
| PF | Proliferation Financing |
| UN | United Nations |
| UNSC | United Nations Security Council |
| RI | Reporting Institution as per Schedule 3 of the FIA |
| STRs | Suspicious Transaction Reports |
| SRA | Sectoral Risk Assessment |
| SVA | Sectoral Vulnerability Assessment |
| TBML | Trade Based Money Laundering |
| TF | Terrorism Financing |
| POCA | Prevention of Organised Crime Act, 2004 (Act No. 29 of 2004) as amended |
| POCOTPAA | Prevention and Combating of Terrorist and Proliferation Activities Act, 2014 (Act No. 4 of 2014) as amended |
| PEPs | Politically Exposed Persons |
| VAs | Virtual Assets |
| VASPs | Virtual Asset Service Providers |

TABLE OF CONTENTS

A. INTRODUCTION ..... 7
B. MAIN OBSERVATIONS ..... 8
i. TF Risk Assessment ..... 8
ii. Legal Persons and Arrangements ..... 9
iii. Risks in VASPs ..... 10
iv. Trafficking in Persons (TIP) ..... 10
CHAPTER I: UPDATED TF ..... 11
RISK ASSESSMENT ..... 11
1. Methodology and Overall TF Risk Ratings ..... 13
1.1 Aggregating TF Threat and Vulnerability Outcomes ..... 13
1.2 TF Threats ..... 14
1.3 TF Vulnerability Considerations ..... 23
1.4 NPO Sector: TF Threat and Vulnerability Assessment ..... 35
CHAPTER II: LEGAL PERSONS ..... 50
AND ARRANGEMENTS ..... 50
2. Overview of Legal Persons and Arrangements ..... 52
2.1 Companies and Close Corporations ..... 52
2.2 Trusts ..... 53
2.3 Prevalence of threats ..... 53
2.4 CCs and *Inter-vivos* Trusts are Highly Exposed ..... 54
2.5 NAMPOL and the Prosecutor General's Asset Forfeiture Unit (AFU) ..... 56
2.6 Factors that enhance UBO Vulnerabilities ..... 57
2.7 Overall Risk Ratings ..... 60
CHAPTER III: VASPs' ..... 61
RISK EXPOSURE ..... 61
3. Overall VASP Risk Level ..... 63
3.1 Industry Size ..... 65
3.2 Industry Characteristics ..... 65
3.3 Threats in VASPs ..... 68
3.4 Vulnerability Considerations ..... 70
3.6 Other Sectors' Risk Exposure from VASPs ..... 80
CHAPTER IV: TRAFFICKING IN PERSONS (TIP) ..... 86
4. Threats and Vulnerabilities ..... 88

4.1 Threats and prevalence ..... 88
4.2 Vulnerabilities in Combatting Framework ..... 89
CHAPTER V: RECOMMENDATIONS ..... 91
5. Recommendations ..... 92
5.1 Supervisory Authorities ..... 92
5.2 Investigating and Combatting Authorities ..... 93
5.3 Financial Institutions, NBFIs and DNFBPs ..... 94
5.4 Trafficking in Persons ..... 95
ANNEXURE A: TF Vulnerability Map – Transit TF ..... 97
ANNEXURE B: TF Vulnerability Map – Incoming TF ..... 98
ANNEXURE C: TF Vulnerability Map: Outgoing TF ..... 99
ANNEXURE D: TF Vulnerability Map: Domestic TF ..... 100
ANNEXURE E: Basis for TF Vulnerability Risk Ratings and Prioritization List ..... 101
ANNEXURE F: SMUGGLING ATTEMPTS ..... 102
ANNEXURE G: TF RISK ASSESSMENT OUTCOMES (FOR OTHER NPO SUBSETS CAN BE AVAILED ON REQUEST) ..... 108
ANNEXURE H: ML/TF/PF VASP RISK ASSESSMENT OUTCOMES ..... 110
ANNEXURE I: CHAINANALYSIS API DATADUMP (wallet address screening outcomes) ..... 111
ANNEXURE J: Data on ties to high risk jurisdictions ..... 112
ANNEXURE K: NAMPOL statistics on ML & other commercial crimes ..... 114
ANNEXURE L: Anti-Corruption Commission (ACC) ML statistics ..... 118

## A. INTRODUCTION

The primary object of ML/TF/PF combatting and prevention frameworks is to ensure ML/TF/PF threats are prevented or timely detected and disrupted, criminals are sanctioned while depriving them of access to their illicit proceeds. In furtherance of this, countries periodically assess the effectiveness of their prevention and combatting frameworks with regard to domestic and international threats that such frameworks may be exposed to. The primary outcome of such assessment is to help inform and guide the implementation of prevention and combatting frameworks at national, sectoral and entity level. In keeping with this spirit, Namibia completed her first ever full scope NRA in 2012. Such NRA, amongst others, contributed to the eventual passing of the PACOTPAA and creation of a specialised terrorism combatting unit within the Namibian Police.

In 2015/16, an NRA update1 was undertaken with a particular focus on Trade Based Money Laundering (TBML). Such update resulted in the decision to include Customs Clearing and Forwarding Agents in the AML/CFT/CPF supervision framework, owing to their vulnerability to TBML and tax evasion related threats. In Namibia, risk assessments are continuing and ongoing activities that need to align to prevailing exposure and it is for this reason that risk assessment updates are conducted at least every three to four years while full scope assessments are undertaken every five to seven years. In line with this, Namibia revised and updated her 2015/16 risk assessment in 2018. This update focused on NPOs and their risk exposure to financial crimes. Observations and recommendations from this update led to the establishment of the FIC's NPO supervision framework in the third quarter of 2020.

The 2023 NRA update builds on the coverage of the 2020 full scope NRA, mainly focusing on areas highlighted in Namibia's 2022 Mutual Evaluation Report (MER). Such areas include VASPs, TF risks in general and NPOs' exposure to TF activities. VASPs have emerged as an alternative to the conventional financial system as we know it and naturally, such emergence is accompanied by risks. The need to periodically align risk understanding commensurate to the evolving VA ecosystem is paramount to combatting and prevention efforts, hence its inclusion in this year's review. Similarly, the need to expand on TF risks and in particular NPOs vulnerability serves to enhance on the limited scope covered in the 2020 NRA.

1 The need, timing, objectives and scope of NRA related activities is informed by observations from desk reviews.

The Republic of Namibia remains committed to combatting and preventing ML, TF and PF risks which have the impact to not only undermine the integrity of the financial system but derail economic as well as the national progression of democratic and developmental objectives.

The 2023 NRA project team stakeholders remained the same as in the 2020 NRA. See Appendix 16 of the 2020 NRA2 for a list of core project stakeholders.

Various Updates to the 2023 NRA Report:

**a. August 2023 Update**

The NRA's first revision was necessitated by guidance and updates on information relating to the following areas:

a. Incorporation of Annual Return data from high risk NPOs; and
b. Incorporating updates informed by supervisory observations in the VASP sector.

**c. November 2023 Update**

After considering guidance and inputs from the ESAAMLG Reviewers and International Monetary Fund (IMF), the Namibian authorities updated the 2023 NRA in November 2023, building on, amongst others:

d. the updated NPO risk related due diligence from the banking sector; and
e. contextual overview of the various types of legal persons and arrangements, amongst others.

## B. MAIN OBSERVATIONS

### i. TF Risk Assessment

National TF combatting effectiveness, rated as Highly Effective in the 2020 NRA has been revised to a Lower rating. Vulnerabilities in the national framework including limitations in the

2 https://www.fic.na/uploads/Publications/ML%20TF%20PF%20Risk%20Assessment%20Reports/2020%20NRA/Final%20Approved%20NRA%20Report%20Sept%202021.pdf

TF definition as per PACOTPAA, NAMPOL's combatting ability and supervision related shortcomings are core considerations not duly processed in the prior NRA. The TF threat rating on the other hand, previously rated as Low has not changed much. The overall TF risk rating has thus been revised from Low to Medium with this Update. Although the overall TF risk is Medium, with threats being rated low, detailed analysis herein suggests that an area of concern could be cross border threats from persons (especially within Namibia) that may be sympathetic to terrorist groups or related ideologies beyond the borders of Namibia.

In terms of NPOs which are most vulnerable to TF, the 2020 NRA found FBOs as highly exposed to TF risks. This update has also found charities to be highly exposed. Therefore, FBOs or religious activities, along with NPOs involved in charitable activities meet the standards of FATF-NPOs in Namibia. FBOs have been subjected to CTF outreach and monitoring activities since the third quarter of 2020 while similar work only started for charities in May 2023.

**ii. Legal Persons and Arrangements**

Section 8.22 of the 2020 NRA report, amongst others raised observations around vulnerabilities in accessing Ultimate Beneficial Ownership (UBO) information at a national level. This is attributed to shortcomings within trust and company registries administered by the Business and Intellectual Property Authority (BIPA) and the Master of the High Court. The 2020 NRA report however failed to assess the extent to which ML/TF and PF threats exploit shortcomings in various types of legal persons and arrangements such as trusts and partnerships. This is an essential element of a NRA as it would help FIs, DNFBPs, combatting and prevention authorities to duly prioritise their activities in as far as risks across different legal persons and arrangements are concerned.

The 2023 NRA update has found that overall, Close Corporations (CCs) appear most prominently abused in advancing ML activities. Companies also appear to have been significantly abused but to a lesser extent. Findings herein also suggests only *inter-vivos* trusts[3] may have been abused in advancing ML. Additionally, all such trusts that have been subject of investigations were Namibian initiated or founded (owned).

3 Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.

### iii. Risks in VASPs

The 2020 NRA covered VAs and VASPs to a limited extent given the limited size and nature of VASP operations in the country at the time. Such assessment also rated ML/TF/PF risks associated with VAs as Very High, primarily owing to the lack of any form of supervision and absence of a prudential licensing regime at the time. Over time, the sector has emerged and grown. Similarly, AML/CFT/CPF supervision commenced in September 2021. Having considered the impact of such supervisory activities, the national ML, TF and PF VASP risk level is revised from Very High to Medium level.

This update, along with the Virtual Assets Act will lay the foundation for prudential licensing, supervision and regulation of VAs, Initial Token Offerings (ITOs) and VASPs. This will further complement AML/CFT/CPF supervision activities and enhance overall risk mitigation associated with the sector.

### iv. Trafficking in Persons (TIP)

Namibia was upgraded to a Tier 1 country in the 2020 TIP Report for fully meeting the minimum standards for the elimination of human trafficking. This signalled relative effectiveness in combatting TIP. At the time, Namibia was the only country in Africa to achieve a Tier 1 ranking in 2020, joining 34 nations globally. In 2023 however, Namibia was downgraded[4] to Tier 2 owing to reduced effectiveness levels observed in combatting frameworks over the last 2-3 years.

4 https://www.state.gov/reports/2023-trafficking-in-persons-report/namibia/#:~:text=An%20NGO%20noted%20an%20increase,jobs%20and%20groom%20potential%20victims.

# CHAPTER I: UPDATED TF RISK ASSESSMENT

## *Chapter Summary*

*TF risk was assessed by aggregating outcomes of threat and vulnerability considerations. While TF threats speak to persons, events or activities that can resource or finance terrorist activities, TF vulnerabilities speak to the control frameworks designed to ensure that threats are prevented from supporting terrorist activities through financing or resourcing same.*

*As a UN Member State, Namibia has obligations to prevent and combat all forms of terrorism and terrorist financing activities nationally and internationally. Domestically, there are no known terrorist activities in Namibia, thus domestic funding of terrorist activities remains non-existent. Internationally however, there are jurisdictions with active terrorist activities and Namibian entities and persons engage in trade, remit resources or funds to other stakeholders in other jurisdictions. This inherently increases the risk of Namibia being party to or availing a platform through which terrorist activities can be resourced.*

*Historically, the Southern African region has not had active terrorist activities. This has changed with recent attacks in Mozambique, resulting in enhanced TF risks for neighbouring countries. South Africa remains one of Namibia's most significant trading partner. Naturally, South Africa being placed on the FATF list of countries under 'Increased Monitoring' inherently escalates Namibia's risk exposure emanating from or associated with that country.*

*National TF combatting effectiveness, rated as Highly Effective in the 2020 NRA has been revised to a Lower rating. Vulnerabilities in national combatting ability not previously considered have been duly processed in this update, especially with the guidance from Namibia's ME report. The TF threat rating on the other hand previously rated as Low has not changed much. The overall TF risk rating has thus been revised from Low to Medium, primarily due to considerations of significant Vulnerabilities, with TF threat levels remaining unchanged. Considerations herein suggests that an area of concern remains cross border threats from persons (within Namibia) that may be sympathetic to terrorist groups or related ideologies beyond the borders of Namibia.*

*In terms of NPOs, the 2020 NRA found FBOs as highly exposed to TF risks. This update has also found charities to be highly exposed. Therefore, FBOs or religious activities, along with NPOs involved in charitable activities meet the standards of FATF-NPOs in Namibia. FBOs have been subjected to CTF outreach and monitoring activities since the third quarter of 2020 while similar activities for charities only commenced in May 2023.*

## 1. Methodology and Overall TF Risk Ratings

It is common cause that the adopted methodology of assessing risks considers both vulnerability and threats in arriving at risk positions. Such methodology, premised on threat and vulnerability assessments is explained is sections 3 and 4 of the 2020 NRA report published on the FIC website5.

### 1.1 Aggregating TF Threat and Vulnerability Outcomes

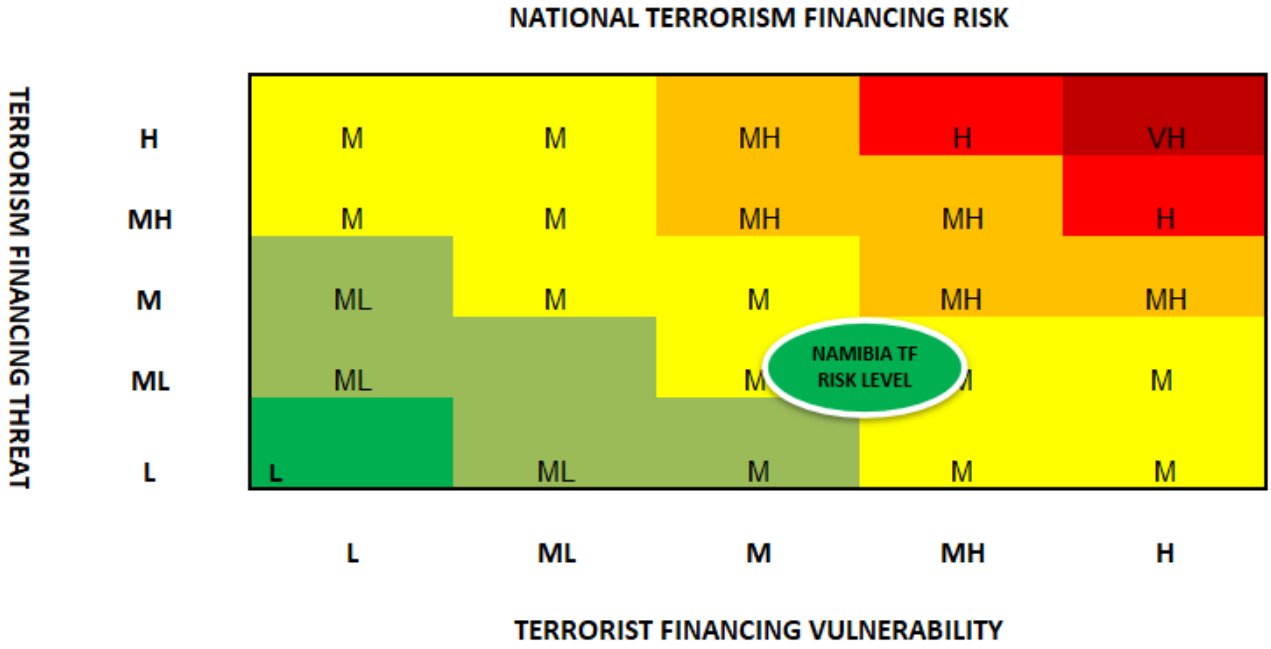



Figure 1: TF threat and vulnerability map

The 2023 NRA Update revised TF vulnerability (or extent to which controls can be abused) to **0.7 – 0.8 or 70% - 80%**. This suggests a **Medium High** TF vulnerability level because national combatting effectiveness is therefore only between 0.2 – 0.3 or 20% – 30%6.

Threats speak to persons, activities, events, cases etc that undermine or exploit TF vulnerabilities. The relatively lower number of TF threats (partly reflected in cases) that could

5 https://www.fic.na/uploads/Publications/ML%20TF%20PF%20Risk%20Assessment%20Reports/2020%20NRA/Final%20Approved%20NRA%20Report%20Sept%202021.pdf

6 The methodology used combines effectiveness to a total of 1.0 or 100% with splits occurring for ineffectiveness on the one hand and effectiveness on the other.

undermine such vulnerability over the period speaks to the reduced threats that materialized or were noted in the period. In assessing threat levels, **domestic TF Threats** were rated Low **(0.3 or 30%)** while **Foreign TF Threats** were rated Medium **(0.5 or 50%)**, resulting in an overall conservative[7] TF threat rating of **Medium (a score of 0.5 or 50%)** (see Figure 2). The threat outcomes generally concur with the 2020 NRA in that the area of concern is cross border TF threats (including foreign threats transiting through Namibia), especially from local persons who may be sympathetic to terrorist groups or related radical ideologies beyond the borders of Namibia.

Vulnerability levels in risk assessments speak to effectiveness of gatekeeping, preventative and combatting frameworks. Increased vulnerability, as per above, significantly drives overall TF risk exposure as national and institutional frameworks are increasingly open to abuse or unable to deter threats. This consideration overwhelmingly informed the increased national TF risk rating from the lower-level rating reached with the 2020 NRA.

### 1.2 TF Threats

Namibia's domestic TF threats can be summarised around the two cases, involving two subjects. Since 2014, the number of threats has not increased. Most of the threat ratings remain 'constant' as there has not been changes in TF threats for close to 10 years. This has to be cautiously appreciated as the absence or lack of threats can be attributed to ineffective detection and combatting mechanisms (which is a finding in this report).

The table below presents outcomes of TF threat ratings as per the 2023 NRA update. As mentioned above, the overall conservative rating of TF threat is Medium, a score of 0.5 or 50%.

7 more accurately a 'Medium-Low' rating would be appropriate.

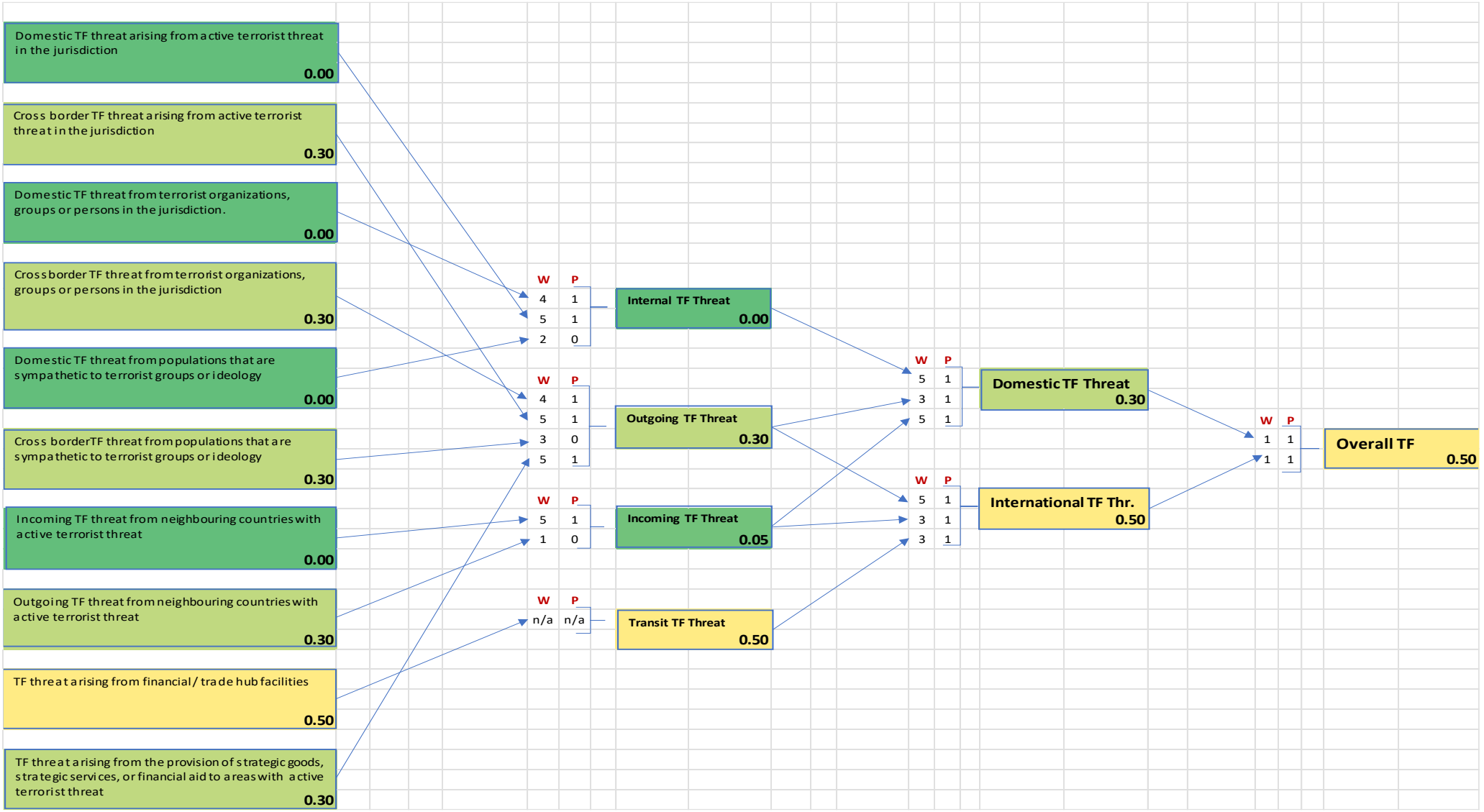



Figure 2: 2023 NRA Update/Review on TF Threat Assessment Outcomes

### 1.2.1 Threats Observed in STRs[8] and SARs[9]

Many concerns were raised in the 2020 and 2023 NRA update by participants suggesting that the TF risk is generally non-existent in Namibia but the risk assessment observations appear to suggest otherwise. FIs, DNFBPs and LEAs are required to appreciate considerations herein that inform TF risk conclusions in this regard.

Namibia, like all other countries must assess and continue to monitor their TF risks regardless of the absence of known threats. This approach should be similarly adopted at institutional level. The absence of known or suspected terrorists and TF cases does not necessarily mean that a jurisdiction has a low TF risk, similarly, it does not suggest that institutions in such jurisdiction are not exposed to TF risks. In particular, the absence of threats or cases does not eliminate the potential for funds or other assets to be raised and used or transferred abroad. Jurisdictions without active terrorism incidents may still need to consider the likelihood of terrorist funds being raised domestically (including through willing or defrauded donors) and transferred to areas with active terrorism. Equally, Namibia should, and has considered the likelihood of the transfer of funds and other assets through, or out of the country in support of terrorism, and the use of funds for reasons other than a domestic terrorist attack.[10]

TF process organically involves four stages being: raising, moving, storing or using funds and other assets. The TF threat assessment herein considered such stages. Such stages are certainly not sequential, nor linked to a specific known terrorism-related activity but serve as a general guide through which to appreciate TF. Below is a breakdown of such four TF stages:

a. **Raising funds** via numerous methods including legitimate means, donations, self-funding and criminal activity.

b. **Moving funds** to an individual terrorist or a terrorist group, network or cell through a series of knowing or unknowing facilitators and/or intermediaries by means of banking

[8] Suspicious Transaction Reports.
[9] Suspicious Activity Reports.
10 FATF Report: Terrorist Financing Risk Assessment Guidance, July 2019.

and remittance sectors, informal value transfer systems, bulk cash smuggling and crypto assets, and smuggling high-value commodities such as oil, art, antiquities, agricultural products, precious metals and gems, as well as used vehicles;

c. **Storing funds** intended for an individual terrorist or a terrorist group, network or cell by similar means used in moving funds while planning for their use; and

d. **Using funds** for payment when needed to further the terrorist organisation, group, network or cell's goals, including living expenses, to purchase weapons or bombmaking equipment and/or to finance terrorism operations.

The case study and sections below outline how Namibia's national, sectoral and entity level frameworks can be abused to advance TF through raising, moving, storing and to a limited extent using11 funds.

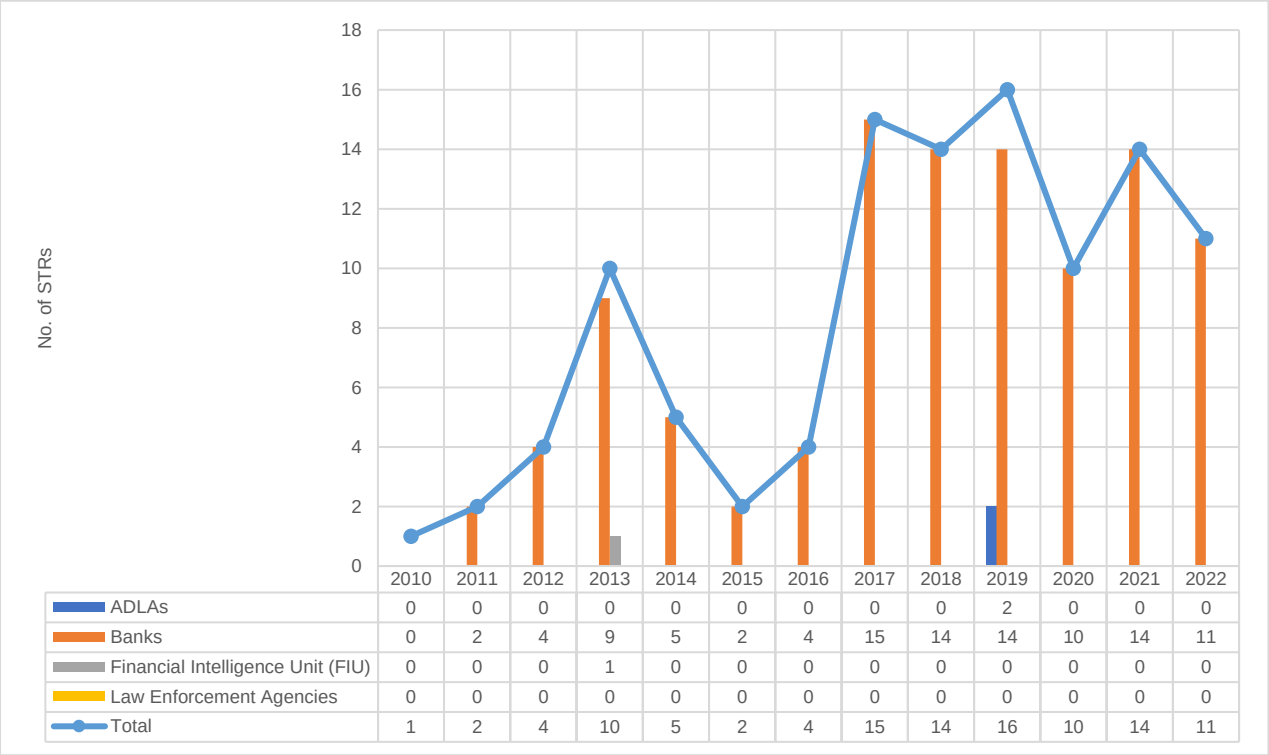
#### 1.2.1.1 Potential TF Threats

This section was primarily based on information from LEAs and FIC. It is essential for combatting authorities to fully understand the pressures and risks posed by terrorism and TF, in order to effectively prevent and duly investigate such offences. Considerations around how TF is facilitated through the financial system is one key element worth considering in this regard.

This section provides an overview of STRs related to possible TF threats filed by various sectors and reporting institutions since the reporting obligation commenced in 2009 until 31 December 2022. Worth noting is that when reports are received by the FIC, they are cleansed to determine each report's prioritization level. This process usually results in the decision of whether such reports should be escalated for further investigation (case files opened), or regarded as low priority. In some cases, some reports are set aside when it is concluded that there may not be merits for further investigations. Further, this section presents the total number of reports escalated for investigations based on potential TF activities.

11 The NRA findings are that using of funds, as the final stage of TF is more in the execution of terrorist activities or sustaining terrorist organisations and there has not been indications of same in Namibia.

Though the FIC has received many reports from the sectors suggesting potential TF, almost all such reports were determined to be false positives, after FIC analysis. The FIC has only escalated two intelligence reports to LEAs that had indications of potential TF. The STR-related information herein should thus be considered within this context.




| | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ADLAs | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| Banks | 0 | 2 | 4 | 9 | 5 | 2 | 4 | 15 | 14 | 14 | 10 | 14 | 11 |
| Financial Intelligence Unit (FIU) | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Law Enforcement Agencies | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 1 | 2 | 4 | 10 | 5 | 2 | 4 | 15 | 14 | 16 | 10 | 14 | 11 |

Figure 2: Summary of STRs received per sector

Figure 2 above presents a summary of STRs filed by sectors related to potential TF. The year 2019 saw the highest volume of reports related to potential TF offences with 16 STRs. It is worth noting that 96% of the reports originate from the banking sector. This reporting trend could be attributed to various factors, including the fact that banks appear to have the most matured AML/CFT/CPF control systems. It can also be argued that banking services are generally exposed to a higher risk of abuse for financial crimes as almost all other sectors make use of the banking systems. The ME, as per Immediate Outcome 4 found that TF is understood to some extent by FIs and to a negligible extent by DNFBPs.

As mentioned above, note that many such potential TF reports were deemed false positives within the FIC and not escalated to Law Enforcement for further investigation. Many a times, institutions simply reported potential TF based on the fact that transactions involved foreign individuals and entities who transferred funds or had links to high-risk jurisdictions without

further due diligence. The mere remittance to a high risk jurisdiction appears to be the sole indicator of potential TF in these cases, without other additional indicators.

### 1.2.2 Threats from Neighbouring and Other Countries

The 2020 NRA rightly speaks of potential TF threats emanating from Mozambique. It highlights how resources could be locally raised (or transited through Namibia) and moved to Mozambique and other terrorist groups around the world. The Republic of South Africa (RSA) remains one of Namibia's biggest trading partner and the two countries share socio-political ties beyond economics. The engagements between the two countries naturally renders Namibia vulnerable to TF risks that may emanate from RSA, inherently. An ongoing study to determine ties to high risk jurisdictions in the banking and ADLA sectors shows that South African citizens and entities represent the highest number of non-Namibians with footprints in these sectors. This further demonstrates the close ties between the two jurisdictions.

The FATF's findings12 suggesting ineffective frameworks to prevent and combat TF in RSA escalate Namibia's inherent TF threat level associated with or emanating from RSA.

a. **RSA under Increased Monitoring:** Below are a few conclusions from RSA's ME which enhances its risk exposure and that inherently exposes Namibia to same:

a. RSA falls short of the required ability to proactively identify potential TF cases by broadening its perspective, at the investigative stage, of acts that may be terrorism related;
b. RSA does not, more effectively integrate TF investigations into its framework;
c. RSA's policy of not pursuing domestic designation of terrorists, terrorist organizations and support networks as a tool to counter terrorism or TF;
d. The lack of policies, procedures and strategies in place to identify, investigate and prosecute all the different types of TF activity (e.g. collection, movement and use of funds or other assets);

12 RSA was recently greylisted by the FATF for not having effective measures in place to duly mitigate ML, TF and PF risks.

e. RSA, though efforts are at and advanced stage, has not begun the process of identifying NPOs who, based on their activities or characteristics, are at risk of TF abuse. The authorities have yet to apply specific measures, nor commenced monitoring or supervision, of NPOs at risk of TF abuse; and

f. Measures taken to deprive terrorists of their assets and to combat abuse of NPOs are not in line with RSA's TF risk profile. They do not reflect the number of terrorist related activities being monitored in the country, nor the risk posed by foreign terrorist fighters (FTFs).

The above demonstrates how Namibia could be vulnerable to TF associated with or originating from RSA by, amongst others, resources being moved through Namibia[13], terrorists using Namibia as a safe haven etc., in the advancement of terrorist objectives.

g. **OFAC Listing and Security Alerts:** The US embassy in RSA has twice raised the alarm in recent times about potential terrorism in the country. On 26 October 2022, it issued a security alert for a possible terror attack in Sandton, the financial centre of Johannesburg. Days later, it blacklisted four individuals and eight companies as terrorist financiers for Islamic State (ISIS). This followed media reports[14] showing that ISIS was using RSA to add to its war chest. The alleged RSA-based ISIS members designated by OFAC are said to be associates of Treasury-designated ISIS cell leader Farhad Hoomer, who continues to pursue ISIS's objectives in southern Africa and express the will and intent to attack the interests of the United States and its allies.

The case studies below centered around Namibia's potential TF incidences show how potential TF threats can arise through funds possibly being raised in Namibia and South Africa before being remitted to other countries.

***Case Study A***

13 At least given absence of active domestic terrorism (in Namibia).

14 Treasury Designates Members of ISIS Cell in South Africa, https://home.treasury.gov/news/press-releases/jy1084

*Mr-JJ has been on the Police radar and monitoring as a potential subject of terrorist acts and/or terrorist funding. The profiling of the subject started close to eight years ago and the initial case was registered in early 2019. The subject case docket bearing Windhoek CRXXXX was registered for contravention of section 2(1) & (2)- of the Prevention and Combating of Terrorists and Proliferation Activities Act, Act No. 4 of 2014.*

***Methods of moving funds and transfers***

*It was established that the subject has been sending funds to individuals in foreign countries in the middle east that are considered high risk in terms of terrorist activities through various foreign money exchange entities. With the information collected, it was discovered that the subject has been using Western Union and Money Gram remittance services via ADLA-A, ADLA-B, ADLA-C, and ADLA-D (these are money service businesses) to send and received the money. It is further confirmed that the subject sent and received money from countries such as Country-D, Country-T, Country-M, and Country-F through the same entities. These are countries highly exposed to TF or active terrorism in the middle east. Although the subject was operating in small businesses such as: car washing and dealing in hand second-hand or used car sales, as a source of income, this could not sustain him to frequently send money out of the country in the amounts that he did. This is further supported by the observation that the subject received over NAD 11 million into his bank account from a certain Mohammed Karim in the first quarter of 2023. He also appears to have received through his bank account, NAD 200,000 from the bank account Abdul Hasaan. These persons appear to be based in South Africa or used South African bank accounts in such names. The latter appears to have received such funds from a private company (Pty) Ltd, before remitting same to the bank account of the suspect.*

***Indications of UBO15 fronting***

*It was also established that the subject was last involved in the charcoal16 industry operating under two companies in the northern district as follows:*

***Legal Entity 1: A Close Corporation***

*a. Mr-KK (7%): Namibian national who is subject to TF investigations;*

*b. Mr-IM (38%): Country-K national;*

*c. Mr-Fx (30%): with dual citizenship of Country-S1 and Country-S2; and*

15 Ultimate Beneficial Ownership fronting

16 Namibia is a producer and exporter of charcoal. Note that this may or may not be a coincidence that the suspect is involved charcoal. There has been indications of terrorist financiers using the charcoal industry to raise or move funds. See: https://home.treasury.gov/news/press-releases/jy1499 - Treasury Designates Terror Operatives and Illicit Charcoal Smugglers in Somalia, May 24, 2023; See article at: https://ourworld.unu.edu/en/213bn-illegal-wildlife-and-charcoal-trade-funding-global-terror-groups titled - $213bn Illegal Wildlife and Charcoal Trade 'Funding Global Terror Groups'.

*d. Mr-HJ (25%): Country-S.*

***Legal Entity 2: Another Close Corporation***

*a. Mr-KK (10%): and*

*b. Mr-HAA (90%): Country-KK national.*

*Worth noting is that 80% of the other co-owners in these CCs hail from or hold nationality of countries rated as highly exposed to terrorism as per the Global Terrorism Index.*

***Case Study B***

*Mr-DD, a Namibian national, suspected of financing terrorism was subject to investigations some years ago. The subject was suspected to have joined an extremist Muslim guerrilla militant movement known as the Mujahideens abroad and was requesting friends and former colleagues to join the Jihad. The FIC conducted a financial analysis on the Bank-D account held in the name of the involved subject. Analysis showed that for the period of 23 October 2010 to 15 May 2015, the subject was a student at a university in South Africa and was also for some periods employed at an entity named GHGH Limited. The investigations further confirmed that the subject received a monthly salary ranging between NAD 3,000.00 and NAD 20,000.00 from such entity. Further, the analysis on the bank account confirmed that a certain lady (Ms-SS) has made regular cash deposits into the subject's bank account. Between January 2014 and December 2014, the subject transferred an amount of NAD 40,000.00 to an account in favour of "Sadaqa". It is alleged that Sadaqa is an Islamic term that means "voluntary charity"17*

*The analysis further revealed that the subject purchased an air ticket in February 2015. The subject was destined for the vicinity of IISS in Country - TTk and surrounding areas. Subsequently, on 16th February 2015, an amount of NAD 25,000.00 was transferred from the Bank-D account held in the name of Mr-JN into the subject's bank account. The subject later made several cash withdrawals in Country-SAA and other structured foreign cash withdrawals in Country-TTk. This potentially represents the final stages of the subjects' journey from Namibia to Country-TTk and beyond, to join the Islamic Jihad. It is further confirmed that the subject was reported killed abroad (see below media report18)*

17 Sadaqa is charity given voluntarily in order to please God. Sadaqa also describes a voluntary charitable act towards others, whether through generosity, love, compassion or faith.

18 https://www.facebook.com/254396731264515/posts/namibian-isis-trained-terrorist-killed-in-syriaby-max-hamata-in-oshakatian-islam/979458092091705/


### 1.3 TF Vulnerability Considerations

TF vulnerability refers to a country's effectiveness in preventing and combatting TF threats from materializing. This section revises and replaces relevant parts in section 1.3 of the 2020 NRA on TF vulnerabilities. The parts in section 13.4 that speak to potential TF risks associated with Mozambique remain unchanged. Sections 13.5 and 13.6 dealing with CTF combatting framework and TF vulnerability are complemented by this revised section. When conflicts arise in observations and conclusions from prior NRAs, the contents of this update are upheld and all other prior NRA positions in conflict are replaced (fall away).

As mentioned above, the 2023 NRA Update revised TF vulnerability to 0.7 – 0.8 or 70% - 80%. This suggests a Medium High TF vulnerability level because national combatting effectiveness is only between 20% – 30%19. *Annexures A to E*, attached hereto summarises outcomes of the latest TF vulnerability assessment at national level. Below are the vulnerability variables or considerations which informed such assessment.

19 The methodology used combines effectiveness to a total of 1.0 or 100% with splits occurring for ineffectiveness on the one hand and effectiveness on the other.

### 1.3.1 Shortfalls in TF Definition – PACOTPAA

Before the June/July 2023 PACOTPAA amendments, there were limitations in the country's TF definitions20. Whilst acknowledging that the said amendments effected now duly address previously identified deficiencies, relevant LEAs must be accorded time to demonstrate effective implementation of the said provisions, especially in investigating and prosecuting the full scope of TF offences, as per Recommendation 5.

### 1.3.2 Prosecution of TF

Until May 2023, while a few potential TF cases were observed over the years, Namibia has not prosecuted any TF case. This is mainly attributed to the different LEAs inability to identify TF activities even in cases where it was evident that there are potential TF activities. This inability to identify TF activities for prosecution stems from the LEAs approach to TF investigations which focuses on CT as opposed to TF. Namibia's long running case involving a subject suspected of supporting terrorist activities over the years was eventually arrested and charged with TF, amongst others in June 2023. *(See below media publication)*

20 For example, failure to comply with FATF Criterion 5.2(a) and (b).


Figure 3: As report in The Namibian Newspaper, subject arrested and charged with TF offence

### 1.3.3 National Anti-Terrorism and TF Strategy

The Mutual Evaluation observed that TF investigation is not duly integrated and used to support the National CT Strategy. Such strategy does not have dedicated pillars to deal with TF matters as it is primarily focused on the offence of terrorism. It fails to duly breakdown TF as an offence and how relevant preventative and combatting activities at national level deals

with the relevant elements of TF including raising, moving of funds or assets. Such has been revised and awaits adoption/approval from relevant authorities.

### 1.3.4 Poor Mechanisms to Identify and Investigate TF Effectively

TF cases are **not routinely identified and investigated**. There are no mechanisms in place which NAMPOL: CID relies on to proactively or routinely identify TF threats and take the necessary preventative or combatting actions. Understanding TF overall amongst NAMPOL is inadequate, this was observed from the ME findings. The NCIS and FIC have a better TF understanding though. NAMPOL's challenge in this regard is reflected through the inability to identify and investigate TF activities even in cases where it was evident that there are potential TF activities *(See examples in the TF Typology Reports issued by the FIC in May/June 2023 at https://www.fic.na/index.php?page=fic-trends-and-typology-reports) .*

### 1.3.5 Poorly Resourced TF Combatting Unit

The AML-CFT Division under **Namibia's CID has generally been understaffed over the last five years. At some point, the unit only had one staff member.** At some point a few years ago, such staff member had also left the unit. There are also no indications that such staff member was duly trained to undertake TF investigations effectively. In the last week of May 2023, four new staff members were transferred to the unit. It must however be said that such new staff members were not duly trained at the time of this assessment and more would need to be done to build their capacity before effectiveness levels can be attained. The first training on terrorism and TF they would have been exposed to was one held in May 2023, presented by experts from the Kenyan Government. The severe resource constraints including trained staff hampers effective identification and investigation of potential TF incidences. This is the underlying reason for Namibia's inability to proactively identify, investigate and prosecute TF cases and significantly reduces over combatting ability, thus enhancing vulnerability. This variable would be revised in future NRA updates depending on the effectiveness of the newly staffed CFT unit in NAMPOL.

### 1.3.6 Poor Coordination and Collaboration

The level of coordination and collaboration effectiveness, amongst others, was assessed on the lack of means to ensure TF matters are routinely identified and investigated and combatting authorities' resources dedicated towards such collaborative efforts. While collaborations and coordination on ML threats can be demonstrated, authorities could not demonstrate effectiveness on TF matters. The lack of dedicated resources in NAMPOL, as mentioned above, which is the primary investigating authority for terrorism and TF, also makes it challenging to ensure effective collaboration.

Namibia established an Inter-Agency Memorandum of Cooperation known as the Integrated Investigative Task Team (IITT). It is made up of the FIC, the NAMPOL and other LEAs with a mandate to cooperate domestically on AML/CFT investigations. While the IITT framework is supposed to ensure TF identification and prosecution, by end of May 2023 however, the task team had no record of having investigated TF, nor caused the prosecution thereof. This position only changed in late June 2023 with the charging of a suspect for TF.

The ideal expectation would be to have a standing task team or similar body which comprises of all the authorities mentioned in the IITT plus Immigration officials and others to ensure it has a broader representation. Such task team ought to have timely access on a continuous basis to records of cross border movements, imports, exports, records within the financial sector, records of all other possible threats such as refugees etc, visibility around smuggling corridors that Namibia is linked to etc.

### 1.3.7 TF Preventive Measures and Targeted Financial Sanctions (TFS)

Namibia has failed to implement TFS measures on TF without delay over the last few years. The implementation of TFS is hampered by the delayed procedure. TFS implementation only commences in practice after publication in the Gazette of a freezing order by the Minister responsible for Home Affairs, Immigration, Safety and Security. Once received from Namibia's Permanent Mission at the UN, the MIRCO has 48 hours to transmit the 1267 designations to the Minister responsible for Security and Safety who also has another 48 hours to publish the sanctions list by notice in the Gazette and issue the freezing order. This falls short of the 'without delay' expectation which speaks to implementing TFS 'within hours'.

Additionally, until April 2023, the FIC's supervision relating to TFS remained inadequate. The inspections or compliance assessments only limited TFS reviews to sanctions screening. No due regard to effectiveness of freezing and prohibition requirements although the PACOTPAA provides for same. Targeted TFS compliance assessment activities were undertaken in the months of April to June 2023. The findings overwhelmingly suggests that while screening appears to be undertaken, significant room for improvement on assets freezing without delay and prohibition, especially in DNFBPs remains a concern. A Directive and different Guidance Notes on TFS were workshopped and issued to help enhance supervised sectors' appreciation of TFS measures that need to be implemented. Over time, the impact of such actions will be considered.

Additionally, until mid-2022, the FIC has not timely communicated UNSC updates as can be seen in Table 1 below:

| UNSC Lists Circulars | Date of Update of UNSCR | Year | Date of issuing of Circular by FIC | Date Posted on FIC website | Days taken to post |
|---|---|---|---|---|---|
| FIC Circular 1 of 2022 | 03-Jan-22 | 2022 | 03-Jan-22 | 07-Jan-22 | 4 days |
| FIC Circular 2 of 2022 | 17-Jan-22 | 2022 | 17-Jan-22 | 19-Jan-22 | 2 days |
| FIC Circular 3 of 2022 | 24-Jan-22 | 2022 | 24-Jan-22 | 25-Jan-22 | 1 |
| FIC Circular 4 of 2022 | 07-Mar-22 | 2022 | 14-Mar-22 | 05-Apr-22 | 23 days |
| FIC Circular 5 of 2022 | 01-Apr-22 | 2022 | 04-Apr-22 | 05-Apr-22 | 1 |
| FIC Circular 6 of 2022 | 27-May-22 | 2022 | 30-May-22 | 27-May-22 | 0 |
| FIC Circular 7 of 2022 | 30-Jun-22 | 2022 | 01-Jul-22 | 30-Jun-22 | 0 |
| FIC Circular 8 of 2022 | 26-Jul-22 | 2022 | 26-Jul-22 | 28-Jul-22 | 2 days |
| FIC Circular 9 of 2022 | 14-Sep-22 | 2022 | 19-Sep-22 | 19-Sep-22 | 0 |
| FIC Circular 1 of 2023 | 16-Jan-23 | 2023 | 17-Jan-23 | 17-Jan-23 | 0 |
| FIC Circular 2 of 2023 | 27-Jan-23 | 2023 | 30-Jan-23 | 30-Jan-23 | 0 |
| FIC Circular 3 of 2023 | 02-Feb-23 | 2023 | 03-Feb-23 | 03-Feb-23 | 0 |
| FIC Circular 4 of 2023 | 26-Apr-23 | 2023 | 28-Apr-23 | 28-Apr-23 | 0 |
| FIC Circular 5 of 2023 | 02-Jun-23 | 2023 | 05-Jun-23 | 05-Jun-23 | 0 |
| FIC Circular 6 of 2023 | 05-Jun-23 | 2023 | 06-Jun-23 | 06-Jun-23 | 0 |
| FIC Circular 7 of 2023 | 30-Jun-23 | 2023 | 04-Jul-23 | 05-Jul-23 | 1 |
| FIC Circular 8 of 2023 | 24-Jul-23 | 2023 | 24-Jul-23 | 24-Jul-23 | 0 |
| FIC Circular 9 of 2023 | 16-Aug-23 | 2023 | 20-Aug-23 | 21-Aug-23 | 1 |
| FIC Circular 10 of 2023 | 05-Oct-23 | 2023 | 06-Oct-23 | 06-Oct-23 | 0 |

Table 1: Timeliness within which UNSC updates are communicated to FIs and DNFBPs

The FIC's supervision function has recruited two persons with IT skills in early 2023 to drive automation and digitization of all supervision activities. The impacts thereof are being felt.

Part of the IT personnel's responsibilities since March 2023 is to timely upload such UNSC update circulars on the FIC website, a function previously assigned to the IT team of the Bank of Namibia. This arrangement with the Bank of Namibia partly contributed to delays in publication of update notices on the FIC website.

### 1.3.8 Targeted Approach, Outreach and Oversight of High Risk NPOs

The 2020 NRA found that Namibia has identified FBOs as the FATF NPOs. This update, as noted herein below (1.4) found Charities as inherently exposed to TF risks as well. The FATF NPOs has thus been expanded to include all charities. The position with charities is not entirely clear, though the FIC maintains that such are also FATF NPOs. The following summarizes concerns which does not reduce TF risks associated with FATF NPOs:

a. **Absence of an effective licensing and market entry regime:** The proposed FIA amendments to have the FIC assume some licensing and prudential responsibilities of the FATF NPOs is yet to be tested as the FIA is not yet amended by June 2023. This largely undermines all other preventative and combatting activities associated with NPOs; and

b. **Outreach and monitoring activities:** The FIC has over the last 12 months conducted periodic monitoring activities over the high risk NPOs. Monthly periodic reports are produced that captures outcomes of analysis of the financial activities of high risk NPOs. This is very helpful but more can be done in terms of oversight and targeted outreach activities to enhance NPOs' combatting abilities. While all high risk NPOs are known to the FIC, timely creation or enhancing of governance frameworks within such NPOs could be an area that will add value to prevention activities. Annual returns have been introduced to be filed by all FBOs and Charities NPOs with the FIC. Other returns introduced are for banks to avail banking information they have on NPOs. The impact of information from such returns is yet to be seen.

### 1.3.9 Illegal Entry and Exit

It is well documented in sections 8.11 to 8.13 of the 2020 NRA that Namibia has porous borders, some challenges with effective entry/exit as well as border regulations in general. Vulnerabilities emanating from same can impact TF risks overall. In the twelve months leading up to June 2023, Immigration Officials have not recorded people with irregular or fake passports attempting to enter Namibia. There were two cases however in which two passengers from South Africa attempted to use legitimate passports that were fraudulently obtained from that country, to enter Namibia. All of them were refused entry and sent back to South Africa for further handling. This section should be considered with observations in sections 1.3.10 and 1.3.12 below.

### 1.3.10 Cross Border Smuggling Risks

This section should be considered with observations in section 1.3.12 herein which deals with ties to high risk jurisdictions. Similarly, sections 8.11 to 8.13 of the 2020 NRA presents a summary of challenges related to border regulations and the effectiveness thereof, worth noting in this regard. It is common cause that such challenges remain vulnerable for TF abuse. The ease with which persons can illegally smuggle items and contrabands throughout the country's borders reflects vulnerabilities that can similarly be exploited to advance TF activities, especially given that Namibia's TF risk is higher with cross border or international elements and not domestically. Building onto the 2020 NRA observations in *Annexure F* list incidents of smuggling and attempted smuggling through the country's borders in 2021 and 2022.

Overall, the smuggling cases record in 2021 to 2022 suggests that smuggling corridors include China, South Africa and Brazil with the latter being involved in cases related to drugs smuggling. To a lesser extent, countries such as Hong Kong, Egypt and Zambia also feature. The port of Walvis Bay and Noordoewer feature prominently as a preferred ports for smuggling goods and contrabands in large quantities while Hosea Kutako International appears to commonly detect cash smuggling attempts.

It is also worth noting that from 30 April 2021 to 30 September 2021, NamRA participated in the WCO INTERPOL operation codenamed "STOP II" focusing on counterfeit/illicit medicines and medical supplies while also maintaining a general focus on all goods related to the

COVID-19 pandemic which may pose a threat to consumer health and safety. Out of 146 countries, NamRA reported 107 ranking no. 7 out of 146 countries. In 2020 during STOP I out of 42 cases reported by the East and Southern Africa region, NamRA reported 41 cases, achieving a score of 97.61%. The higher detections and reporting could either suggest higher incidences of smuggling or detecting effectiveness by Customs officials in such countries. See Figure 4 below.

ANNEX I : Reporting Members and their reported seizures

| No. | Reporting Member | Phase I | Between Two Phases | Phase II | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 30 April-4 June | 5 June - 24 June | 25 June - 4 July | 5 July - 11 July | 12 July - 18July | 19 July-25July | 26 Jul.- 1 Aug. | 2-8Aug | 9-15 Aug. | 16-22 Aug. | 23-29 Aug. | 30 Aug.- 5 Sep. | 6 Sept.- 12 Sept. | 13-19 Sept. | Total |
| 1 | BENIN | 79 | - | 48 | 14 | 4 | 15 | 10 | 22 | 24 | - | 16 | 16 | - | 28 | 276 |
| 2 | NETHERLANDS | - | - | 13 | 57 | 31 | 8 | - | - | - | - | - | 30 | - | 57 | 196 |
| 3 | FRANCE | - | 30 | 15 | 42 | - | - | - | 43 | - | - | - | 14 | - | 23 | 167 |
| 4 | UNITED KINGDOM | 10 | - | 7 | 61 | - | 4 | - | - | 6 | 12 | 8 | 31 | 21 | - | 160 |
| 5 | PERU | 92 | 26 | - | - | 23 | - | - | - | - | 8 | - | - | - | - | 149 |
| 6 | NAMIBIA | 32 | 16 | 3 | 18 | 1 | 6 | 1 | 2 | 9 | 5 | 1 | - | 11 | 2 | 107 |
| 7 | TOGO | 29 | 7 | - | 14 | - | 32 | 10 | 1 | 2 | - | - | - | - | 1 | 96 |
| 8 | JAPAN | 6 | 14 | 15 | 17 | 6 | 4 | 1 | 1 | 7 | - | 7 | - | 3 | 2 | 83 |
| 9 | ARMENIA | 8 | 15 | - | 0 | - | - | - | - | - | - | - | - | 47 | - | 70 |
| 10 | NIGERIA | 61 | - | 5 | - | - | - | - | - | - | - | - | - | - | - | 66 |
| 11 | RUSSIAN FEDERATION | 5 | 3 | - | 4 | 3 | 8 | 25 | 1 | 1 | - | 1 | 2 | 4 | - | 57 |
| 12 | SENEGAL | 34 | - | - | - | 22 | - | - | - | - | - | - | - | - | - | 56 |
| 13 | SWITZERLAND | 18 | - | 17 | - | - | - | 20 | - | - | - | - | - | - | - | 55 |
| 14 | COTE D'IVOIRE | - | - | - | - | - | - | - | - | - | - | 6 | - | 49 | - | 55 |
| 15 | BANGLADESH | - | - | - | 5 | 2 | 1 | - | - | 8 | - | 10 | - | 7 | 21 | 54 |
| 16 | NORTH MACEDONIA | 39 | 3 | - | - | - | - | - | - | - | 3 | 1 | - | - | - | 46 |
| 17 | SOUTH AFRICA | 17 | 13 | - | 4 | - | - | - | - | - | - | 6 | 1 | - | - | 41 |
| 18 | CROATIA | 11 | 10 | - | 2 | 1 | 1 | 2 | 4 | 2 | 1 | 1 | 1 | - | - | 36 |
| 19 | BOLIVIA | 4 | 5 | 8 | 1 | - | - | 7 | - | - | - | 8 | - | - | - | 33 |
| 20 | ARGENTINA | 18 | 2 | - | - | 4 | - | - | - | 3 | 3 | - | - | - | - | 30 |
| 21 | GERMANY | 8 | - | - | - | 2 | 4 | 1 | - | 4 | 4 | - | 3 | 1 | - | 27 |
| 22 | SERBIA | 1 | 19 | 5 | - | - | - | - | - | - | - | - | - | - | - | 25 |

Figure 4: Customs reporting member countries and the reports

### 1.3.11 Refugees and Other Groupings

Osire Refugee Settlement (ORS) is the only place where refugees and asylum seekers reside. Currently there are about 8,900 recognized refugees and asylum seekers with the majority of them being from the Democratic Republic of Congo (DRC). As can be seen in section 1.3.12 and Annexure J of this report, DRC nationalities appear amongst the highest foreign nationals who travel to and from Namibia. Similarly, remittance data via ADLAs places remittances to and from such country amongst the highest in the period reviewed. Whilst the majority of DRC refugees are based at ORS, some reside outside ORS, commonly referred to as 'urban refugees'. The Ministry could not avail the number of such urban refugees. Refugees are required to only reside in ORS. Refugees and asylum seekers may apply for and be issued with exit permits to enable them to leave such site. This happens mostly when they would like to go shopping or seek medical treatment elsewhere.

The ORS has been housing refugees and asylum seekers since independence and there has not been any indications of potential TF vulnerabilities (or terrorism threats) emanating from or associated with refugees in Namibia (including the so-called 'urban refugees').

### 1.3.12 Ties to High Risk Jurisdictions

This section should be considered with observations in sections 1.3.10 and 1.3.11 above.

The NRA considered Namibia's ties to countries with escalated ML/TF/PF risk levels as per FATF and Global Terrorism Index21. With the FATF lists, the jurisdictions included in such review include those on the FATF black list22 and those under increased monitoring23 or grey list. In this regard, banks availed information about the number of clients who hail from, or are citizens of such jurisdictions as at 31 May 2023. This section should be considered with section 7.7 of the 2020 NRA which deals with considerations of BOPCUS information (cross border remittances by banks). Similarly, ADLAs availed information related to remittances to and from such jurisdictions.

TF can also be advanced through the smuggling of items, articles and cash by travellers through borders. In this regard, immigration records related to such identified jurisdictions, as per the MHISS data, were reviewed and considered along Namibia's data around potential smuggling corridors contained in Annexure F of this report and section 8.11 of the 2020 NRA report. Below is a summary of notable observations which could speak to the probability of potential TF materializing via ties to the said high risk jurisdictions:

a. There appeared to be an increase in the number of travellers to and from the People's Republic of Iran in the period 2020 to 2022;

---

21 Global Terrorism Index, Measuring the Impact of Terrorism, 2022. Accessible via: file:///C:/Users/ham638/Downloads/GTI-2022-web_110522-1.pdf

22 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2020.html

23 https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-june-2023.html

b. Citizens of the Democratic People's Republic of Korea (DPRK) who hold bank accounts locally appear few across the banking sector. On the other hand, ADLAs did not process any remittances to and from the DPRK in the period. This trend is similar for the People's Republic of Iran (PRI), despite the PRI recording higher travelling volumes to and from Namibia;

c. Amongst the FATF greylisted jurisdictions, nationals from the Philippines, DRC, Mali, Mozambique, Uganda, South Africa, Nigeria, Tanzania and Cameroon feature prominently amongst the highest number of foreigners who hold bank accounts in the local banking sector. This trend is similar with travellers to and from such jurisdictions. Senegal, Jamaica, Jordan and Croatia are an anomaly with very few local bank account holders from such jurisdictions but comparatively higher rates of travellers to and from such;

d. Amongst jurisdictions on the Global Terrorism Index, Pakistan, Ethiopia and Kenya feature prominently amongst the highest number of foreigners who hold bank accounts in the local banking sector. This trend is similar with travellers to and from such jurisdictions. There is an anomaly with Somalia as nationals from that country appear to hold very few bank accounts locally but comparatively record higher rates of travellers to and from such country; and

e. Overall, there appears to be a growing number of travellers to and from Namibia in relation to these high risk jurisdictions.

Economic and socio-political relations between countries, amongst other factors may impact the number of travellers to and from a country. This can also be true for foreign nationals who may hold bank accounts in Namibia. The nature of a risk assessment is to help establish probability trends along existing structures or frameworks. In view of this, the 2023 NRA update, amongst others, thus concluded that:

a. The presence of foreign nationals who do not make use of formal banking systems could be an indicator that such persons may be using or relying on informal financial systems, which are inherently high risk for TF purposes;

b. The increasing number of travellers to and from high risk jurisdictions, in the review period which align to the post COVID era may suggest a recovery in tourism and travelling patterns. Similarly, it should be equally accepted that those traveling the world to advance terrorism may hide within the huge travel volumes. This does not reduce TF risks overall as exposure or vulnerability is enhanced; and

c. To date, the most prevalent indications of potential TF suggests outward cross border remittances as a prominent mechanism through which TF may occur, if the few cases at hand are anything to go by. The 2021 TF sanctions screening thematic reviews to which banks and ADLAs were subjected to showed that the average effectiveness of screening manipulated data/names had some room for improvement while screening of controlled or unchanged names remained well above 90%. The FIs were cautioned to take corrective measures as per Directive 01 of 2022 (available on the FIC website) and this resulted in significant enhancements in screening effectiveness, as observed with the 2022 thematic reviews (see section 1.3.7). This, together with the immigration screenings at points of entry are considered to reduce TF exposure reasonably.

### 1.3.13 Vulnerabilities in Close Corporations in potential TF abuse

As mentioned in Chapter II of this report, Close Corporations (CCs) appear to be the type of legal person most used in potential TF cases. The TF Typology Awareness Report24 issued by the FIC in June 2023, especially the case studies therein, shows that CCs were most prevalent in TF suspicions. The average CC does not have conventional governance framework such as board of director. They are relatively easy to set up and the case studies in the said TF Typology Awareness Report referred to suggests they were the preferred means through which funds could be moved, mobilized or raised to support or advance terrorist activities. The case studies in section 1.2.2 herein, including others in the 2023 FIC published TF Typology reports25 largely show how CCs are used and ADLAs or money service businesses are most preferred as a means to remit funds.

24 FIC website: https://www.fic.na/index.php?page=fic-trends-and-typology-reports

25 https://www.fic.na/index.php?page=fic-trends-and-typology-reports

## 1.4 NPO Sector: TF Threat and Vulnerability Assessment

This section deals with NPOs' exposure to TF threats. The FATF issued guidance that assists countries in their implementation of Recommendation 8 on NPOs, [26] in line with Recommendation 1 and the risk-based approach. It is essential that a risk based approach is adopted to ensure the NPO's compliance expectations, while adhered to, does not undermine a country's obligations to respecting the freedom of association, assembly, expression, religion or belief, and international humanitarian law. The 2020 NRA identified Faith Based Organisations or religious bodies as highly exposed to TF risks *(see section 13.4.2.2 and figure 52 in 2020 NRA)*. The 2023 NRA update further found charities in general as highly exposed to TF risks. The section below avails outcomes of such NPO TF risk assessment.

### 1.4.1 Specified/Identified NPOs[27]

The 2023 FIA amendments refer to Identified or Specified NPOs as the NPOs which are vulnerable to TF abuse and thus the typical FATF NPOs. NPO supervision, particularly of FBOs commenced in 2020. One of the inherent challenges in assessing the risk of terrorist abuse in the NPO sector is defining what a NPO is, and more importantly, which of the sub-sectors within NPOs are most at risk for TF abuse. The FATF has defined a NPO in its Interpretive Note to Recommendation 8 as "a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or the carrying out of other types of 'good works.' The FATF has also stated in its Best Practices guidance for Recommendation 8 that measures to combat TF activity in the NPO sector should *"apply to NPOs which account for a:*

*a. significant portion of the financial resources under control of the sector; and*

[26] FATF Recommendation 8: "*Countries should review the adequacy of laws and regulations that relate to nonprofit organisations which the country has identified as being vulnerable to terrorist financing abuse. Countries should apply focused and proportionate measures, in line with the risk-based approach, to such non-profit organisations to protect them from terrorist financing abuse, including: a) by terrorist organisations posing as legitimate entities; (b) by exploiting legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and (c) by concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations."*

[27] To be the FATF NPO as per proposed FIA Amendments.

*b. substantial share of the sector's international activities."*

The FATF Study 28 on TF risks in NPOs found, through case studies, that there is a correlation between the types of activities an NPO is engaged in, and the risk of TF abuse. The majority of the case studies dealt with NPOs engaged in *'service activities'* such as housing, social services, religion, education, or health care. None of the case studies dealt with NPOs engaged in *'expressive activities'* such as programmes focused on sports and recreation, arts and culture, interest representation or advocacy such as political parties, think tanks and advocacy groups. Additionally, the case studies and available research indicate there is a stronger risk of abuse for NPOs carrying out activities in populations that are also targeted by terrorist movements for support.

#### 1.4.1.1 Threats: Faith Based Radical and Extremist Ideologies

This update, like prior NRA updates could not find anything within local NPOs that would deviate from the trend noted b the FATF on NPOs as explained above (1.4.1). If anything, faith based activities, particularly those with potential extremist ideologies exhibited the highest level of exposure to TF risks. The two local cases of potential TF speaks to such trend consistently, as follows:

a. all subjects previously subscribed to Christianity;

b. at some point, such subjects departed from the Christian faith/religion and subscribed to other faith based or religious activities; and

c. eventually, or at some point, they became radicalized with extremist ideologies beyond legitimate Islam and were suspected of potentially supporting internationally known foreign terrorist groups such as ISIS. In all such cases, note that there is no evidence implicating legitimate FBOs or Islam but rather extremist and radical ideologies through which subjects are indoctrinated.

28 file:///D:/09%20November%202022/NPOs/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf

The FIC issued a TF typology report29 which speaks to the abovementioned cases. The role that faith and ideology-based indoctrination played in the local TF cases is observable from a radical and extremist point as a driving force which coerced subjects into such activities. There is suspicion that subjects could be indoctrinated outside legitimate FBO settings.

### 1.4.2 Large and Active NPOs

Over and above the observations in this section, the banking sector's annual FIA compliance returns make provision for banks to indicate the number of active NPO accounts on their books in the reporting period. Findings from the few potential TF suspicions locally (though not involving NPOs) suggests funds may have been remitted to other countries via banks. Though the 2020 NRA listed many registered NPOs, the high risk NPOs or active ones are fewer than 3,60030 if regard is had to their banking behaviour. Most NPOs previously registered are dormant or ceased operations but have not deregistered with relevant authorities. The table below suggests banks identified only 3,587 FBOs and Charities nationally, with active bank accounts. Over 30% of such accounts hardly record any meaningful transactions.

| Bank | FBOs and Charities with active bank accounts: June 2023 |
|---|---|
| Bank A | 45 |
| Bank B | 1914 |
| Bank C | 170 |
| Bank D | 1450 |
| Bank E | 8 |
| Bank F | 0 |
| Bank G | 0 |
| Bank H | 0 |

Table 1A: Active NPO bank accounts

Table 1A above shows that NPO bank accounts are mostly concentrated in two of the big four banks. No peculiar reasons could be established to explain why most NPOs conducted their banking activities with such banks only. Table 1B below shows that the CDD related controls

29 https://www.fic.na/uploads/TrendsandTypologies/FICTrendsandTypologyReports/Terrorist%20Financing%20Risks%20in%20the%20Non-Profit%20Organization%20Sector.pdf

30 In August 2016, over 1,900 NPOs were registered with various authorities as per section 11.12.2, Table 37 of the 2020 NRA.

upon bank account opening for NPOs is generally the same across the large four banks in the sector. The smaller banks account for the lowest number of NPO bank accounts.

| Prudential Licensing and Registration as a requirement | | Controls to gain assuarance that NPOs are subjected to regulatory oversight | | | FIC Registration as a requirement / Proof of FIC registration | |
|---|---|---|---|---|---|---|
| Bank | Does Bank have controls to restrict opening of NPO bank accounts without proof of licensing? | Proof of registration with self-regulatory bodies | Proof of formation or incorporation documents | None | Religious / FBOs | Charitable NPOs |
| Bank A | ✗ | | ✓ | | ✗ | ✗ |
| Bank B | ✗ | | ✓ | | ✗ | ✗ |
| Bank C | ✗ | | ✓ | | ✗ | ✗ |
| Bank D | ✗ | | ✓ | | ✗ | ✗ |
| Bank E | | | | | | |
| Bank F | | | | | | |
| Bank G | ✗ | ✓ | ✓ | | | |
| Bank H | | | | | | |

Table 1B: NPO Bank account opening related CDD

Table 1C below presents an overview of financial and asset information of some of the largest NPOs nationally. A total of NAD 17,776,826.26 in financial aid was received from local and foreign donors with 60% of this amount being received from foreign donors. Note however that almost all of this is derived from credible international donors such as Redcross. The estimated total value of assets of large NPOs amounted to NAD 888,498,788.75 with one charitable NPO accounting for over 90% of such assets.

| No. | NPO's Name | FIC registration? | Assets/Funds Received from (NAD) | | Assets/Funds/Benefits Remitted to (NAD) | | Value of All NPO Assets (NAD) |
|---|---|---|---|---|---|---|---|
| | | | **Foreign Donors** | **Local Donors** | **Foreign Beneficiaries** | **Local Beneficiaries** | |
| 1 | FBO 1 | Yes | 70,911.53 | - | - | - | 32,181,357.54 |
| 2 | FBO 2 | Yes | - | - | - | - | - |
| 3 | Charity 1 | Yes | 1,972,000.00 | 1,495,300.00 | - | - | 9,459,074.80 |
| 4 | Charity 2 | No | 140,000.00 | - | - | - | - |
| 5 | Charity 3 | No | 556,028.81 | 359,400.00 | - | - | 1,227,212.00 |
| 6 | FBO 3 | Yes | - | - | - | - | 282,045.02 |
| 7 | Charity 4 | No | - | - | - | - | 826,557,587.00 |
| 8 | Charity 5 | Yes | 48,800.00 | 606,900.00 | - | - | 6,830,000.00 |
| 9 | Charity 6 | No | 4,796,405.00 | 483,000.00 | - | - | 3,615,983.66 |
| 10 | Charity 7 | No | 280,722.85 | 26,225.07 | - | - | 2,391.57 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 11 | FBO 4 | Yes | - | - | - | - | 10,395.16 |
| 12 | FBO 5 | Yes | - | - | - | - | 74,355.00 |
| 13 | Charity 8 | Yes | 2,916,133.00 | 4,025,000.00 | - | - | 8,258,387.00 |
| | Total | | **10,781,001.19** | **6,995,825.07** | **-** | **-** | **888,498,788.75** |

Table 1C: Presents an overview of the finances and assets of some of the largest NPOs

### 1.4.3 Means of Abusing NPOs for TF

There are various means of abusing NPOs to advance TF though local cases have not found domestic NPOs abused to advance TF. All local NPO abuses only show other financial crimes such as fraud, theft and embezzlement of funds by NPO directing officials (see 2018 and 2020 NRA reports).

The following are primary means through which TF abuse can take place:

a. NPOs or *directing officials maintain an affiliation with a terrorist entity*, either knowingly or unknowingly. In these instances, an NPO could be abused for multiple purposes, including general logistical support to the terrorist entity;
b. In several cases, NPOs are abused to provide support to *recruitment efforts* by terrorist entities;
c. NPOs are also targeted for *abuse of programming*. In these instances, the flow of resources may be legitimate, but NPO programmes are abused at the point of delivery; and
d. Some terrorist entities abuse the NPO sector *through false representation*. In these instances, terrorist entities start ‘sham’ NPOs or falsely represent themselves as the agents of ‘good works’ in order to deceive donors into providing support.

FIC Guidance Note 12 of 2023 (sections 5.1 and 5.2) presents detailed information around the methods through which NPOs can be abused.

### 1.4.4 Assessing NPO TF risk exposure

The TF risk assessment identified six major sub-categories of NPOs (as per Table 2 below) that raise and spend funds. Such were subjected to a TF risk assessment and service NPOs

such as Charities were identified as high risk TF NPOs. FBOs were found, as per 2020 NRA, to be exposed to TF risks and this update confirmed same.

| NO. | NPO CATEGORY | DESCRIPTION |
|---|---|---|
| 01 | Section 21 Companies | These are entities incorporated in terms of Section 21 of the Companies Act, ideally not-for-profit and excludes31 FBOs and charities that may register as section 21. |
| 02 | Faith Based Organisations (FBOs) | Includes all religious organisations and Faith Based Charities (FBCs). Some FBOs manage their own charities. |
| 03 | Residential Children Care Organisations (RCCOs), including Safety Homes and Educational Institutions | A sub-section of Charities. These are mostly facilities that accommodate the homeless (the so-called 'street kids' or less fortunate children, the homeless etc).<br>Educational institutions such as kindergartens and non-governmental schools/education/academic institutions. |
| 04 | Charities (Other Welfare Organisations) | The broader category of charities. Most of these organisations which are involved in humanitarian activities. |
| 05 | Research and Scientific Organisations | These are non-profit organisations created to advance research, studies or similar goals. |
| 06 | Sports and Recreational Facilities | These are also non-profit organisations created to advance sport related interests. |

Table 2: NPO sub-categories meeting the FATF definition in Namibia

Each NPO sub-category's level of TF risk differs depending on the nature of its operations and various other factors such as governance frameworks. Figure 5 below avails outcomes of such assessment. On the vertical axis, the more effective mitigating or control measures are in a category, the higher its score. The opposite is applied on the horizontal axis which speaks to inherent risks. The more vulnerable the NPO sub-category is, the higher its rating on the horizontal axis.

31 For this context, FBOs and Charities are separately identified as high risk TF NPOs. Any type of NPO can register as a section 21 entity in terms of the Companies Act.

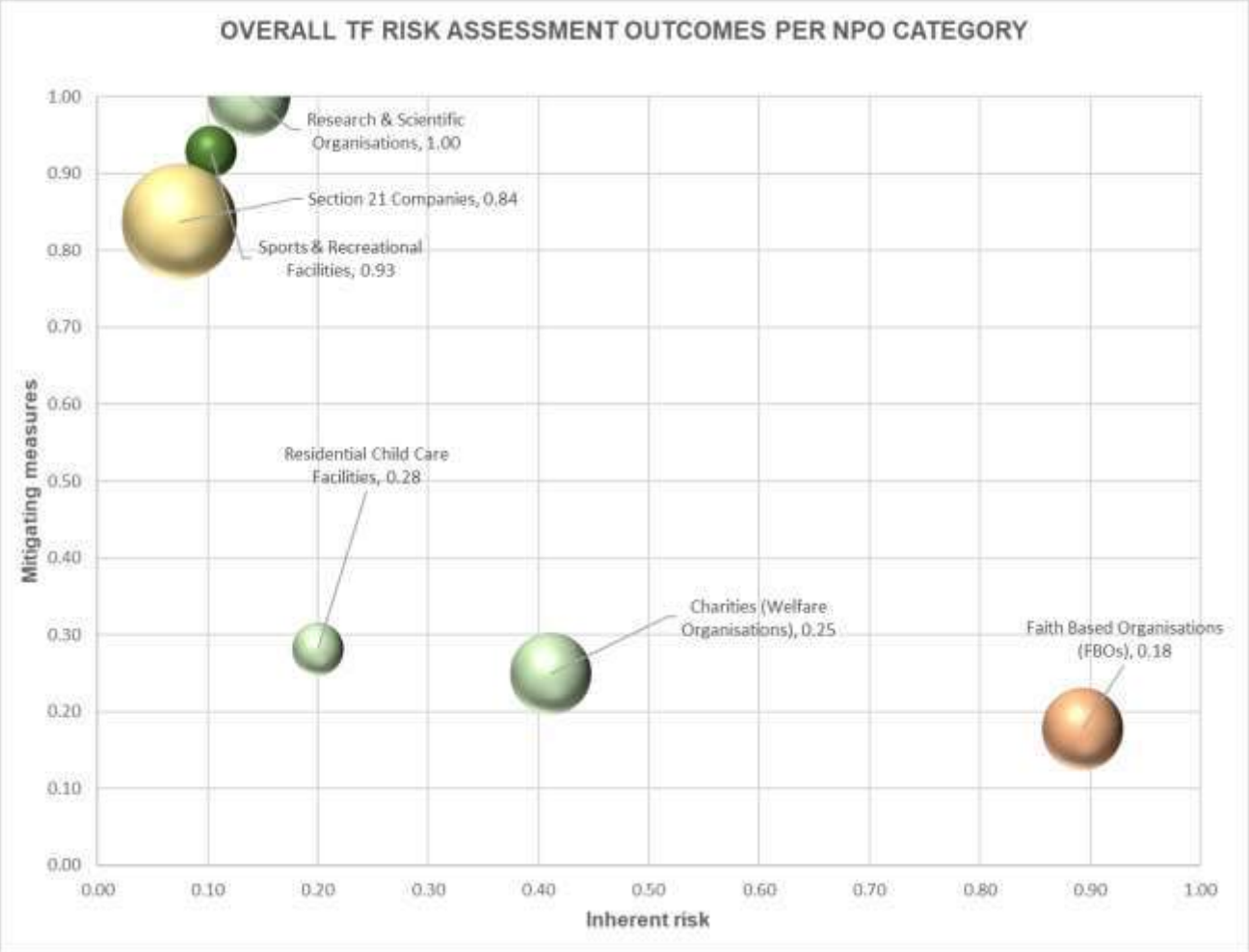



Figure 5: Overall TF risk assessment outcomes per NPO category

### *e. Section 21 Companies*

This reference to Section 21 Companies herein excludes FBOs and charities registered as section 21 Companies. Section 21 Companies are naturally not as inherently high risk for TF activities given governance frameworks around them such as being subjected to audits and establishing boards as per the Companies Act. In terms of the overall implementation of governance controls, section 21 Companies appear to have implemented more effective controls than most other NPO sub-categories. These measures enhance transparency overall and thus reduces risks of abuse to advance TF activities.

Section 21 Companies' overall TF mitigating measures or combatting effectiveness level was rated **High** (0.84 or 84%) while the TF inherent threat was rated **Low** (0.07 or 0.07%). This

suggests this sub-category of NPOs is not the vehicle most TF threats want to use in advancing TF activities.

### *f. FBOs (religious bodies)*

Overall, the inherent TF threat level was rated **High** (0.89 or 89%) while the TF mitigating measures (inherent vulnerability level) or ability to prevent such TF threats was rated **Very Low** (0.18 or 18%). The risk mitigating controls are thus way below the threat level exposure, rendering this the most highly exposed NPO sub-category to TF threats. *See Annexure G.*

The 2017/18 NRA update32 and 2020 NRA both raise findings of FBOs, mainly churches, that were abused for financial crimes such as theft, fraud and embezzlement, mostly committed by church leaders.

The absence of basic financial controls, governance and transparency in most FBOs contribute to this exposure. Apart from a few self-regulating bodies or those registered in terms of Section 21 of the Companies Act, there are no regulators of FBOs. Market entry requirements are almost non-existent and FBOs are at liberty to decide whether to have financial reporting as such is not a legal requirement. Some of the lager religious bodies have some means of accounting by reporting to their members though. The majority do not have governance structures in place. The extent to which self-regulatory bodies are able to influence or coerce their member/associate FBOs to implement governance frameworks is not certain as many FBOs are not obliged to execute instructions or guidance from such bodies. It was observed that in the main, FBOs' association to such bodies is to enhance their faith based interests and operations as such self-regulating bodies have little regard to governance that can be helpful to combat TF activities.

The fact that FBOs are involved in cross border remittances largely enhances their overall vulnerability to TF abuse as funds could emanate from or be directed to high risk jurisdictions.

32 https://www.fic.na/uploads/Publications/ML%20TF%20PF%20Risk%20Assessment%20Reports/2017%2018%20NRA%20Updates/NPO%20risk%20assessment%20report%20updated%20August%202020.pdf – see especially the Annexure which lists sanitised cases from page 25 – 31.

The majority of the Namibian population appear to subscribe to Christianity, making this the largest FBO sub-category in the FBO space, in terms of memberships. The NRA observed that FBOs consist of a wide range and type as some are large and well established with own sources of revenue while others rely on donor funding. Smaller FBOs mainly rely on contributions or donations by members. Most churches, from FIC supervision and monitoring activities bank within the formal financial system and this reduces risk exposure. Apart from churches, the Islamic faith has also grown in Namibia in recent years. The FIC has raised some concerns with poor cooperation from a few such establishments. Unwillingness to avail information around financing, risk assessments or complete the Annual Compliance Returns recently circulated speaks to such. The poor cooperation in itself is a red flag as far as the few non-cooperating entities is concerned.

Case studies in section 1.2.2 herein above suggests all subjects implicated have an affiliation to radical and extremist ideologies.

### *g. Residential Child Care Organisations (RCCOs) & Educational Institutions*

This category mainly consists of organisations involved in humanitarian activities specializing in child-care services. They are expected to register with the Social Services Department within the Ministry of Health and Social Services (MoHSS). The MoHSS' supervisory and regulatory activities do not entail strict guidelines or if such are in place, they are not largely enforced, found the 2023 NRA update. The NRA could not find significant regulations these NPOs need to comply with to help mitigation of TF risks while some requirements certainly add value. These organisations are generally small and operate informally except the larger NPOs. The larger, more established ones have slightly more formal governance and management systems in place such as boards. Overall, the smaller NPOs are most vulnerable to TF activities as they have lesser control frameworks in place.

Kindergartens or crèches are registered with the Ministry of Gender. The Ministry of Education also registers private or non-governmental educational institutions. This is done through the Directorate of National Examinations and Assessments (DNEA) and the primary purpose is to ensure quality in the administration of examinations and assessments. The Planning and Quality Assurance (PQA) function within the Ministry is responsible for ensuring quality

standards. The overall due diligence at market entry within the said government Ministries appear to have no TF or financial crime related mitigations. The focus remains on gaining assurance around competence to delivery on NPO mandate. The NRA could not observe threats related to this category domestically and internationally.

With consideration of all variables, the effectiveness of TF mitigating measures were rated **Low** at 0.28 or 28%. Despite this, the inherent threat level was also rated **Low** at 0.20 or 20%. This suggests despite reduced or limited controls, childcare facilities and educational institutions are not the vehicle most TF threats want to use in advancing TF activities.

### *h. Charities: Other Welfare Organisations (WOs)*

This sub-category is simply referred to as Charities. The TF threat level was rated **Medium**, at 0.41 or 41% while the effectiveness of TF mitigating measures were rated **Low** 0.25 or 25%. There is a mismatch between mitigating measures and threats. The relatively higher TF threat level is way above the effectiveness level of mitigating measures, rendering this sub-category highly vulnerable and second only to FBOs in terms of TF exposure. *See Annexure G.*

Like RCCOs and educational institutions, this category mainly consists of organisations involved in humanitarian activities ranging from health, education, social and other welfare services or operations. With the exception of NPOs involved in education related services, many others are under the supervision of the MoHSS. The NRA could not find significant regulations they need to comply with which help with mitigation of TF risks. These organisations are generally small and some operate informally, except for the few larger NPOs. The larger, more established ones have more formalized management systems in place. The NRA thus found that smaller and informal NPOs in this category are most vulnerable to TF than the larger firms which have proven to have reasonably sound governance and control measures in place.

With consideration of international typologies and cases on how charities are abused to advance TF, the risk rating of charities is increased. At the time of issuing this report, in August 2023, the FIC commenced analysing a potential TF suspicion reported by a financial

institution. Below is a summary of the early indications of potential abuse through suspected diversion from legitimate NPO objects and programs.

***Case Study C***

***Background***

*The NPO operates under a trust. The object of the trust is said to be promotion of positive social change in Southern Africa and matters related to HIV/AIDS, LGBTQ+ and sex workers. The NPO receives grants or donations running into millions. It has seven founders and trustees and only two are Namibian with the rest being South African nationals.*

*Large transfers amounting to millions are constantly transferred into the NPO's local bank account. The bank could not readily establish the purposes of such remittances. The trust appears to have many bank accounts with a few being USD and Euro accounts.*

***Reason for Suspicion***

*While funds are being received into the local bank account of such NPO, there is minimal social footprint of what the NPO does locally, especially in view of the significant amount of funds it receives and remits internationally for its charitable causes. The charitable NPO remits to high risk jurisdictions in south east Asia, Tunisia and Uganda. Even if the suspicion of TF is later cleared, there may be potential abuse of violations of Exchange Control Laws and Rulings. Additionally, payment reference details do not seem to support the stated NPO objectives. A similar trend was observed with the so-called Fishrot payment references. The NPO is not registered with the FIC, nor the National Welfare Board. Initially, it seemed challenging to get hold of trustees who are based in South Africa to conduct due diligence around them.*

***Banking and regulatory Interventions***

*The bank froze this NPO's bank accounts in August/September 2023, immediately filed a report with the FIC after the FIC's July 2023 bankwide workshops giving guidance on the four primary means of abusing NPOs for TF. The NPO, after various engagements requested for unfreezing of its bank accounts. This requested transpired at the same time as the FIC's calls to ensure all high risk NPOs are registered with the FIC, as per Directive 06 of 202333, issued on 26 September 2023. Such froze was only uplifted when the said NPO submitted registration documents with the FIC and commenced registration with the National Welfare Board as a Charity, in terms of the National Welfare Act.*

33 https://www.fic.na/uploads/Publications/Directives/2023%20Directives/Directive%20No%206%20of%202023%20-%20VASP%20Registration%20Deadline.pdf

*While investigations lately show this may not necessarily be a TF incident, the vulnerabilities in control systems shows how such can be similarly abused to advance actual TF.*

### *i. Civil Society, Research and Scientific Organisations*

In terms of size, this sector is smaller than other NPO categories. Many organisations in this category are formally set up in terms of Section 21 of the Companies Act. Civil Society, Research and Scientific Organisations appear to be more structured with prudent governance and transparency frameworks than most other NPOs. Many governance and control frameworks cited for Section 21 Companies above are also present in this category of NPOs. These are institutions mostly associated with professionalism and governance is usually an essential component of all such bodies. The level of governance often has an impact on the number of professionals who would want to associate with such Research and Scientific Organisations. Such governance measures ensure these NPOs have financial management policies and processes in place that enhance accountability. For example, financial reporting in terms of the Companies Act appears a norm in this type of NPOs, as per FIC's oversight functions. This is also essential as members, associates, funders or donors of such bodies usually have an expectation that sound governance practices are in place to ensure resources are used for the intended purposes.

The inherent TF threat level in Civil Society, Research and Scientific Organisations was rated **Low** (0.14 or 14%) while the inherent vulnerability or threat mitigating controls were rated **Very High** (1.0 or 100%). This suggests this sub-category of NPOs are not the vehicle most TF threats want to use in advancing TF activities.

### *j. Sports and Recreational Organisations*

Many sports and recreational organisations are also Section 21 Companies under the companies Act. Governance frameworks explained above within Section 21 Companies also apply to sports bodies that are incorporated in terms of such Act. However, there are also smaller sports bodies that operate informally or without being registered in terms of the said Act. In such entities, governance frameworks are typically non-existent. Despite the reduced controls in some sports and recreational organisations, this category of NPOs was found to

be the least vulnerable to TF activities amongst all NPOs. Though most rely on donations,[34] the level of TF threats targeting sports bodies to advance their causes was rated Very Low. Internationally, there are not many typologies that reflect TF abuse through sporting and recreational activities.

The inherent TF threat level in Sports and Recreational Organisations was rated **Very Low** (0.10 or 10%) while the inherent vulnerability or risk mitigating controls were rated **Very High** (0.93 or 93%). This suggests this sub-category of NPOs are not the vehicle most TF threats want to use in advancing TF activities.

[34] Except for professional sports organisations that at times rely on sponsorships and other incomes from sporting activities.

| No | Input variables | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Section 21 Companies | | Faith Based Organisations (FBOs) | | Residential Children and Safety Homes | | Charities (Welfare Organisations) | | Research & Scientific Organisations | | Sports & Recreational Organisations | |
| 1 | Number of TF/Terrorism Convictions (Charities: Foreign typologies only) | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | Does not exist | 0.0 |
| 2 | Number of TF/Terrorism Prosecutions (Charities: Foreign typology) | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | Does not exist | 0.0 |
| 3 | Number of TF/Terrorism Investigations | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | Medium | 0.5 | Does not exist | 0.0 | Does not exist | 0.0 |
| 4 | Number of TF/Terrorism Intelligence | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 5 | Number of TF/Terrorism STRs | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 6 | Number of TF/Terrorism Allegations in credible open sources (Charities: Foreign Only) | Does not exist | 0.0 | High | 1.0 | Does not exist | 0.0 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |

Table 3: Outcomes of TF evidence (threat) evaluation in NPOs

| No | | Intermediary variables | Inherent risk | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating | Assessment | Rating |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Input variables | Section 21 Companies | | Faith Based Organisations (FBOs) | | Residential Child Care Facilities | | Charities (Welfare Organisations) | | Research & Scientific Organisations | | Sports & Recreational Organisations | |
| 1 | Threat | TF Typologies | Diversion of funds | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 2 | | | Affiliation with a terrorist entity | Does not exist | 0.0 | Low | 0.2 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 3 | | | Abuse of programming | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Medium | 0.5 | Does not exist | 0.0 |
| 4 | | | Support to recruitment efforts | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Medium | 0.5 | Does not exist | 0.0 |
| 5 | | | False representation/Sham NPO | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 6 | | Proximity to active terrorist threat | Collection of funds | Medium | 0.5 | High | 1.0 | Low | 0.2 | Medium | 0.5 | Medium | 0.5 | Does not exist | 0.0 |
| 7 | | | Transfer of funds | Medium | 0.5 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 8 | | | Expenditure of funds | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 1 | Inherent vulnerability | NPO Profile | Size | Large | 1.0 | Medium | 0.5 | Small | 0.2 | Medium | 0.5 | Medium | 0.5 | Small | 0.2 |
| 2 | | | Activity type | Expressive | 0.0 | Service | 1.0 | Service | 1.0 | Service | 1.0 | Expressive | 0.0 | Expressive | 0.0 |
| 3 | | | Offshore/complex control structure | Medium | 0.5 | Medium | 0.5 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Medium | 0.5 |
| 4 | | | Level of accountability required by funding sources | High | 0.0 | Low | 1.0 | Medium | 0.5 | Low | 1.0 | High | 0.0 | High | 0.0 |
| 5 | | | Level of verifiability of fundraising methods | High | 0.0 | Low | 1.0 | Medium | 0.5 | Low | 1.0 | High | 0.0 | High | 0.0 |
| 6 | | | Level of cash transfers, valuable in-kind goods | Medium | 0.5 | High | 1.0 | Low | 0.2 | High | 1.0 | Medium | 0.5 | Medium | 0.5 |
| 7 | | Operational features | Level of risk appetite | Does not exist | 0.0 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 8 | | | Complexity / length of operational chains | Medium | 0.5 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 9 | | | Reliance on transitory or informal workforce | Low | 0.2 | High | 1.0 | Low | 0.2 | Medium | 0.5 | Does not exist | 0.0 | Does not exist | 0.0 |
| 10 | | | Level of professionalism | High | 0.0 | Low | 1.0 | Medium | 0.5 | Low | 1.0 | High | 0.0 | High | 0.0 |
| 11 | | Methods to transfer funds | Use of cash | Low | 0.2 | High | 1.0 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | Does not exist | 0.0 |
| 12 | | | Use of virtual currency | Low | 0.2 | Low | 0.2 | Does not exist | 0.0 | Medium | 0.5 | Does not exist | 0.0 | Does not exist | 0.0 |
| 13 | | | Use of informal money transfer system | Low | 0.2 | Medium | 0.5 | Low | 0.2 | Medium | 0.5 | Does not exist | 0.0 | Does not exist | 0.0 |

Table 4: Outcomes of inherent TF vulnerability assessments

| Mitigating measures | ASSESSMENT RATING | RATING | ASSESSMENT RATING | RATING | ASSESSMENT RATING | RATING | ASSESSMENT RATING | RATING | ASSESSMENT RATING | RATING | ASSESSMENT RATING | RATING |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| GENERAL INPUT VARIABLES | Section 21 Companies | | Faith Based Organisations (FBOs) | | Residential Child Care Facilities | | Charities (Welfare Organisations) | | Research & Scientific Organisations | | Sports & Recreational Organisations | |
| Quality of outreach and education | Low | 0.2 | Low | 0.2 | Medium | 0.5 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |
| Quality of NPO policies | Low | 0.2 | Low | 0.2 | High | 1.0 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |
| Scope of registration of FATF NPOs | High | 1.0 | Low | 0.2 | Low | 0.2 | Medium | 0.5 | High | 1.0 | High | 1.0 |
| Availability and accessibility of accurate NPO information | High | 1.0 | Does not exist | 0.0 | Low | 0.2 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |
| Avoiding disruption of NPO activities | High | 1.0 | Low | 0.2 | Does not exist | 0.0 | Medium | 0.5 | High | 1.0 | High | 1.0 |
| Quality of Governance | High | 1.0 | Low | 0.2 | Medium | 0.5 | Medium | 0.5 | High | 1.0 | High | 1.0 |
| Quality of Financial management | High | 1.0 | Low | 0.2 | Medium | 0.5 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |
| Quality of Project management | High | 1.0 | Medium | 0.5 | Medium | 0.5 | Medium | 0.5 | High | 1.0 | High | 1.0 |
| Quality of staff vetting and oversight | Low | 0.2 | Does not exist | 0.0 | Does not exist | 0.0 | Does not exist | 0.0 | High | 1.0 | Low | 0.2 |
| Level of commitment to ethics and transparency | High | 1.0 | Low | 0.2 | Low | 0.2 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |
| Level of self-regulation (incl. implementation) | Low | 0.2 | Low | 0.2 | Low | 0.2 | Does not exist | 0.0 | High | 1.0 | High | 1.0 |

Table 5: Outcomes of TF mitigating measures' effectiveness assessments

# CHAPTER II: LEGAL PERSONS AND ARRANGEMENTS

***Chapter Summary***

*Legal persons within this context refers to incorporated entities such as companies and close corporations (CCs). These can include companies, body corporates, foundations, or associations and other similar entities. On the other hand, legal arrangements refer to partnerships, express trusts or other similar arrangements.*

*Legal persons and arrangements such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements conduct a wide variety of commercial and entrepreneurial activities. Despite the essential and legitimate role that corporate vehicles play nationally and in the global economy, their unique legal status also renders them vulnerable to be used in complex schemes designed to conceal the true beneficial owners and, in many respects, the real reason for holding assets and conducting transactions. Corporate vehicles can be misused for various illicit purposes, including ML, bribery and corruption, insider dealings, tax fraud, TF, sanctions evasion and other illegal activities. For criminals trying to circumvent AML/CFT/CPF measures, corporate vehicles are an attractive way to hide or disguise their identity and conceal the origin and/or destination or ultimate purpose of funds or assets.*

*The ML risk assessment methodology of considering threats and vulnerabilities adopted in 2020 NRA was used herein. Section 8.22 of the 2020 NRA report, amongst others raised observations around vulnerabilities in accessing Beneficial Ownership information at a national level, with emphasis on effectiveness of relevant controls within the Business and Intellectual Property Authority (BIPA) and Master of the High Court. The former is Namibia's company registry while the latter is the registrar of trusts. The 2020 NRA report however failed to assess the extent to which ML/TF/PF threats exploit shortcomings in various types of legal persons and arrangements. This is an essential element of a NRA as it would help FIs, DNFBPs, combatting and prevention authorities to duly prioritise their attention in as far as risks across different legal persons and arrangements are concerned. This is necessary to help Namibia, like all other countries, take measures to prevent the misuse of legal persons and such arrangements for ML/TF/PF.*

*The 2023 NRA update has found that overall, CCs appear most prominently abused in advancing ML activities. Similarly, as per the previous chapter, CCs appears to have been the vehicle of choice in the few domestic suspicions of TF. Companies also appear to have been significantly abused but for ML only. The 2020 NRA found that Companies were the main vehicles used in the suspected PF related to entities from the Democratic People's Republic of Korea.*

## 2. Overview of Legal Persons and Arrangements

The main types of legal persons and arrangements in Namibia are:

| Type of Entity | Total Registered in 2022 | Total Registered to Date |
|---|---|---|
| Closed Corporations | 52,166 | 187,268 |
| Companies (Public and Private companies) | 15,764 | 26,432 |
| Trusts (inter vivos and testamentary trusts) | 401 | 10,823 |

Table 5A: Summary of total registered entities

### 2.1 Companies and Close Corporations

| Entity Type | Number of Active Entities | Number of BO Filling Submitted | Number of BO Filing Approved |
|---|---|---|---|
| Section 21 Company | 2,985 | 80 | 61 |
| Close Corporations | 186,050 | 5,238 | 4,248 |
| Private Companies | 25,632 | 1,521 | 991 |
| Public Companies | 170 | 11 | 8 |
| Foreign Company | 405 | 15 | 6 |
| **Grand Total** | **215,242** | **6,865** | **5,314** |

Table 5B: BIPA's statistics as at 20 Nov 2023

While a significant number of registered entities submit annual returns, many companies and close corporation do not submit annual returns as expected. BIPA is thus unable to duly establish the number of dormant or inactive entities registered.

*Annual Returns received and processed during the financial year*

| CY maintenance applications | Received | Approved | % Processed against receipts |
|---|---|---|---|
| Maintenance Annual Returns (CC7) | 47,802 | 46,460 | 97% |
| Maintenance - Annual Returns (CM23) | 14,855 | 13,997 | 94% |
| Maintenance - Annual Returns (CM23B) | 15,531 | 2 | 0% |
| **Total applications** | **78,188** | **60,459** | **77%** |

Table 5C: Annual returns received and processed in the 2021/22 financial year35, BIPA

35 file:///C:/Users/ham638/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/P4LRIOTJ/BIPA%202022%20Annual%20Report%20Design_Final.pdf

## 2.2 Trusts

The total number of trusts in the registry of the Master of the High Court (MOHC) was 10,823, including 10,685 registered and 140 in pending for registration, as at 10 October 2023. Among the registered trusts, the number of *inter vivos* trusts is 5,151 and the number of testamentary trusts is 94. The remaining 5,440 trusts are imported historical cases and cannot be distinguished by trust type. The majority of trusts registered in Namibia are *inter vivos*, which includes business trusts, charitable trusts and family trusts. Number of trusts registered in the year 2021 is 354 and number of trusts registered in the year 2022 is 401.

## 2.3 Prevalence of threats

Namibian authorities did not previously record data helpful to identifying the level of threat exposure across different legal persons and arrangements. For example, information around the type of legal persons involved in cases under investigation, prosecution or finalised in courts was not kept. For this reason, the 2020 NRA36, in section 8.22 focused on vulnerability of various legal persons, with no emphasis on threats exploiting such vulnerabilities. This has since changed and combatting authorities record such data. In arriving at the risk levels of the various types of legal persons, this chapter complements section 8.22 of the 2020 NRA by highlighting threat levels across different types of legal persons in an effort to estimate overall risk levels.

Table 5A lists CCs, companies and trusts as the main legal persons in Namibia. Other instruments or vehicles through which persons can conduct business include operating as sole traders (registering defensive names), partnerships, associations and co-operatives. These are recognised as legal persons in the FATF framework though they may not be legally recognised as such in-country. In the cases investigated by various LEAs, there are no indications of threats arising through such entities' in advancing ML, TF and PF. If their involvement in investigated or prosecuted cases arise in future, such will be noted and incorporated. This threat level record keeping across different LEAs commenced post the ME in 2023.

36 DETAILED REPORT: NATIONAL MONEY LAUNDERING, TERRORIST AND PROLIFERATION FINANCING RISK ASSESSMENT: PERIOD Jan' 2015 – dec' 2019 (fic.na)

## 2.4 CCs and *Inter-vivos* Trusts are Highly Exposed

Observations herein suggests that CCs are the most abused type of legal persons in terms of financial values37 in ML investigations. This observation suggests that large scale ML in terms of financial values or impact is more likely to be advanced through CCs and to a lesser extent through companies and trusts.

| | PERIOD: 2009 – 2021 (Amounts in NAD) | | | |
|---|---|---|---|---|
| | **Total STRs Received** | **No. of Cases (SDs)** | **Total Financial Value from such Cases/SDs** | **Average Financial value Per Case** |
| CCs | 228 | 104 | 34,807,766,160.75 | 334,690,059.24 |
| Private Companies | 232 | 115 | 8,659,067,618.13 | 75,296,240.16 |
| Inter Vivos trusts | 96 | 55 | 1,613,992,815.33 | 29,345,323.92 |
| Natural Persons | 5,690 | 1,696 | 23,404,719,080.81 | 13,799,952.29 |

Table: 6 Potential ML in FIC cases referred for further investigations

While the above cases speak to ML and related predicate offences, the TF Typology Awareness Report38 issued by the FIC in June 2023, especially the case studies therein, shows that CCs were also most prevalent in TF investigations. Governance frameworks, or the lack thereof, could potentially be a contributing factor. The average CC does not have conventional governance frameworks such as board of directors, nor are they subjected to periodic audits like companies as such controls are not legal requirements for CCs. CCs are relatively easy to set up and the case studies in the said TF Typology Awareness Report suggests they were the most preferred vehicle through which funds could be moved, mobilized or raised to support or advance terrorist activities. It is also commonly accepted that ML control vulnerabilities or shortcomings can similarly be exploited to advance TF and this assessment did not find any considerations to dispute this.

37 As per cases analysed by the FIC and referred to various investigative authorities on findings that suggest possible ML.

38 FIC website: https://www.fic.na/index.php?page=fic-trends-and-typology-reports

Companies are not necessarily significantly less riskier than CCs despite the legal requirement for them to implement better governance frameworks than CCs.

As per Table 6 above, the high number of natural persons implicated in ML activities still suggests that, by and large, people advance ML activities in their individual capacities or self-laundering39. The NRA could not observe threats materializing through partnerships, body cooperates and cooperatives. With partnerships, because they are not legal entities, LEAs indicated that a very few and insignificant cases suggests a few natural persons subjected to investigations may have been part of partnerships but it may not have been conclusively established that partnerships may have been abused. No cases were recorded of ML, or its predicate offences involving body cooperates or cooperatives at all. The NRA however cautions that care needs to be had in interpretation of this information as Namibia's ME found challenges in investigating authorities' ability to duly investigate large and complex cases. This suggests some ML investigations may not have duly revealed abuse of certain legal persons and arrangements. The likelihood of this is worth considering given that observations in some cases suggest higher risks arose owing to suspected use of personal funds (which may not readily reveal involvement of partnerships) for business purposes, or vice-versa.

Locally, a trust can either be a private trust or a public charitable trust. Findings herein suggests only *inter-vivos* trusts[40] may have been abused in advancing ML. Equally all such trusts (100% of the trusts in cases investigated) were Namibian initiated or founded (owned). None such trusts in ML or related predicate offence investigations were charitable trusts. The NRA further found that about 82% of these trusts have Namibian donors and Namibian trustees. Additionally, only 40% of the trusts involved in potential ML cases have foreign nationals listed as beneficiaries, with the majority being South African citizens.

39 In this context referring to not using other vehicles through which to launder.

40 Trusts created between living persons registered under the Trust Moneys Protection Act 34 of 1934.

| PERIOD: 2009 – 2021 (Amounts in NAD) | | | | | | |
|---|---|---|---|---|---|---|
| | **Fraud** | **Total Financial Value** | **Potential Tax Evasion** | **Total Financial Value** | **Corruption** | **Total Financial Value** |
| CCs | 25 | 404,533,140.88 | 66 | 28,400,797,080.66 | 7 | 394,575,890.57 |
| Private companies | 56 | 656,836,151.56 | 141 | 738,080,077.59 | 35 | 284,419,187.68 |
| Inter vivos trusts | 3 | 14,016,585.60 | 7 | 776,270,899.40 | 6 | 56,516,585.60 |
| Natural Persons | 667 | 1,695,855,636.13 | 2264 | 15,632,296,444.92 | 84 | 1,955,490,671.17 |

Table: 7 Cases disseminated for investigations per predicate offence

## 2.5 NAMPOL and the Prosecutor General's Asset Forfeiture Unit (AFU)

### 2.5.1 NAMPOL

As part of the recommendations to help place the country in a position to better appreciate her scale and magnitude of ML, NAMPOL has enhanced her record keeping mechanisms and the below reflects a summary of relevant ML and commercial crimes. The consistent trend shows that CCs are still most exposed to threats. Companies referred to herein are private companies only. There were no public companies observed as per table herein below. This record is updated monthly and Annexure K, attached hereto, shows the detailed monthly records from September 2021 to April 2023.

| Period | CCs | Companies | Trusts | Natural Persons | Namibian Nationa | Foreign National | Amount (NAD) |
|---|---|---|---|---|---|---|---|
| **Total** | **26** | **4** | **0** | **402** | **246** | **10** | **9,797,720.91** |

Table 7A: NAMPOL statistics on ML and commercial crimes

Annexure L of this report lists the Anti-Corruption Commission (ACC) ML/corruption data which suggests a similar trend with CCs being highly abused.

### 2.5.2 Asset Forfeiture Unit (AFU)

The AFU has created a mechanism to enhance estimating the national scale and magnitude of ML. Table 8 below shows a summary of cases processed involving legal persons and arrangements. A total of 62 cases were referred to the above-mentioned unit from the year 2016 to end of 2022. Records show that 66% of these cases involved CCs while Trusts and Companies represent 6% and 5% respectively. This again concurs with the statistics in Tables 5 and 6 which suggests that CCs are generally the most abused legal persons in Namibia, in the advancement of ML.

| | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | Total |
|---|---|---|---|---|---|---|---|---|
| Natural persons | **15** | **10** | **10** | **8** | **4** | **8** | **7** | **62** |
| CCs | 11 | 9 | 5 | 6 | 1 | 4 | 5 | **41** |
| Inter vivos trusts | 0 | 1 | 0 | 0 | 1 | 1 | 1 | **4** |
| Private companies | 0 | 2 | 0 | 0 | 0 | 0 | 1 | **3** |

Table 8: Cases by Natural and Legal Persons

At the time of conducting this assessment the OPG's criminal prosecution function had not availed statistics of cases under prosecution or finalised showing the types of legal persons involved in each case. This again speaks to the record keeping challenges experienced across various LEAs. It must however be said that the OPG has commenced keeping statistics in a manner that would help risk assessments.

### 2.6 Factors that enhance UBO[41] Vulnerabilities

The 2020 NRA focused on vulnerability elements related to legal persons and arrangements as contained in section 8.22 of the 2020 NRA. Below is a summary around vulnerabilities that builds on such earlier observations:

a. **No timely access to information:** This is perhaps the most significant challenge undermining UBO information in Namibia. In the period under review,

41 Ultimate Beneficial Ownership.

timely access to adequate, accurate, updated or current basic and beneficial ownership information on legal persons and arrangements has not been addressed yet, for various reasons. Primarily, it is because not all UBO information for all entities was obtained by the Master of the High Court and BIPA while the need for a web based or similar platform through which information can be timely shared remains unaddressed;

b. **Lack of UBO appreciation by authorities:** Competent authorities, including some prudential licensing authorities do not fully appreciate the concept of UBO due diligence, as observed in the ME report. They thus do not require that sufficient BO information be obtained at registration and during information updates. Legal ownership is mostly misunderstood for UBO information;

c. **BIPA's Annual Returns:** Until recently, the requirements only obliged legal persons to provide UBO information when submitting their annual returns and not at the time of registration of the legal person. Hence no information is obtained on UBO at the time of registration, in the period under review. BIPA has not started collecting all UBO information even when annual returns are filed and such information is not collected and updated. This greatly undermines the adequacy of the basic and UBO information accessed and/or requested by the public, competent authorities;

d. **Absence of AML/CFT/CPF UBO Registry Responsibilities:** The FIA designates the BIPA and Master of the High Court as supervisory authorities to enforce the requirements to obtain BO ownership and keep the information accurate and updated, however this mandate has hardly been exercised. In the period under review, no initiatives have been undertaken by the authorities to establish the level of compliance, and as such the quality and efficacy of the information held at registries is undermined and may not be of great use to persons who access or request it;

e. **Condoned Non-Compliance:** In Namibia no sanctions have been applied for non-compliance with the AML/CFT/CPF UBO Registry requirements to keep

such information accurate and updated. Whereas this may be attributed to a lack of awareness of the authorities of their designated mandate, or challenges relating to limited resources including staffing, the state of affairs gives room for any ongoing abuse for ML/TF to continue undetected;

f. **Bearer shares[42]:** In the period under review, bearer shares were not prohibited in Namibia in terms of sections 107 and 110(4) of the companies act 2004 as amended 2007. Further, no legal provisions exist for immobilizing bearer shares and share warrants by requiring them to be held with a regulated financial institution or professional intermediary[43]. Bearer shares present increased ML/TF/PF risk; and

g. **Nominee Persons and shell/shelf companies:** In the period under review, legal persons are allowed to have nominee shareholders and directors in terms of the Companies Act. However, there is no mechanism to prevent the misuse of legal persons by requiring the nominee shareholder and directors to disclose their identities, to be licensed for their nominee status to be included in company registries or any other mechanism identified in country. The use of nominees increases ML/TF/PF risks. Situations where a nominee is being used (e.g friend or family member is named as owner of property/assets where it is clear that the friend or family member is receiving instructions from the UBO), with no apparent legal, tax, business, economic or other legitimate reason is high. Below is an example of shell company risks that materialized in ML.

***Attractiveness of shell and shelf companies to criminals***

*A shell company or entity is a company which serves as a vehicle for business transactions without itself having any significant assets or operations. Shell companies are not in themselves illegal and they do have legitimate business purposes. Shelf companies are 'readymade' or 'off the*

42 In simple, terms, a bearer share is equity security wholly owned by the person or entity that holds the physical stock certificate, thus the name "bearer" share. The issuing firm neither registers the owner of the stock nor tracks transfers of ownership; the company disperses dividends to bearer shares when a physical coupon is presented to the firm. Because the share is not registered to any authority, transferring the ownership of the stock involves only delivering the physical document.

43 See Page 171, Under Recommendation 24, Criterion 24.11.

*shelf' companies that have often been acquired by a service provider such as a TCSP or Legal Practitioner, who holds the company with the aim of selling same in future. Shell and Shelf companies are also known as 'aged corporations', implying entities in existence for longer period. Some clients or entities may legitimately require to enable immediate trading, without prolonged business registration processes. Using a shell or shelf company promotes a long-standing image and prestige which buys social trust as a reliable entity, which has been long in existence and is not a 'fly by night'.*

*The fastness with which criminals can access such a corporate vehicle increases risks. In the so-called Fishrot case, shelf companies may have been used to receive bribes and other payments for the benefit of implicated government officials and their associates. The findings around legal persons' vulnerabilities can help inform prioritization or risk ratings for Legal Practitioners.*

## 2.7 Overall Risk Ratings

Having considered all threat and vulnerability elements raised herein and in section 8.22 of the 2020 NRA, below is an overall summary of risk ratings for legal persons and arrangements:

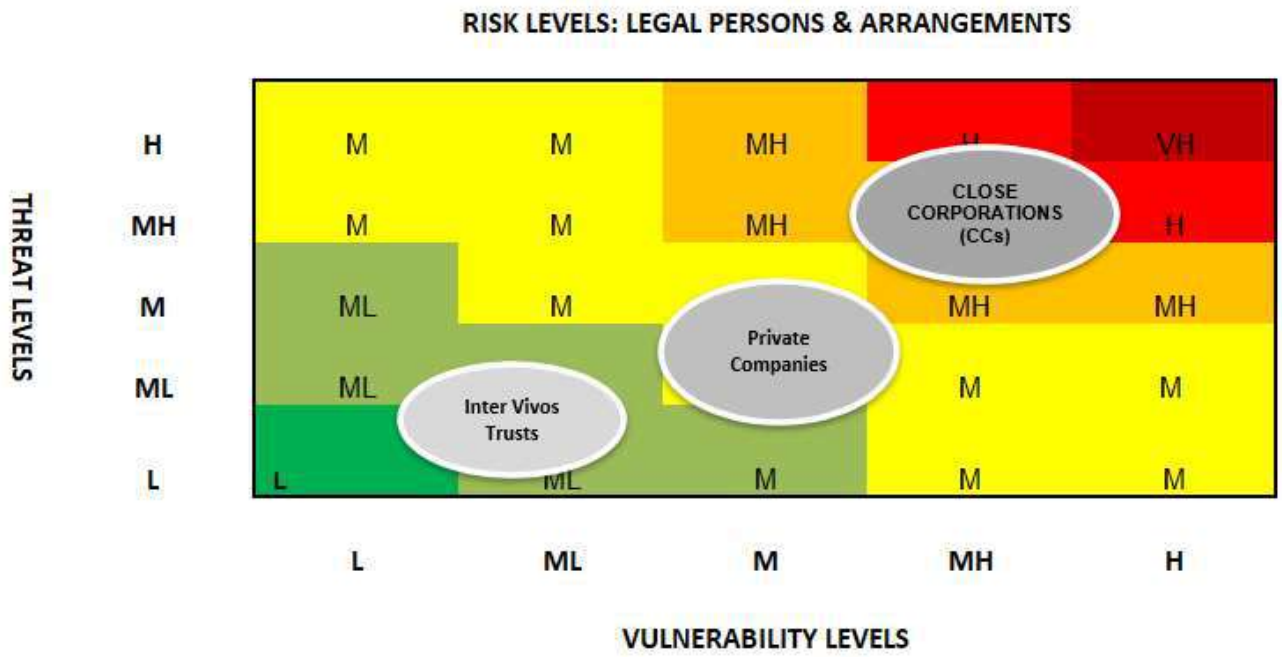



Figure 5A: Risk levels of legal persons and arrangements

# CHAPTER III: VASPs' RISK EXPOSURE

## *Chapter Summary*

*It is common cause that the amended FATF Recommendation 15 (R15) requires that VASPs be regulated for AML/CFT/CPF purposes, licensed, registered, and subject to effective systems for monitoring or supervision. Namibia has made strides in this regard. The country's 2022 Mutual Evaluation found amongst others that VASPs were not duly supervised and could expose the country to ML, TF/PF risks.*

*The ML risk assessment methodology of considering threats and vulnerabilities adopted in 2020 NRA (see sections 3 and 4) was used herein for the VASP risk assessment. Such 2020 NRA covered VAs and VASPs to a limited extent given the limited size and nature of VASP operations in the country at the time. Such assessment also rated ML/TF/PF risks associated with VAs as* ***Very High****, primarily owing to the lack of any form of supervision and absence of a licensing regime at the time. Over time, the sector has grown, with AML/CFT/CPF supervision commencing in September 2021. The 2023 NRA update is issued when Namibia has passed the Virtual Assets Act. Such Act, the first of its kind in Namibia, will lay the foundation for prudential licensing and regulation of VAs, Initial Token Offerings (ITOs) and VASPs, which until this point have only been supervised for AML/CFT/CPF purposes.*

*The main objectives of the VASP risk assessment are:*

a. *Identifying, understanding, and assessing the overall ML, TF and PF risks related to VA and VASP ecosystems in order to best ensure risk mitigation as per the FIA;*
b. *Identifying VASP products/services/delivery channels with high vulnerability to ML, TF and PF;*
c. *Outlining areas that would inform prioritizing action plans to strengthen AML/CFT/CPF controls in the VASP ecosystems; and*
d. *Shaping variables that would inform a risk-based approach to prevention and combatting measures associated with VAs and VASPs.*

*Overall, the VASP risk level, previously established as* ***Very High*** *has been revised to a* ***Medium*** *level in 2023. The commencement of AML/CFT/CPF supervision in VASPs has largely enhanced risk mitigation, resulting in reduced risk exposure. This chapter explains considerations which informed such rating.*

### 3. Overall VASP Risk Level

The risk assessment develops a comprehensive outlook of different types of VAs and VASPs and describes the main ML/TF threats they pose to Namibia. It describes the threats that can undermine vulnerabilities in VAs and VASPs in various stages of ML, TF and PF. The overall risk rating of VASPs, rated **"Very High"** as per the 2020 NRA is in 2023 revised to **"Medium."** Authorities had less understanding of the sector and VASP AML/CFT/CPF supervision activities were limited to outreach and training activities only. Supervisory activities have since 2021 picked up and this has greatly enhanced overall AML/CFT/CPF measures.

In arriving at the overall **Medium** rating, the effectiveness of mitigating measures (or vulnerability) in VASPs is **Low**, rated **0.3 or 30%**. This suggests a low level of effectiveness in preventing ML, TF or PF risks from occurring. On the other hand, the inherent risk level that VASPs are exposed to is just below the "**Medium"** level of **0.44 or 44%**. See Figure 6 below and *Annexure H* attached hereto.

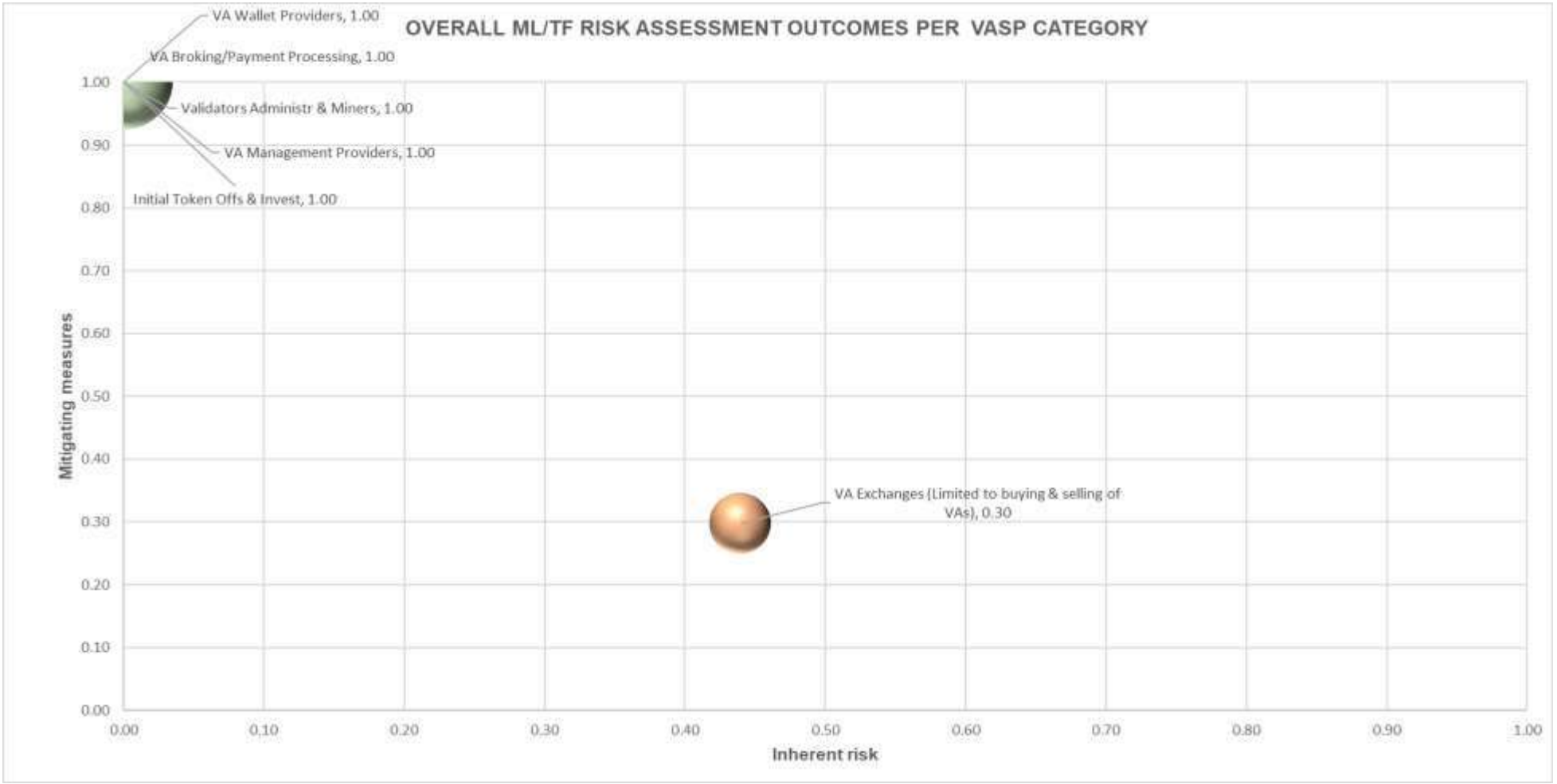



Figure 6: Outcome of VASPs Risk Assessment

### 3.1 Industry Size

Though the sector has five VASPs registered with the FIC for AML/CFT/CPF supervision purposes, only two VASPs have been active 44 . They are both domestically owned, incorporated, relatively small and owner operated. Authorities have not identified any foreign VASPs targeting the domestic VA market as per Directives 01 and 02 of 2021. The VASP sector is thus limited to the two active VASPs. In comparison to other sectors within the AML/CFT/CPF space, the VASP sector is the smallest in terms of active Accountable Institutions and the sheer financial values and transactional volumes it processes. The two active VASPs have facilitated transactions to the values below annually:

| Year | Est. Value of Transactions (both buys & sells)45 |
|---|---|
| 2022 | NAD 20 million |
| 2021 | NAD 9 million |
| 2020 | NAD 16 million |
| 2019 | NAD 3 million |

Table 9: Estimated Industry Values

The average transaction size in VASPs over the last few years has ranged between NAD 4,000 to NAD 7,000.00. Note that the minimum CDD threshold domestically across all FIs and DNFBPs NAD 5,000.00. There are thus a lot of transactions just below the CDD threshold.

### 3.2 Industry Characteristics

Namibia only has two VASPs, both provide VA exchange for fiat and vice-versa. There is no VASP offering custodial and ICOs46 related services to date domestically. Both

44 CBI has been involved in a legal battle with regulators and operations ceased for over a year. Though CBI registered with the FIC as a VASP, the FIC has not seen business activities which supports blockchain trading activities. As part of the 2023 FIA compliance assessments/inspections and the NRA update, much needed information could not be obtained and the CBI offices seem dormant as no responses were forthcoming.

45 It is estimated that the figures represent about 80-85% annually in ‘buy orders’ and the remaining in ‘sell orders’.

46 Initial Tokens Offerings.

domestic VASPs' primary trading VA is Bitcoin, with Euthereum and a few stablecoins gaining some momentum in recent times. The risk assessment identifies the inherent risk of various VA types and sub-types. Pseudo-anonymous VAs such as Bitcoin, and anonymous VAs, such as Monero, are deemed as having a very high inherent risk level due to their anonymity, usability and security features.

### 3.2.1 VA ATM

One VASP operates a VA ATM located in one of the biggest shopping malls in Windhoek. The VA ATM operations47 are similar to any *'Over The Counter'* (OTC) services which enables clients to introduce cash at the ATM in exchange for VAs which will be send to their wallet address. When a client sells VAs to the VASP, the client transfers VAs from their wallet on their device to the VA ATM and in exchange, he or she is rewarded with cash at the ATM. The ATM uses CiperTrace's screening and risk management solution which conducts all CDD/EDD measures including sanctions screening, wallet address screening and thereafter risk rates the transaction/client etc before a sale or buy order is finalised and VAs or cash redeemed.

### 3.2.2 VA Online Purchases

The country's largest domestic VASP operates online48, non-face-to-face operations, primarily in Bitcoin. The core online operations that impact ML/TF/PF risks can be described as follows and demonstrate in-built controls:

a. **Account confirmations during registration:** Prospective clients are required to create accounts online or log into their existing accounts. The registration process has a control feature which requires client confirmation by login or registering via an active email account. This enhances conventional CDD controls as email accounts can, to a certain extent, avail audit trail to authorities when the need arises. With non-face-to-face clients, especially in the virtual assets space, all such verification and confirmations are helpful. Importantly,

47 See the Crypto Kiosk website at: https://namcryptokiosk.com/

48 See: https://www.landifa.com/

identification documents, addresses, contract details and source of funds as well as source of income information are all obtained upon registration (account creation);

b. **Payments via bank services:** Clients can fund their accounts via electronic transfers (EFT), ATM or in branch deposits using the VASP's banking account details found by online. Once the funds are credited to the client's account, client can access and make use of such to buy Bitcoin;

c. **Buying bitcoin:** The entire operation is online. Client simply specifies how much bitcoin (in NAD) or vice versa the client would like to purchase from the VASP. Thereafter, client avails the bitcoin address or lightning invoice where he or she would like to receive the order;

d. **Selling bitcoin to the VASP:** Client simply specifies how much NAD worth of Bitcoin or vice versa he or she would like to sell to the VASP. After verification, the VASP's webpage displays bitcoin payment details which contain a barcode easily scannable with most Bitcoin wallets. There is an option copy such address as well. If client prefers to pay via Lightning Invoice, such option is available. Once the Bitcoin receipt is confirmed into VASP's wallet, the client's account is credited with the amount;

e. **Adding client bank account to his or her profile with VASP:** Client can add his/her bank account to their profiles online. This enhances risk management as the source of funds could come from a regulated/banking space; and

f. **Withdrawing funds to client bank account:** Client can withdraw funds to their conventional fit currency bank account. Withdrawing to bank accounts greatly reduces ML/TF and PF risks.

### 3.3 Threats in VASPs

Threats in this context speak sot the VA or VASP's accessibility by criminal elements. The inherent risk (primarily threat) level that VASPs are exposed to is just below the **"Medium"** level of **0.44 or 44%**. See Figure 6 above and *Annexure H* attached hereto.

VA related cases investigated by NAMPOL are only those few that emanated from the FIC. All such were eventually set-aside or still under investigation at the time of issuing this report. To date, the FIC received 488 STRs alleging possible ML (or predicate offences such as fraud) associated with or linked to VAs with 99% of such being filed by banks, primarily in 2021 and 2022. Only 26% of such reports were categorised as 'High Priority' and thus met the standard for further analysis and investigations while over 70% of the reports were categorised as 'Low Priority'. Most of the 'High Priority' reports were filed on the basis of contravening the Banking Institutions Act. The most common reason for suspicion cited in such reports is that the persons dealing in VAs are collecting funds from members of the public without being licensed as banks (to do so). This primarily indicates signs of persons suspected of operating ponzi or pyramid schemes in what would otherwise be considered a banking space. Apart from such, not many reports could indicate links to ML or its related primary predicate offences such as tax evasion, fraud, corruption, theft etc.

| | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | Total |
|---|---|---|---|---|---|---|---|---|
| **Banks** | 5 | 10 | 23 | 93 | 167 | 155 | 29 | **482** |
| **Financial Intelligence Units** | 0 | 0 | 0 | 0 | 0 | 1 | 0 | **1** |
| **Individual Persons** | 0 | 0 | 0 | 0 | 0 | 1 | 0 | **1** |
| **Legal Practitioners** | 0 | 0 | 0 | 0 | 1 | 0 | 1 | **2** |
| **Virtual Assets Service Providers** | 0 | 0 | 0 | 0 | 0 | 1 | 1 | **2** |
| **Total** | **5** | **10** | **23** | **93** | **168** | **158** | **31** | **488** |

Table 9: STRs received from different sectors relating to VAs

| Name of LEA | No. of SDs | Amount Involved (N$) |
|---|---|---|
| Anti-Corruption Commission of Namibia | 1 | 12,000,000.00 |
| Namibian Police Force | 20 | 27,000,000.00 |
| Office of the Prosecutor General | 5 | 12,000,000.00 |
| Bank of Namibia | 79 | 202,000,000.00 |
| **Total** | **105** | **253,000,000.00** |

Table 10: Financial Values in VA related reports escalated by the FIC to different LEAs

Care needs to be taken in interpreting the threat or impact emanating from Financial Values cited in Table 10 above as a few persons who have claimed to be trading in VASPs appear to be suspected of running Ponzi or Pyramid Schemes. The VA component is alleged to be simply used as a front for such 'get-rich quick' schemes, which are illegal. Investigations almost always find that there are hardly any indications or footprints on the blockchains to support claims of VA related crimes.

### 3.3.1 Unidentified Threats

From their own EDD, monitoring and reporting measures, VASPs as a sector only reported two STRs as shown in Table 9 above, with both reports being filed by one VASP. FIA Compliance inspections in VASPs observed client conduct or transactions that should have been detected and subjected to EDD, with an eventuality of either preventing the continuation or reporting such to the FIC or law enforcement. From the FIC's June 2022 compliance inspections as well as both 2020 and 2023 NRA observations, VASPs' EDD, monitoring and reporting measures were largely ineffective and thus generally failed to detect and prevent or report potential ML suspicions. The next section expands on this observation. Note however that as at end of August 202349 VASP follow up assessment activities revealed enhancements in risk management frameworks at individual VASP level.

### 3.3.2 National Threat Level Validation

Wallet address screening is an essential component in any VASP operation. Pseudonimity and Anonimity means quite often only wallets are visible to a VASP or LEAs on a distributed ledger (blockchain). The mere wallet address screening to determine if such addresses are in any way sanctioned, linked to darkwebs/nets, associated with or made use of mixers, tumblers or similar anonymity enhancing sites or services is an essential control in VASP operations. One of the VASPs had a subscription with CipherTrace which enabled them to make use of CipherTrace's

49 VASPs were made to sign enforceable undertakings in June/July in which they committed to address compliance findings by 10 August 2023. Such was indeed attended to and significant improvements were noted in August 2023 follow up assessments.

AML/CFT solution. Such solution not only does risk assessments of each client/transaction but importantly also screens to establish if a wallet address can be associated with mixers, tumblers or similar anonymity enhancing sites or services.

As part of the NRA threat level validation activity, wallet addresses were sampled from both VASPs and results thereof suggests no single wallet address could be linked with or associated with any such high risks. *Annexure I* present outcomes of such validation exercise with wallet addresses from local VASPs. The exercise was premised on a ChainAnalysis API data dump by running all the addresses through the ChainAnalysis sanction screening API. Thereafter, the transactions were reversed by a few hops and such were screened as well. Threats can originate from different elements including privacy coins. Privacy coins such as Monero which are privacy-focused and encrypt their transactions using zero-knowledge proofs or similar private technology naturally enhance risks as they are attractive to criminals. The FATF50 draws special attention to unlicensed and non-compliant exchanges that offer privacy coins as an area of specific and significant risk. Fortunately, the FIA Compliance Assessment and this risk assessment did not detect privacy coins or links thereto in domestic wallets and VASP activities.

Again, all outcomes indicate that no wallet address tested was in any way sanctioned, nor linked to darkwebs/nets, mixers, tumblers or similar anonymity enhancing sites or services.

### 3.4 Vulnerability Considerations

The effectiveness of mitigating measures (or vulnerability) in VASPs is **Low**, rated **0.3 or 30%**. This suggests a low level of effectiveness in preventing ML, TF or PF risks from occurring. This has changed slightly from the 2020 NRA observations which found same literally non-existent. Supervisory authorities had no assurance that AML/CFT/CPF controls are implemented and are operating effectively.

50 FATF Report on VA Red flag Indicators: Accessible via: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pd

### 3.4.1 Comprehensiveness of the AML Legal Framework

The comprehensiveness of the prudential regulation and licensing framework is an essential component for AML/CFT/CPF effectiveness. At the time of issuing this report, there was no prudential licensing regime for VASPs in Namibia. VASPs are only registered and supervised by the FIC for AML/CFT/CPF purpose. Given the above, VASPs are not subjected to any form of prudential, licensing and regulation domestically. The Virtual Assets Act has since passed and come into effect. The law creates a prudential regulation and licensing regime for VASPs under the Bank of Namibia (within the Exchange Control function).

Having the above in mind, the assessment rated this component **Low** (a score of 0.3 or 30%).

### 3.4.2 Availability and Effectiveness of Market Entry Controls

The primary component of market entry controls that emanate from prudential licensing and regulation is ensuring UBOs and persons managing the affairs of an institution are fit and proper and thus cannot unduly expose institutions or sectors to ML, TF and PF abuse. Given the absence of such prudential licensing regime, the FIC conducted due diligence on the UBOs (owners and those managing their affairs) of all VASPs. All financial supervisory bodies confirmed that such persons were not at any point denied market entry to sectors under their supervision, nor where they subjected to any disciplinary matters that could bring their integrity or fitness into question. The Namibian Police equally availed clearance certificates which indicates that none of them were ever convicted of criminal offences. Within the FIC's database, they do not appear to have been subjects in matters investigated either. There has not been any indication of them having had any ties to other foreign jurisdictions, which would have necessitated due diligence with such relevant foreign authorities.

The sector is the smallest under FIC supervision and comprises of two entities only. Due diligence measures as highlighted herein are deemed helpful though not ideal. The fitness and probity exercise undertaken by the FIC has availed reasonable

assurance that BOs in VASPs are fit and proper. The overall rating was thus set at **Medium** (a score of 0.5 or 50%)

### 3.4.3 Effectiveness of AML/CFT/CPF Supervision

The FIC is the VASP supervisory body for AML/CFT/CPF. Below is the FIC's supervisory footprint in the sector since 2020.

| Date | Supervisory Activity |
|---|---|
| | |
| Jun-20 | Sectoral vulnerability and threat engagements for the 2020 NRA. |
| | |
| Feb-21 | Sectoral NRA Vulnerability engagements plus considerations of draft NRA report. |
| | |
| July - August 2021 | Consultations on drafting Directives 01 and 02 of 2021 on VASP FIA Compliance. |
| | |
| 22/03/2022 | Issued Directive 01 of 2022 and Directive 02 of 2022 |
| | |
| 29/03/2022 | Sectoral Stakeholder Engagement |
| | **Agenda** |
| | 1. Sectoral CDD Guidance Note for VASPS and MVTS |
| | 2. VASPS Compliance Assessment Methodology |
| | |
| Jan 2023 - April 2023 | Sectroral Risk Assessments |
| 13 to 17 February 2023 | Public consultation for VASP Bill (VASP and Various other sectors) |
| 14-Mar-23 | Public Consultation engagement for VASP BILL (VASP and Various other sectors) |
| | |
| 16-May-22 | CBI Exchange Directive |
| | |
| 01-Jul-22 | Financial Technology (Fintech) Innovations Regulatory Framework |
| | |
| May-23 | Notification on the Compliance Assessment for Landifa |
| | Notification on the Compliance Assessment for CRYPTO Kiosk |
| | |
| 07-Jun-23 | Sectoral Stakeholder Meeting |
| | **Agenda:** |
| | 1. 2020 National Risk Assessment update |
| | 2. Proposed amendments to CDD threshold of NAD 5,000 |
| | 3 STR/SAR Reporting Behaviour |
| | 4. TF Risk Awareness and TFS |
| | 5. Sectoral Guidance a) VASP Risk Assessment methodology and b) VASPS RBA |
| | |
| 03-Jun-23 | Completion of each VASPs' FIA Compliance Assessment. Full scope compliance assessments tested every key FIA obligation's compliance. |
| 05-Jul-23 | Referral of all such reports for Enforceable Undertakings: Both VASPs agree to address all FIC findings by no later than 10 August 2023. FIC to conduct follow up review to assess progress after such date. |
| 06-Jul-23 | Both VASPs sign Enforceable Undertakings with the FIC Director, commiting to address findings within one month. |
| | |

Table 11: FIC's risk-based supervisory activities in the sector

In September 2023, follow up reviews were undertaken to understand the progress in implementation of controls by the one active VASP. The impact of the above-mentioned supervisory activities can be summarised in the findings of the FIA compliance assessments. Below is a summary thereof, as taken from inspection/assessment reports:

| Risk Management Measure | June 2023 Findings/Ratings | Way Forward | Aug/Sept 2023 Findings/Ratings |
|---|---|---|---|
| Risk assessment | Ineffective | Signed an undertaking end of July 2023 with FIC Director to address controls by 10 August 2023. | Compliant |
| AML/CFT Program | Partly Compliant | | Compliant |
| CDD | Effective | | Effective |
| EDD Measures: Include ability to detect PEPs, monitor to report STRs (Sector has reported 2 STRs only) | Ineffective | | Moderately effective |
| Record keeping | Effective | | Effective |
| Screening against UNSC sanctions lists | Moderately effective | | Effective |
| Subjecting AML/CFT controls to independent audit | Ineffective | | Ineffective |
| Targeted Financial Sanctions: freezing, reporting without delay and prohibition) | Ineffective | | Effective |

Table 12: Impact of supervision activities

Table 12 above suggests simplified CDD was being undertaken but not so with EDD measures as at June 2023. Findings from the June 2023 FIA compliance Assessments suggests that though local PEPs may not be using VASPs (at least not directly), there are high networth clients making use of the domestic VASPs. The few PEPs were duly identified and subjected to relevant measures. High networth clients on the other hand were duly identified and source of income, funds etc obtained but they were not considered inherently high risk even when their transacting behaviour suggested such. Both VASPs did not meet expectations in this regard. The sector is considered attractive to this type of customer due to its reduced transparency. VASPs should keep in mind that the terrorist financing risk is also significant as these vulnerabilities exploited for ML can equally be exploited by those advancing terrorist activities as they explore means to raise and move value or funds without detection or tracking by LEAs. The primary concern in findings remains VASPs' ability to duly monitor, detect and

report suspicious transactions and activities. The FIC was not convinced that control improvements as per September 2023 findings were to the desired satisfaction. Equally, VASPs have yet to comply with the FIA obligation of subjecting their AML/CFT controls to independent audit reviews.

Before the first assessment VASPs conducted screening against UNSC sanctions lists but documenting proof of same was not done consistently. This has changed for the better as per September 2023 follow-up reviews. TFS measures were duly documented and VASPs demonstrated how they are able to timely detect, and cause assets freezing and reporting of subjects without delay while prohibiting further transactions. AML programs and entity level risk assessments fell short of requirements in June 2023 because they lacked adequate details to avail FIC reasonable assurance. VASPs were availed guidance on how to improve on such. The entity level risk assessments had, to a large extent, improved as per September 2023 findings. Worth noting is that one of the VASPs in particular has subscribed to CipherTrace which enables effective risk assessment51 and wallet screening before a transaction is finalised.

VAs where not subjected to any AML/CFT/CPF supervision in the period leading up to the 2020 NRA and hence the impact of supervisory activities was thus rated Zero or Non-existent (score of 0.0 or 0%). Given the enhanced supervisory impact reflected in Table 12, effectiveness of supervision and oversight activities was thus assigned a **Medium High** rating (score of 0.6 or 60%). Despite the September 2023 improvements, the NRA is of the view that time needs to be accorded to the sector to demonstrate sustainability of effectiveness over time.

### 3.4.4 Integrity of VASP staff

The domestic VASPs are relatively small and owner operated. With each VASP, the owner is thus also the registered AML Compliance Officer who attends to all AML/CFT/CPF risk management activities. The fitness and probity exercises

51 This risk assessment measure appears to have been in place as per June 2023 compliance assessment but its effective functioning mechanism was not duly demonstrated to the FIC's inspection team during the assessment activity.

undertaken by the FIC as part of market entry controls did not find anything that would impair the integrity levels of the staff managing VASPs. They have no criminal records and had not been found in breach by any supervisory bodies such as the Bank of Namibia or NAMFISA. An overall rating of **High** (0.8 or 80%) was reached for this variable.

### 3.4.5 AML knowledge of VASP staff

See above findings (3.4.4). Staff members appear to duly understand their ML, TF and PF risk exposure and FIA obligations though implementation challenges which often require investments are a challenge for the VASPs. Accordingly, a rating of **Medium High** (score of 0.6 or 60%) was assigned.

## 3.5 Inherent Vulnerability: Products, Services and Delivery Channels

### 3.5.1 Use of Cash

VA transactions operate on various platforms including the blockchain. Pseudonimity and anonymity are significant and they are the cornerstones of blockchain transactions. Non-face-to-face engagements are also the order of the day on the blockchain. All these features escalate ML vulnerability of VAs.

The higher the volume of cash activities, the higher the inherent risk of a service to potential ML. One VASP accepts cash deposited at its ATM as its only source of receiving fiat currency. Inherently, its risk exposure is higher. The other VASP does not accept any cash and receives funds only via transfers from bank accounts via EFT or mobile financing services. When funds are directly sourced from a client's bank account, overall threat levels are reduced because funds are originating from a regulated space which is subject to AML/CFT/CPF. At a national level, overall risk is reduced because the VASP with a significantly higher market share does not accept cash. The use of cash is high risk but consideration of the nationally aggregated volume and values of cash suggests its use is relatively limited to about 20% of the market, at most. Therefore, the risk rating for cash usage is rated Low (0.20 or 20%).

### 3.5.2 Absence of Face-to-Face Controls

The absence of face-to-face engagements when business relationships are established or when client conducts VA transactions is inherently high across conventional VASP platforms.

Domestically, at an individual VASP level, the VA ATM enables identification by requiring a scanning of the client ID and client posing in front of the ATM for the machine to take an ID photo of the client as part of simplified CDD measures before services are availed. All clients are identified through such photos and scanning of their ID documents. The June 2023 FIA Compliance Assessment found such to be very reliable. All tests conducted suggest that the ID photo taken at the machine matches the face/image on the national ID documents scanned in and such can be reconstructed by LEAs if need arises. This technology is used around the world in similar services.

The VASP which avails services online relies on prudent CDD upon client account opening which is verified through email confirmations, along with the submission of a scanned ID copy. This control could be abused easier by criminals who may transact through other persons but the fact that clients' funds can only be received from bank accounts helps reduce risks significantly.

As mentioned above, VASPs should keep in mind that the terrorist financing risk is also significant as these vulnerabilities exploited for ML can equally be exploited by those advancing terrorist activities as they explore means to raise and move value or funds without detection or tracking by LEAs.

Taking into account the volume of transactions in both domestic VASPs, the degree of anonymity/pseudonymity and the peer-to-peer (which can arise after securing VAs from local VASP) transferability without bespoke control, this input variable, while inherently High is reduced to a residual level of **Medium**. There is a very high threat that non-face-to-face activities could lead to transactions with high-risk individuals or entities, transfer of value, or undertaking third-party funding through virtual exchanges.

Therefore, VA-related activities represent a growing ML/TF threat on the basis of abuses which could arise from non-face-to-face controls/engagements.

### 3.5.3 Traceability

Blockchain technology provides transparency and traceability for all transactions. However, it is common cause that the transaction conductor's true identity may never be known if the travel rule is not implemented. At present, as mentioned herein above, the two VASPs in operation do not avail services beyond the exchange of VAs for fiat currencies and vice versa. The travel rule thus does not apply as there are no custodial or remittance services facilitated by local VASPs. VAs that have not been subjected to the travel rule generally maintain some form of pseudonymity or anonymity.

There are several attributes that LEA may use to trace users and uncover anonymity. These could be through unique Internal Protocol (IP) addresses and transaction history through blockchain forensics. VAs can be analysed through different mechanisms to understand their ML/TF risks. Nevertheless, VAs carry significant ML/TF threats due to the unavailability of dedicated tools at Namibian Authorities' disposal to effectively and efficiently traced VAs on the blockchain. At the time of issuing this report, the FIC is in the process of subscribing with a service provider to make use of such services. Until authorities are able to better trace blockchain transactions, this remains a **High** risk.

### 3.5.4 Speed of Transfer

Although transactions involving VAs are, in most cases, quickly verified and permanently recorded on distributed ledgers publicly, the ability to send large volumes of value across borders is very much easier than through traditional financial institutions. With no controls over the size and value than can be transferred, the system is vulnerable to abuse by criminals. Similarly, the vulnerability is enhanced due to the lack of tools and training for LEAs in Namibia to trace a financial transaction through a public ledger.

With terrorist activities, they often want to operate as fast as possible before LEAs can catch up and disrupt their activities. The speed with which values can thus be moved around the world on blockchains is attractive to those advancing and supporting terrorism.

The lack of potential to trace, monitor, and detect suspicious criminal activity encourages 'speed transfer' by service operators. The threat of evading investigations and probing from competent authorities through these speedy transactions is **Medium**.

### 3.5.5 Dark Web and Darknet Access

The NRA, as stated in section 3.3.2 above has not observed any signs of darknet market operations in the local VA space. This is however limited to jurisdictional footprints within the scope of the two VASPs. Inherently, vulnerability is enhanced because in spaces where these darknets or dark markets operate – there are usually greater anonymity characteristics, VAs are offered as the preferred form of payment for illicit items or procurement of restricted or sanctioned items usually acquired for criminal activities or nefarious transactions. The service providers offer Web that relies on encrypted services to shield users' identifying information and communications.

Despite the lack of indicators of dark web or dark net operations/services etc., the fact that the VASP with the biggest market share (in terms of financial values and transactional volumes) did not screen clients and transactions to detect and prevent dealing with wallets exposed to such high risks only enhances risk exposure (in the period under review). It is hoped that mechanisms can be established to mitigate against this risk. This variable is rated **High**.

### 3.5.6 Creation and Transfer of Blockchain Valuables

Namibia's risk exposure is enhanced partly from the absence of Travel Rules enforcement and technological solutions for tracing transfers, especially for VAs that could be financed through proceeds of crime and those with unhosted wallets. The country could also be exposed to a rise in thefts of valuable goods as the market for so many valuables such as non-fungible tokens (NFTs) grows. With NFTs, the

challenge is that anyone can create or “mint” a digital file as an NFT, regardless of whether they have rights to as the process is anonymous.

### 3.5.7 Decentralised Environments

Decentralised environments, especially where peer-to-peer transactions take pace are high risk. It should also however be note that the FATF scope of a VASP supervised for AML/CFT/CPF does not call for regulation of peer-to-peer transactions but rather for VASPs to have an ability to identify such (be reverting a few hops back) and if detecting, subjecting such wallets/transactions to EDD like all high risks.

Non-hosted wallets and Decentralised Finance (DeFi) are the medium of the VA ecosystem aiming to reduce or eliminate transaction intermediaries through decentralised computer networks. The system works without intermediaries like VASPs, and banks. There is also NFT which operates through smart contracts. Even when VAs are sourced from a VASP and the necessary due diligence is undertaken as per the FIA, the lack of mechanisms and expertise amongst LEAs to trace values on the blockchain means clients or criminals can simply take such acquired VAs (e.g through proxies) to conduct peer-to-peer transactions. This also means peer-to-peer transactions by locals or between locals and foreigners are not readily accessed by LEAs.

## 3.6 Other Sectors’ Risk Exposure from VASPs

This section looks at the impact of VAs and VASPs on other sectors in the AML/CFT/CPF regime. It was informed by risk assessments of other sectors. Overall, no sectors under FIC supervision accept VAs as a means of payment or appear to trade in that space, apart from VASPs. This therefore suggests that if such sectors are to be abused for ML in particular, it is most likely through VA liquidated payments or handling of funds generated through VAs given that the true origin of such could be proceeds of crime.

### 3.6.1 Banking Sector

As mentioned in section 3.3 above, the FIC received 488 STRs alleging possible ML associated with or linked to VAs with 99% of such reports being filed by banks, primarily in 2021 and 2022. Over the years, the banks have stated[52] that VAs and VASP operations, especially if not effectively supervised can unduly expose their services to abuse. The lack of a licensing regime which result in uncertainty as to who is licensed to operate does not help matters. At some point, a few banks expressed reservations around onboarding customers dealing in VA activities. The two active VASPs however have access to banking facilities. To date, the banks have not shown interest in investing in the VA space or partnering with VASPs despite the emergence of VAs.

In some countries, certain entities licensed as fiduciary service providers or security and investment service providers are involved in NFTs. Under the FATF framework, an NFT could be a VA or an investment if it is not for payment purposes. Therefore, when banking such stakeholders, banks had to perform a test to determine if clients dealing in NFT are VASPs or investment providers. At present, the NRA did not observe presence of NFTs that could be associated to Namibia. It must however be cautioned that the NRA team admitted to not having the expertise to identify all NFTs or such other related tokens which can be associated to Namibia.

The FIC's observations, as AML/CTF/CPF supervisory body of banks, is that some have not duly conducted risk assessments to detect VASPs and subject such to relevant CDD or EDD measures as per the FIA. There are hardly any tailored VA and VASP monitoring activities. It is stated herein above that banking customers are already using banking products and services such as debit and credit cards to acquire VAs online. Customers also undertake wire transfers to VASP exchanges for purchases and even withdraw directly to their bank accounts through the VASP transferring funds from its banking account to that of the client as settlement for VAs. This mainly happens with Bitcoins.

The risk level that banks may be exposed to is rated **Medium**. Primary considerations are that the VA ATM only deals with cash, though the buying of VAs can be redeemed

52 In several FIC/BAN meetings. A position reiterated this year.

in a bank account via another VASP that has the capacity to do so. The Online VASP exposes banks in terms of financial values, such accounts for about NAD 12 – 15 million annually and most of its clients are clients from the banking sector who are already subjected to the banks' due diligence measures. The greatest concern is threats in the form of the origin of various VAs on the blockchains which at some get redeemed via banks directly or indirectly.

### *3.6.2* ADLAs[53] *(Bureaux de Changes)*

There are some similarities in the nature of VA Exchange services and ADLAs' currency exchange and remittance services. A few clients interviewed by the FIC in April 2023 who made use of VASP's services indicated to have previously made use of ADLAs' services. Some appreciate the anonymity but more the speed with which VA remittances are transmitted to beneficiaries. ADLAs, like banks also indicated to not have appetite for VAs and VASPs. However, it was observed that ADLAs may face direct competition from VA exchanges which provides an easy and cost-effective way of transferring value. There is an indication that ADLAs in some parts of the world are partnering with stakeholders in the VA ecosystem or banks to explore using a dedicated network to effect transfer to a country with heavy reliance on money service business. BCD could also be positioned to convert fiat to VA or vice versa.

There are very minimal engagements between VASPs and ADLAs that could enhance risk exposure to ADLAs. Therefore, the risk exposure from VASPs to ADLAs is **Low**.

### 3.6.3 Non-Banking Financial Institutions (NBFI) Sector

NBFIs include ADLAs, lending Institutions and all non-banking financial institutions under NAMFISA supervision. The NBFI's position is not too different from the posture taken by banks but with a slightly higher/better appetite than banks in the appreciation of VASPs. This does not any in way suggest that NBFIs have embraced VASPs. At present, there are no domestic VASPs offering custodial or investment type of services

53 Authorised Dealers in Foreign Exchange with Limited Authority (typical money service businesses)

which could compete with or be an option clients would consider in addition to what is offered in the conventional fiat financial system.

NBFIs have not deliberately identified VASPs and their operations in order to appreciate the risks from the VA space which may impact them. However, local VASPs only provide 'over the counter' services. The NRA observed minimal, if any, direct VA exposure to NBFIs from both local and foreign VASPs. Overall, there are very minimal engagements between VASPs[54] and NBFIs that could enhance risk exposure to NBFIs. Therefore, based on all observations at hand, the risk exposure from VASPs to NBFIs is **Low**. This is however expected to change when the larger VASPs, which avail custodial and investment related services are licensed and roll out operations domestically. Such larger VASPs are in the Bank of Namibia's regulatory sandbox at the time of issuing this report. The NBFI's risk position in this regard may need to be reviewed when this happens.

### 3.6.4 Designated Non-Financial Businesses & Professions (DNFBPs)

With the exception of Legal Practitioners, Accountants and other TCSPs, most other DNFBPs' exposure to ML, TF and PF risks associated with or originating from VAs and VASPs is rated **Low**. Legal Practitioners, Accountants and other TCSPs' exposure to such risk is rated **Medium**. Such rating emanates from these sectors having more exposure than other DNFBPs to VAs, VASPs and persons dealing in that ecosystem, directly or indirectly. The considerations below inform such risk ratings.

#### a. Dealers in precious stones and metals, Real Estate, Casinos, and Motor Vehicle Dealers

These sectors did not record any transactions associated to VAs. Similarly, there are hardly any threats/cases showing proceeds from VAs being used to trade in this space, though the absence can also be attributed to failures to detect. These sectors required to comply with the FIA and subject transactions to CDD or EDD as the need may be. It is quite helpful that some in the sector demonstrated some basic understanding of

54 directly or through their clients.

VAs though most indicated to have not associations or dealings with VAs. Most do not understand VA's technicalities, and this further exposes them to potential abuse.

### b. Legal Practitioners, Accountants and other TCSPs

These sectors appear to have a better understanding of VAs than the above DNFBP sectors. A legal practitioner filed an STR[55] citing valid grounds for a transaction involving a certain client. Some indicated to have serviced clients who at some point had footprint in the VA space. They required to comply with the AML/CFT/CPF obligations but many could not specify any controls tailored to detect client associated with VAs and subject them to the relevant EDD measures. This suggests they could be paid with proceeds from illicit activities potentially channelled through or linked with VAs.

For PF purposes, the 2020 NRA, in the PF risk assessment chapter highlighted how legal practitioners' trust accounts may have been used to avail services to a client de-risked by all banks on suspicion of possible PF risks. The employees of such client would be paid in cash and they ended up remitting such cash via ADLAs (MSBs) to the Democratic People's Republic of Korea (DPRK). Note that there were no VASPs domestically. There is therefore reason to believe that in the current environment were VAs could assist with faster remittances and better anonymity, PF and TF sympathisers or supporters could exploit VAs.

***Examples of abusing professional services***

Professionals like legal practitioners and accountants could interact with VASPs in many ways and may wittingly or unwittingly advise or prepare financial statements in such a way to mask VA activities as there is no VA and VASP legislation in place.

In the absence of a regulatory direction of travel, just like the accountants, lawyers too may wittingly or unwitting partner with digital currency entities to provide legal support on VA

55 It may only be one STR but the grounds for suspicion shows an appreciation for risks emanating from that space. Most sectors, apart from banks have not filed a single STR involving VAs.

| |
|---|
| issuance, developing VA related services etc and hopefully benefit as they achieve traction in the market. |

With the Virtual Assets Act in place, a prudent licensing and regulatory regime will be implemented and such could significantly reduce ML, TF and PF risks that DNFBPs are exposed to emanating from or associated with VAs.

# CHAPTER IV: TRAFFICKING IN PERSONS (TIP)

## *Chapter Summary*

*The ML risk assessment methodology of considering threats and vulnerabilities adopted in 2020 NRA (see sections 3 and 4) was used herein for the TIP risk assessment. There has been a change in Namibia's TIP risk position since the 2020 NRA. This chapter explains considerations which informed such change.*

*Namibia was upgraded to a Tier 1 country in the 2020 TIP Report for fully meeting the minimum standards for the elimination of human trafficking. At the time, Namibia was the only country in Africa to achieve a Tier 1 ranking in 2020, joining 34 nations globally. In 2023 however, Namibia was downgraded to Tier 2 owing to reduced effectiveness in combatting overall threats of TIP. There are not many comprehensive studies and information on this crime. The observations herein are thus based on statistics from the Namibian Police and TIP Study by the US State Department on various countries around the world.*

## 4. Threats and Vulnerabilities

### 4.1 Threats and prevalence

The following statistics, obtained from LEAs, relating to TIP are worth noting:

a. 101 reported cases of TIP from 2020 to mid-2023;
b. Out of these cases, 38 were under investigation, 24 were to be tried or are undergoing trials while 5 have been submitted to the Prosecutor General for a decision on the way forward; and
c. 34 cases to date have been finalised.

The above statistics correspond to the Minster's of international relations and cooperation's statement on the commemoration of *World Day Against Trafficking in Persons (TIP)* and the launch of the TIP national plan at Oshikango, in late July 202356. Overall, the average number of new TIP cases noted or reported annually fluctuates between 4 and 10. The following observations around such cases (threats) are worth noting:

a. As reported over the past five years, human traffickers exploit domestic and foreign victims in Namibia, and traffickers exploit victims from Namibia abroad. Some victims are initially offered legitimate work by recruiters for adequate wages, but then traffickers subject them to forced labor in urban centers and on commercial farms;

b. Traffickers subject Namibian children to sex trafficking and forced labor in agriculture, cattle herding, and domestic service. Following the influx of 5,000 – 8,000 Angolan migrants fleeing severe drought in southeastern Angola, Namibians increasingly employ Angolan children as domestic workers and cattle herders, increasing their vulnerability to exploitation. Traffickers bring children from Angola and neighboring countries and subject them to sex trafficking and forced labor, particularly in agriculture, cattle herding, domestic

56 https://www.namibian.com.na/101-cases-of-human-trafficking-in-13-years/

servitude, street vending in Windhoek and other urban centers, and in the fishing industry;

c. Namibians commonly care for children of distant relatives to provide expanded educational opportunities; however, in some instances, traffickers exploit these children in forced labor; and

d. Among Namibia's ethnic groups, San and Zemba children are particularly vulnerable to forced labor on farms or in homes.

Because in most cases it is persons trafficked for what may seem to be cheap labour, it is not readily determinable what the potential gains or financial flows and ML is. In some cases, the illicit gains can be estimated by understanding what the fair or market wage could be. Also, if sales of products emanating from illicit labour are noted, such sales can be associated with the crime of TIP but such is limiting as the pain and suffering, illicit abuse of children for labour cannot be readily quantified in monetary terms.

### 4.2 Vulnerabilities in Combatting Framework

The TIP report, published by the US Department of State[57] is the world's most comprehensive resource on governmental anti-trafficking efforts. A country's tier ranking in such report reflects outcomes of the assessment of that government's efforts during the reporting period to meet the minimum standards for the elimination of TIP. Namibia was upgraded to a Tier 1 country in the 2020 TIP Report for fully meeting the minimum standards for the elimination of human trafficking. At the time, Namibia was the only country in Africa to achieve a Tier 1 ranking in 2020, joining 34 nations globally. In 2023 however, Namibia was downgraded[58] to Tier 2 owing to the factors which impact overall vulnerability to TIP:

57 U.S Embassy in Namibia. June 2020. https://na.usembassy.gov/namibia-upgraded-to-tier-1-country-in-trafficking-in-persons-report/

58 https://www.state.gov/reports/2023-trafficking-in-persons-report/namibia/#:~:text=An%20NGO%20noted%20an%20increase,jobs%20and%20groom%20potential%20victims.

a. Namibia does not fully meet the minimum standards for the elimination of trafficking but is making significant efforts to do so. These efforts include identifying more victims and providing assistance for a large influx of male trafficking victims, repatriating Namibian victims exploited abroad, and providing anti-trafficking training to law enforcement and members of the judiciary;

b. However, the said efforts were not serious and sustained compared with the efforts during the previous reporting period, even considering the impact of the COVID-19 pandemic, if any, on the government's anti-trafficking capacity. The government did not report on any of its efforts to investigate trafficking crimes or prosecute or convict traffickers. The government also did not report on its efforts to identify trafficking victims;

c. The report found that the government inappropriately penalized victims with incarceration, fines, and deportation solely for offenses committed as a direct result of being trafficked and detained potential trafficking victims, even after identification as such by government officials, instead of referring them to care; and

d. Occasional breakdowns in communication between government officials and civil society and within government ministries led to a lack of coordination among members of the National Coordinating Body (NCB). Limited understanding and inconsistent use of the NRM and SOPs by front-line officials hindered overall efforts.

# CHAPTER V: RECOMMENDATIONS

## 5. Recommendations

Most recommendations in the 2020 NRA and Namibia's 2022 ESAAMLG ME Report are adequate to address risks raised herein, if duly implemented. Most stakeholders have made reasonable progress in implementing such ME recommendations, at the time of issuing this report. suffice. This section lists a few primary recommendations worth prioritising:

### 5.1 Supervisory Authorities

#### 5.1.1 VASP Prudential Licensing and Regulation

a. Commence the prudential licensing and regulation regime now that the Virtual Assets Act is in place. The practical starting points would be:
   - capacitating the supervision team around VAs and VASP, given the technical nature of this ecosystem; and
   - acquiring the necessary digital or automated solution to help with supervision functions on blockchains.

b. Work with AML/CFT/CPF supervision authorities to enhance overall risk mitigation and safeguard the sector from abuse. This should include mechanisms to prevent persons who are not fit and proper from participating in the sector as service providers/operators. Equally, deliberate efforts need to be made to detect unlicensed operators and discourage their operations; and

c. With the desired FIA amendments passed, immediately commence enforcement of the NPO regulatory and licensing regime effectively.

#### 5.1.2 NPO supervisory bodies

a. Enhance the NPO regulatory and licensing regime effectively, as per the FIA and FIC guidance to mitigate TF risks;

b. Work with AML/CFT/CPF supervision authorities to enhance overall TF risk mitigation and safeguard the sector from abuse;

c. This should include mechanisms to prevent persons who are not fit and proper from participating in the sector as service providers/operators. Equally,

deliberate efforts need to be made to detect unlicensed operators and discourage their operations.

### 5.1.3 AML/CFT/CPF Supervision

a. Ensure timely implementation of digitisation and automation efforts or additional recruitments of staff to address resource constraints;
b. Strengthen mechanisms aimed at prioritizing supervision in line with varying risk levels as observed herein, relating to legal persons and arrangements, TF risks, FATF-NPOs, VASPs;
c. Build capacity and enhanced understanding in the growing ecosystem of VASPs and how to effectively supervise such; and
d. Enhance working relationships with prudential licensing authorities of VASPs and DNFBPs to mitigate risks of inadequate market entry controls which could permit access to persons who may not be fit and proper.

## 5.2 Investigating and Combatting Authorities

a. The ACC, NAMRA and NAMPOL are encouraged to align their combatting efforts to key observations herein. One such is realization that CCs and *inter-vivos* trusts are most abused to advance ML and TF, while being mindful that PF could also be advanced through similar vehicles;
b. Though work has recently started in this regard, NAMPOL, ACC and NAMRA are encouraged to maintain data and statistics on cases under prosecution (and finalised ones) in a manner that duly informs the national combatting framework and its effectiveness levels;
c. The 2020 NRA and ME Recommendations to enhance resources or capacity in terms of staff members remains paramount;
d. Similarly, the needs to ensure staff members are continuously availed training or capacitated to deal with technical and evolving challenges such as cases related tax VAs and VASPs. This also requires investing in digital solutions to enable tracing and analysis in blockchains and such ecosystems;

e. NAMRA in particular could do with targeting transactions in the VA space as that is an area increasingly embraced by locals as shown by growing transactions in VAs;
f. Coordination and collaboration: there are no results showing that NAMPOL investigates ML cases associated with or linked with the predicate offence of tax evasion, while the 2020 NRA suggests such offence is the most prevalent amongst a host of ML predicate offences; and
g. Similar to the above, though corruption is a major predicate offence of ML, there are hardly any indications of the ACC making significant use of FIC referrals, disclosures etc to enhance investigations. The minimal prosecutions of ML linked corruption offences as would be expected from results of effective parallel investigations is a concern.

### 5.2.1 Office of the Prosecutor General (OPG)

a. Though work has started in this regard recently, the OPG is encouraged to maintain data and statistics on cases under prosecution (and finalised ones) in a manner that duly informs the national combatting framework and its effectiveness levels;
b. The 2020 NRA and ME Recommendations to enhance resources or capacity in terms of staff members remains paramount; and
c. Similarly, the needs to ensure staff members are continuously availed training or capacitated to deal with technical and evolving challenges such as cases related tax VAs and VASPs.

## 5.3 Financial Institutions, NBFIs and DNFBPs

### 5.3.1 VASPs

a. Duly consider the threats and vulnerabilities highlighted herein and align risk management measures accordingly; and
b. Make use of the recently workshopped and published sectoral guidance notes (available on the FIC website: https://www.fic.na/index.php?page=2023-guidance-notes ) on conducting internal risk assessments and implementing risk based controls effectively.

### 5.3.2 FBOs and Charities

a. Implement relevant internal governance structure and frameworks to protect NPO operations and services. This should start with governance bodies such as boards of directors, management or oversight committees, accountability mechanisms around the deployment and use of NPO resources;
b. As per the sectoral guidance from the FIC (available on the FIC website: https://www.fic.na/index.php?page=2023-guidance-notes ), conduct internal risk assessments with due considerations to donors, beneficiaries or their associates and any ties they may have to high risk jurisdictions or terrorist groups;
c. Duly consider the threats and vulnerabilities highlighted herein and align internal risk management measures accordingly; and
d. Make use of the recently workshopped and published sectoral guidance notes on the FIC website to implement risk based controls effectively.

### 5.3.3 All other Financial Institutions and DNFBPs

All other Financial Institutions and DNFBPs are encouraged to heed the risk observations herein and accordingly align their risk assessments and risk based mitigation controls. The FIC and NAMFISA has of late workshopped and issued sectoral guidance. The guidance notes are available on their respective websites.

## 5.4 Trafficking in Persons

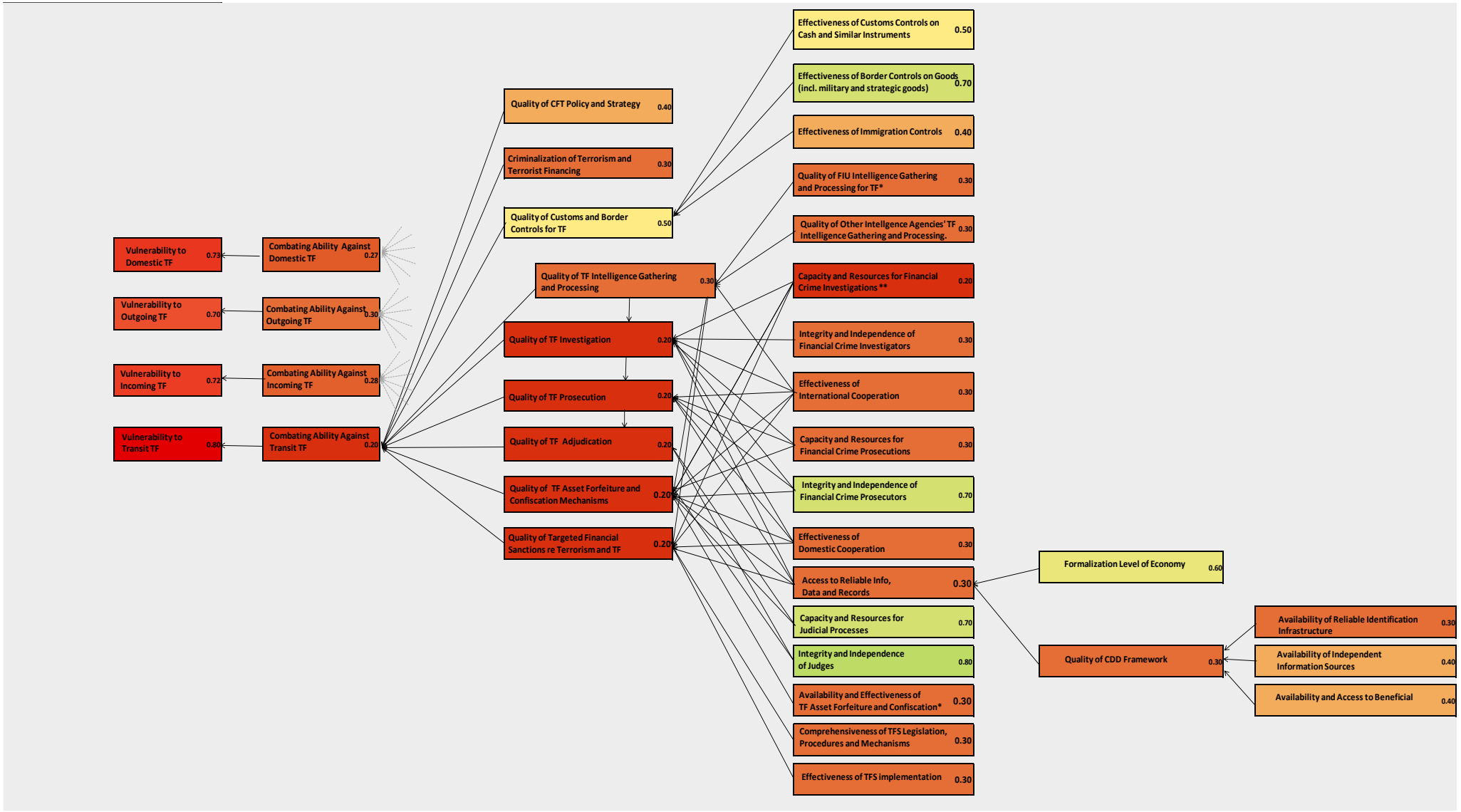
The improvements that need to be made include:

a. Enforcing the Combating of Trafficking in Persons Act of 2018;
b. Training LEAs to duly understand and maintain relevant statistics on TIP crimes;
c. Prosecuting more human traffickers with stricter penalties. For this to happen, Namibia needs to consider enhancing investigative capacity;
d. Identifying and caring for more victims;

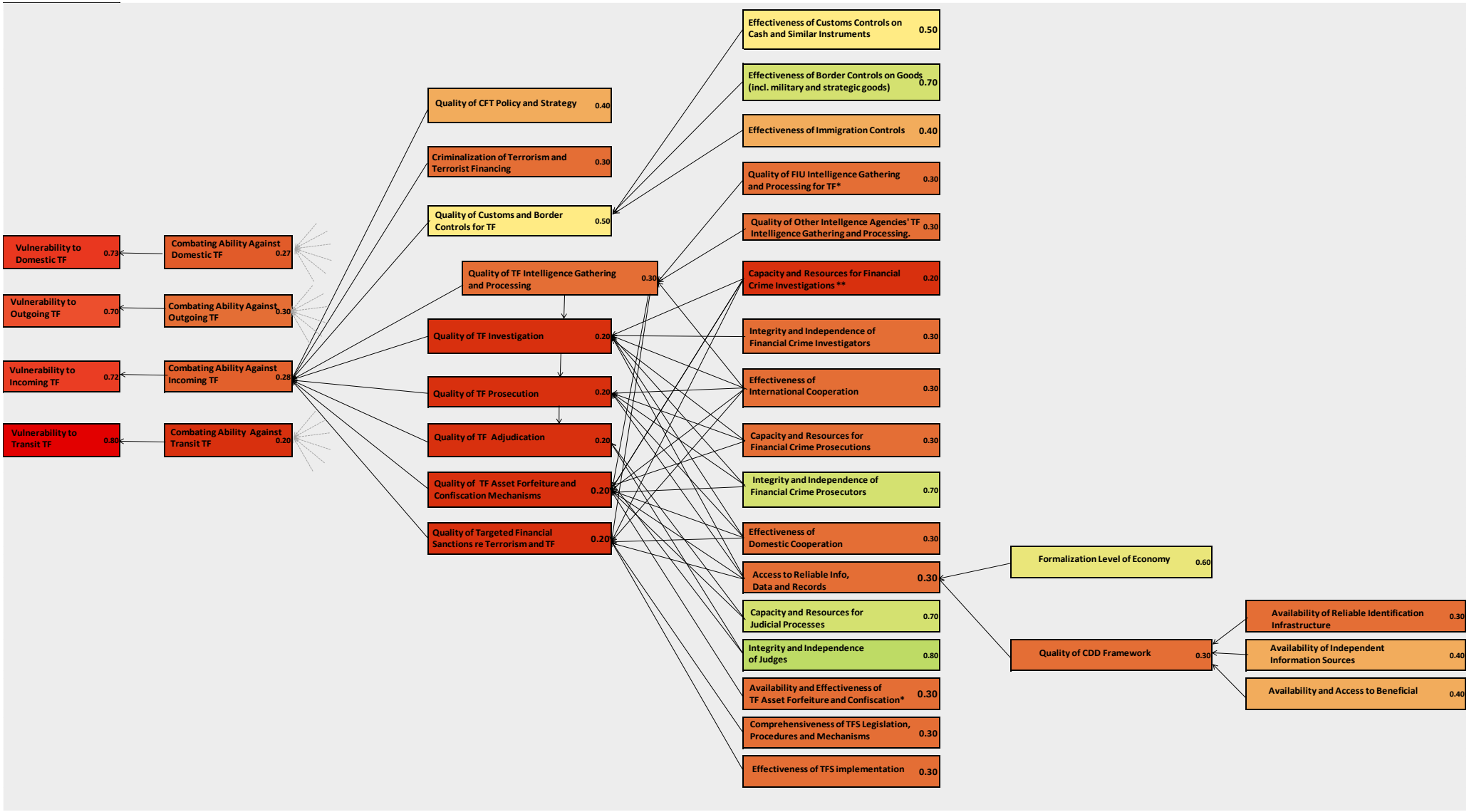
e. Launching ongoing awareness campaigns to reach those marginalized; and

f. Increasing prevention efforts and training.

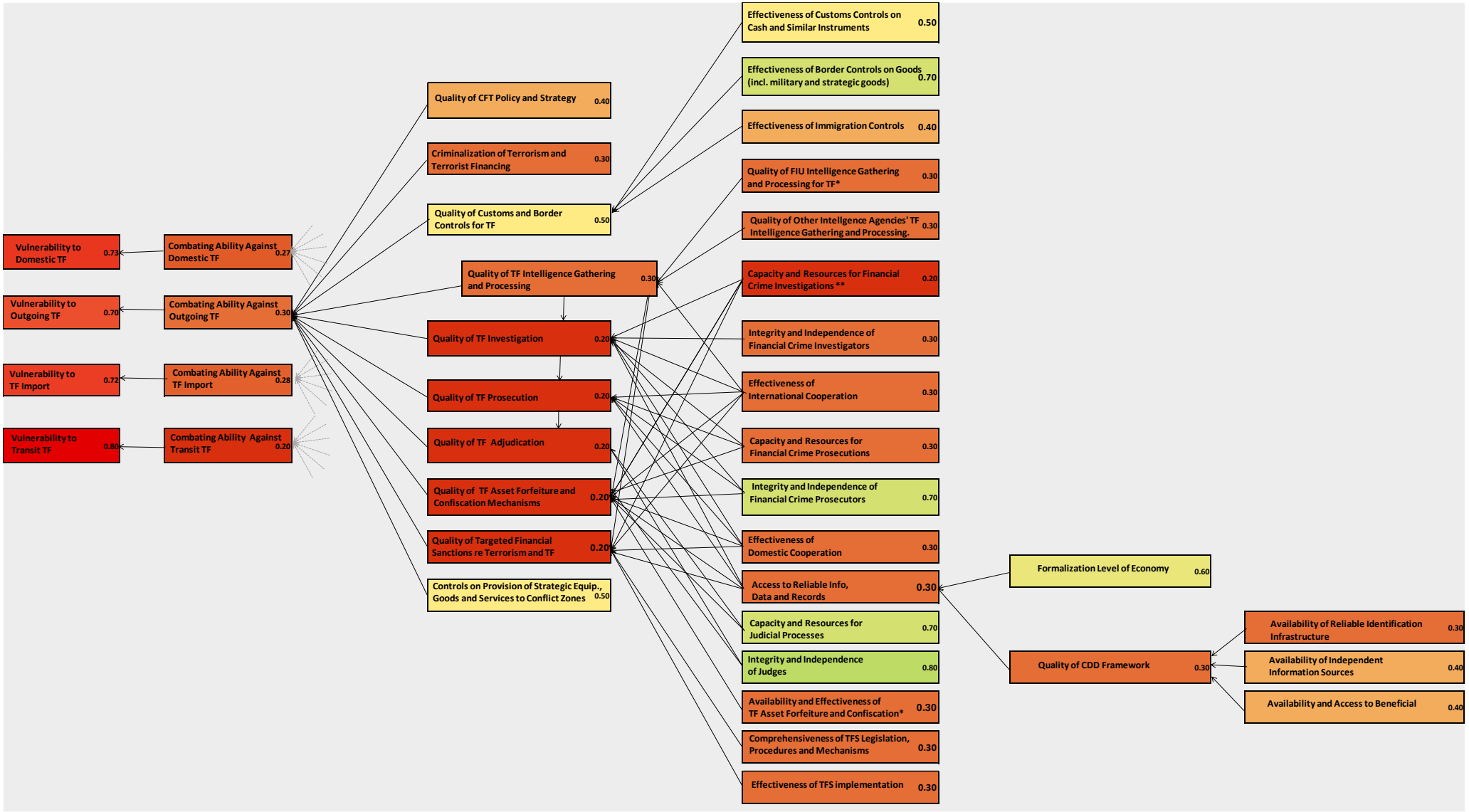
## ANNEXURE A: TF Vulnerability Map – Transit TF



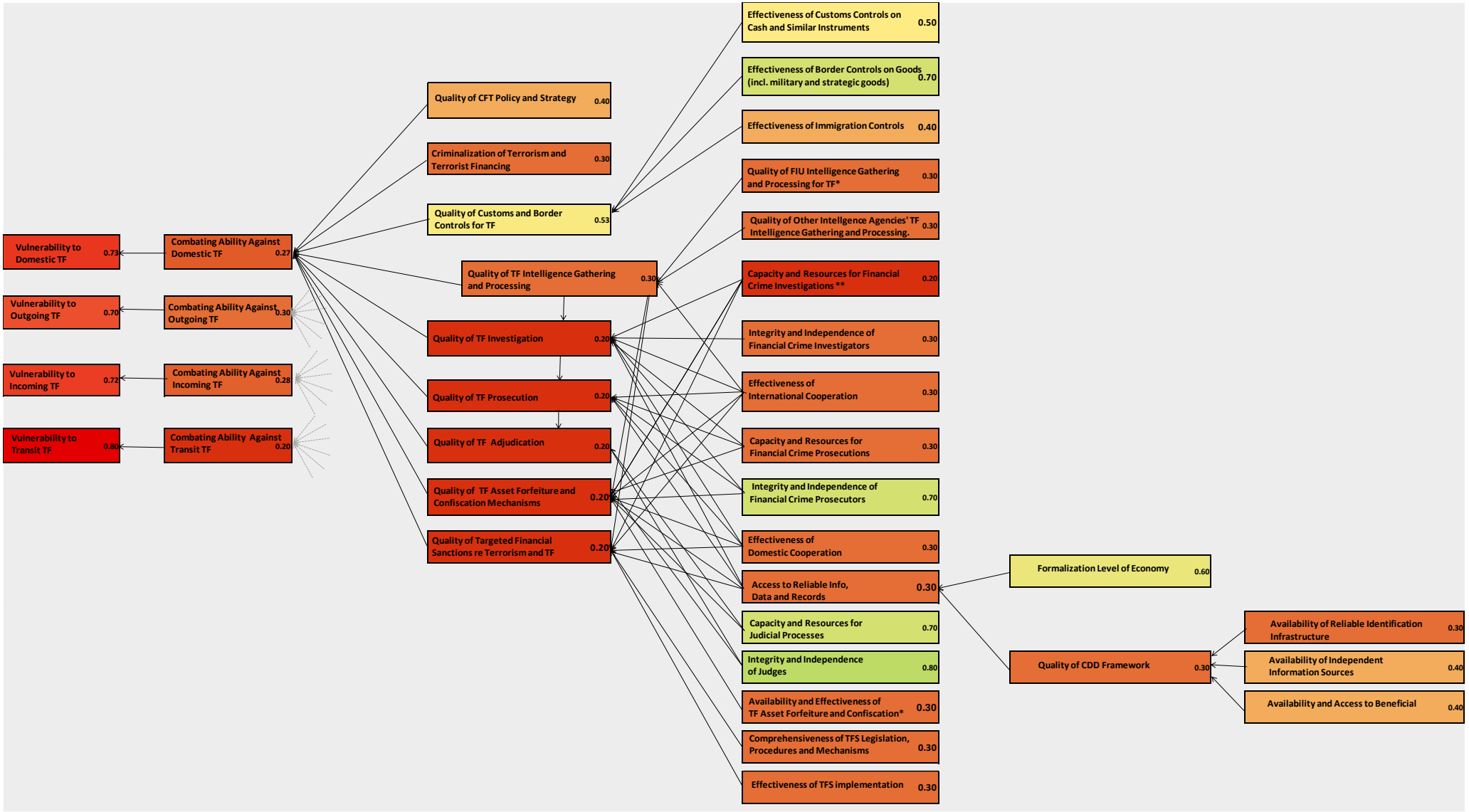
# ANNEXURE B: TF Vulnerability Map – Incoming TF



# ANNEXURE C: TF Vulnerability Map: Outgoing TF



# ANNEXURE D: TF Vulnerability Map: Domestic TF



# ANNEXURE E: Basis for TF Vulnerability Risk Ratings and Prioritization List

| PRIORITIES | Current State | Ideal Scenario | Variable Impact Test Results (Combating Ability) | | | | Comparison with Ideal Scenario (Combating Ability) | | | | Action Priority Score (range 0 -100) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Run the impact test / Reset the test outputs | | 0.7 | Domestic | Outgoing | Incoming | Transit | Domestic | Outgoing | Incoming | Transit | Domestic | Outgoing | Incoming | Transit |
| Quality of CFT Policy and Strategy | 0.4 | 0.7 | 0.659 | 0.668 | 0.667 | 0.664 | 0.041 | 0.032 | 0.033 | 0.036 | 14 | 11 | 11 | 12 |
| Criminalization of Terrorism and Terrorist Financing | 0.3 | 0.7 | 0.300 | 0.300 | 0.300 | 0.300 | 0.400 | 0.400 | 0.400 | 0.400 | 100 | 100 | 100 | 100 |
| Effectiveness of Customs Controls on Cash and Similar Instruments | 0.5 | 0.7 | 0.697 | 0.620 | 0.620 | 0.586 | 0.003 | 0.080 | 0.080 | 0.114 | 1 | 27 | 27 | 38 |
| Effectiveness of Border Controls on Goods (incl. military and strategic goods) | 0.7 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Effectiveness of Immigration Controls | 0.4 | 0.7 | 0.695 | 0.580 | 0.580 | 0.614 | 0.005 | 0.120 | 0.120 | 0.086 | 2 | 40 | 40 | 29 |
| Quality of FIU Intelligence Gathering and Processing for TF | 0.3 | 0.7 | 0.620 | 0.643 | 0.600 | 0.567 | 0.080 | 0.057 | 0.100 | 0.133 | 27 | 19 | 33 | 44 |
| Quality of Other Intellgence Agencies' TF Intelligence Gathering and Processing | 0.3 | 0.7 | 0.300 | 0.300 | 0.300 | 0.300 | 0.400 | 0.400 | 0.400 | 0.400 | 100 | 100 | 100 | 100 |
| Capacity and Resources for Financial Crime Investigations | 0.2 | 0.7 | 0.427 | 0.468 | 0.422 | 0.200 | 0.273 | 0.232 | 0.278 | 0.500 | 91 | 77 | 93 | 100 |
| Integrity and Independence of Financial Crime Investigators | 0.3 | 0.7 | 0.689 | 0.691 | 0.686 | 0.623 | 0.011 | 0.009 | 0.014 | 0.077 | 4 | 3 | 5 | 26 |
| Capacity and Resources for Financial Crime Prosecutions | 0.3 | 0.7 | 0.579 | 0.604 | 0.602 | 0.629 | 0.121 | 0.096 | 0.098 | 0.071 | 40 | 32 | 33 | 24 |
| Integrity and Independence of Financial Crime Prosecutors | 0.7 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Capacity and Resources for Judicial Processes | 0.7 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Integrity and Independence of Judges | 0.8 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Effectiveness of Domestic Cooperation | 0.3 | 0.7 | 0.650 | 0.659 | 0.660 | 0.669 | 0.050 | 0.041 | 0.040 | 0.031 | 17 | 14 | 13 | 10 |
| Effectiveness of International Cooperation | 0.3 | 0.7 | 0.700 | 0.586 | 0.600 | 0.567 | 0.000 | 0.114 | 0.100 | 0.133 | 0 | 38 | 33 | 44 |
| Availability and Effectiveness of TF Asset Forfeiture and Confiscation | 0.3 | 0.7 | 0.664 | 0.657 | 0.670 | 0.668 | 0.036 | 0.043 | 0.030 | 0.032 | 12 | 14 | 10 | 11 |
| Comprehensiveness of TFS Legislation, Procedures and Mechanisms | 0.3 | 0.7 | 0.700 | 0.700 | 0.656 | 0.300 | 0.000 | 0.000 | 0.044 | 0.400 | 0 | 0 | 15 | 100 |
| Effectiveness of TFS implementation | 0.3 | 0.7 | 0.700 | 0.700 | 0.656 | 0.300 | 0.000 | 0.000 | 0.044 | 0.400 | 0 | 0 | 15 | 100 |
| Formalization Level of Economy | 0.6 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Availability of Reliable Identification Infrastructure | 0.3 | 0.7 | 0.666 | 0.672 | 0.669 | 0.654 | 0.034 | 0.028 | 0.031 | 0.046 | 11 | 9 | 10 | 15 |
| Availability of Independent Information Sources | 0.4 | 0.7 | 0.700 | 0.700 | 0.700 | 0.700 | 0.000 | 0.000 | 0.000 | 0.000 | | | | |
| Availability and Access to Beneficial Ownership info | 0.4 | 0.7 | 0.675 | 0.679 | 0.677 | 0.665 | 0.025 | 0.021 | 0.023 | 0.035 | 8 | 7 | 8 | 12 |
| Controls on Provision of Strategic Equipment, Goods and Services to Conflict Zo | 0.5 | 0.7 | | 0.679 | | | | 0.021 | | | | 7 | | |
| | | | | | | | | | | | The higher the score, the higher the priority | | | |

**ANNEXURE F: SMUGGLING ATTEMPTS**

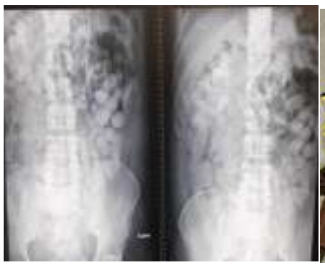
a. **Attempted cash smuggling:** On 21 April 2021, An Egyptian national was arrested for *failure to declare* in terms of Section 36 of the FIA, an amount of USD 16, 018.00 and Euro 2,700.00 which was concealed in a shoe before boarding Ethiopian Airline at Hosea Kutako International Airport.

b. **Attempted drug smuggle:** Namibian woman was caught at the Hosea Kutako International Airport on 14 April 2021 attempting to smuggle crystal methamphetamine worth NAD1.5 million from Namibia to Brazil. The drugs were discovered by a Police K9 unit during a search at the airport. The drugs were covered with carbon, plastic and sellotape and then hidden inside the lining of the suitcase.

c. **Attempted drug smuggling:** On 16 June 2021, The Namibian Police and NamRA Customs intercepted a Namibian national who was in possession of +- 570,000 Mandrax tablets with an estimated street value of NAD 6.8 Million.

**d. Attempted drug smuggling:** On 01 November 2021, a 40-year old Brazilian was arrested

at Hosea Kutako International Airport after he was found with 98 bullets of suspected cocaine valued at NAD 343 000.00**.** This was a NamRA Customs intelligence driven operation.





e. **Attempted drug smuggling:** On 18 October 2021, The Namibian Police and NamRA Customs conducted an undercover operation were five (5) suspects were arrested for smuggling cannabis of 114.810 kg valued at NAD 5,740,500.00.


f. **Attempted abalone smuggling:** On 01 October 2021, a suspect was arrested under Seeis CR 10.09.2021 while attempting to export 25 boxes of Abalone products to Hong Kong without Aquatic Organism import and export permit.


g. **Under declaration of goods:** On 06 January 2021 at 04:00AM, Customs received intelligence that there was a truck offloading goods in Windhoek, Katutura. After opening, customs discovered that company had only declared the consignment of cool drinks valued

at NAD 180,000.00 and goods valued at NAD 233,761.19 were not declared. The trucking company was fined a penalty of NAD 400,000.00 and the owners of the goods were fined a penalty of NAD 71,000.00 for smuggling.

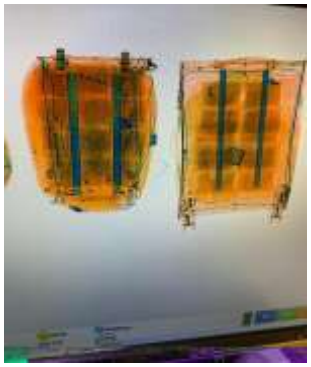

h. **Under declaration of goods:** On 19 January 2021, NamRA Customs Authorities at Walvis Bay conducted a physical examination on a container originating from China. Customs discovered that all the goods in the container were not declared and there was no invoice, nor packing list provided. A total of 10,599 pieces of different goods were found and the importer was allowed to declare all the goods and was levied/charged an amount of NAD 80,457.40 on duties and taxes along with penalties amounting to NAD 40,000.00 which were collected.


i. **Attempted Drugs Smuggling:** Joint drug seizure took place between Trans-Kalahari Border Post and Windhoek through a control delivery. On 16 April 2022, Customs intercepted a truck with drugs and arrested 13 suspects and 7 vehicles that were used in the commission of the crime were impounded along with cash proceeds of NAD18,350.00; R 10,000.00 and 20 Pulas. Drugs seized is as per below.

| Product Name | Weight | Estimated Value N$ |
|---|---|---|
| Cannabis | 357,320 g (357.32 kg) | 10,713,900.00 |
| Crack Cocaine | 390 g | 39,000.00 |
| Mandrax Tablets | 10 185 | 1,222,200.00 |
| **Total Estimated** | | **11,975 100.00** |

j. **Smuggling protected fauna and flora:** Namibia participated in the joint WCO joint operation codenamed “THUNDER 2022 Operation”, had its operational phase from 3-30 October 2022, with the participation of 125 countries and territories. Through routine inspections and targeted controls, hundreds of parcels, suitcases, vehicles, boats, and cargo transporters were examined, often with the use of sniffer dogs and X-ray scanners. Searches at land and air border checkpoints focused on illegally traded species protected by national legislation or CITES. In Southern Africa, a total of twenty-two (22) cases of fauna and flora were reported by Namibia. Majority of these case are from the Blue Rhino anti-poaching unit and only few are from Customs such as timber at Katwitwi and Port of Walvis Bay. The operation also collected NAD 77,714.00 in terms of revenue and issued penalties amounting to NAD 16,000.00.

k. **Attempted Drug Smuggling:** A suspect with a dual nationality of South Africa and Tanzania was on the 01 January 2023 intercepted at Hosea Kutako International Airport coming from Brazil via Angola. The suspect confessed that the drugs in his possession belonged to someone in South Africa, and he was asked to collect the drugs in Brazil and deliver them in Namibia where someone was to collect the parcels and deliver them in South Africa. He further authorities that he was given USD 6,000.00 (NAD 102,000.00) to deliver the drugs. In total two luggage bags consisting of one (1) bag and one (1) suitcase containing 48 parcels of white powder valued at NAD 5 million, weighing 10kg, suspected to be cocaine was seized by the Namibian Police. In addition, an amount equivalent to NAD 8,461.33 *(R70,00; USD 451,00 and Reais 224,00)* and a Huawei mobile phone were also handed over to the Police under same chain of custody.


l. **Smuggling hazardous goods:** A total of 159 ODS cylinders R22 were seized at Ariamsvlei Border Post in August 2022 for contraveing the Customs and Excise Act, 1998 (Act 20 of 1998) Section 123 (1)(e) Prohibitions and restrictions on Import and Export permit Control Act No 30 of 1994 as per the Montreal Protocol on Substances that Deplete the Ozone Layer (the Montreal Protocol).

m. **Attempted Cash Smuggle:** On 07 December 2022, a Namibian national was arrested at Ngoma Border Post after he attempted to smuggle and failed to declare cash valued at USD 3,350,00 *(220 x 100 = USD 22,000; 23 x 50 = USD 1,150)* or NAD 401,710.00. This is in contravention of section 14 of the Customs and Excise Act, 1994 and section 36 of the FIA. The suspect, who was risk profiled by a customs officer, travelled from Namibia to South Africa then to Zambia and back to Namibia as per his travel documents. Goods (cash) were seized by the Police.

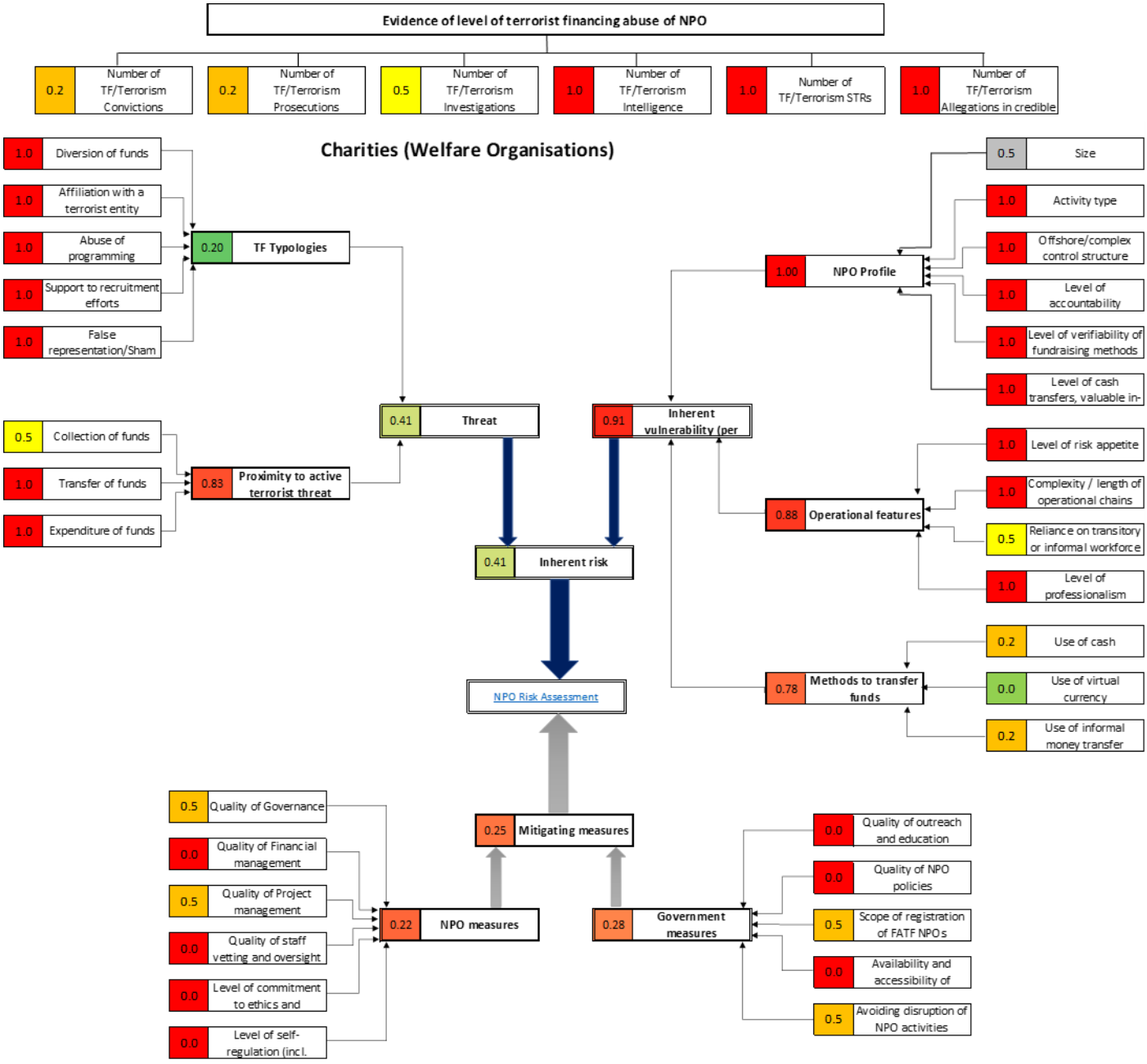
**n.** **Destruction of IPR infringing goods:** Between 10 -13 May 2023, NamRA, in collaboration with the Brand Right Holders from various law firms conducted a workshop in Windhoek and Walvis Bay on Intellectual Property Rights. This was followed by other similar workshops for two days in each region and included the destruction of IPR infringing goods valued at over NAD 5 million seized in Windhoek and at the Port of Walvis Bay in terms of the Customs and Excise Act 20 of 1998 and Part III of the TRIPS Agreement.

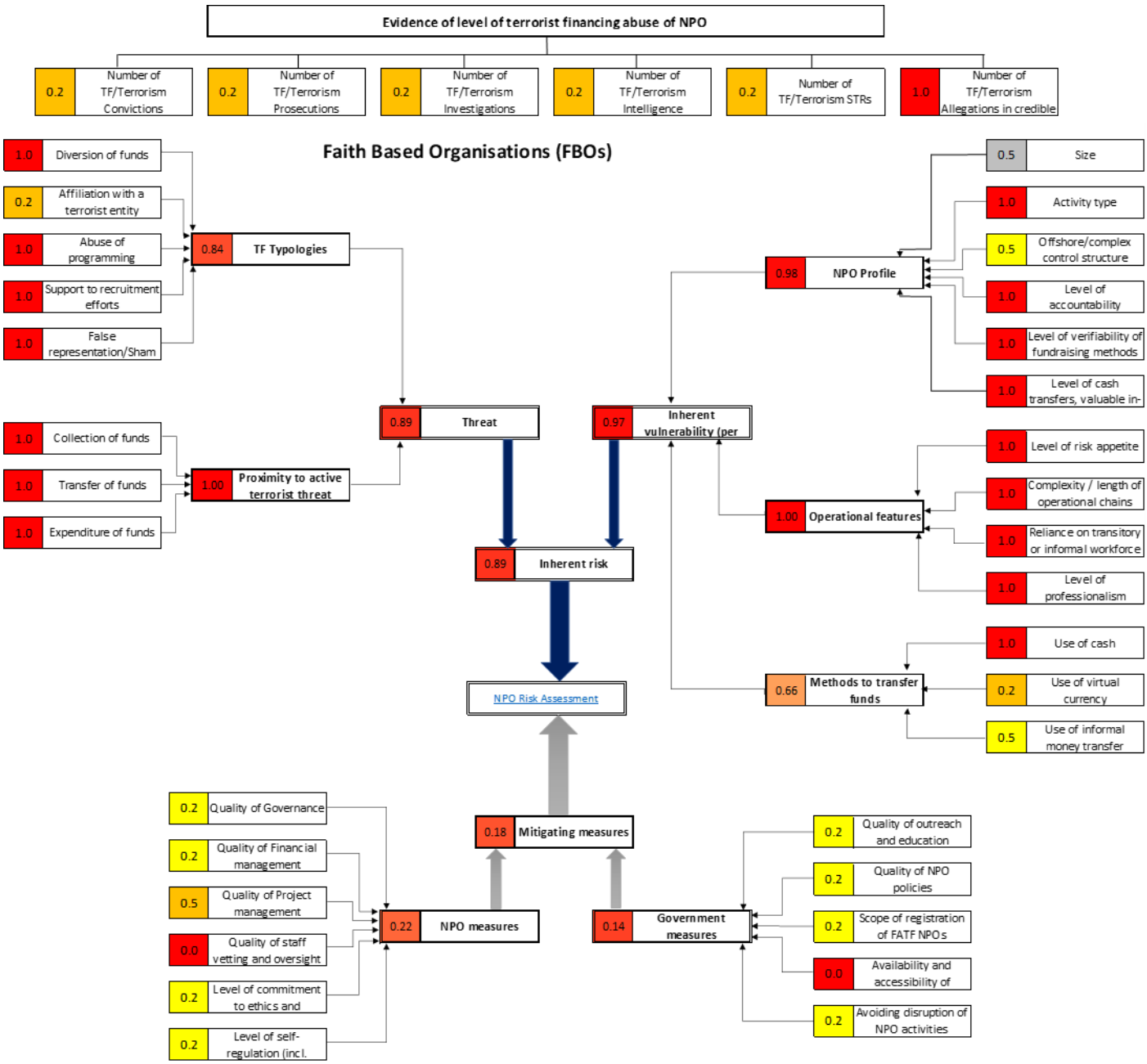
**o.** **Northern Cape police confiscate R3 million worth of drugs en route to Namibia:** News2459 reported that officers were carrying out an inspection at the Nakop border post when they stopped the truck in the early hours of Sunday, 25 June 2023. Police spokesperson Sergeant

59 https://www.news24.com/news24/southafrica/news/northern-cape-police-confiscate-r3-million-worth-of-drugs-en-route-to-namibia-20230626

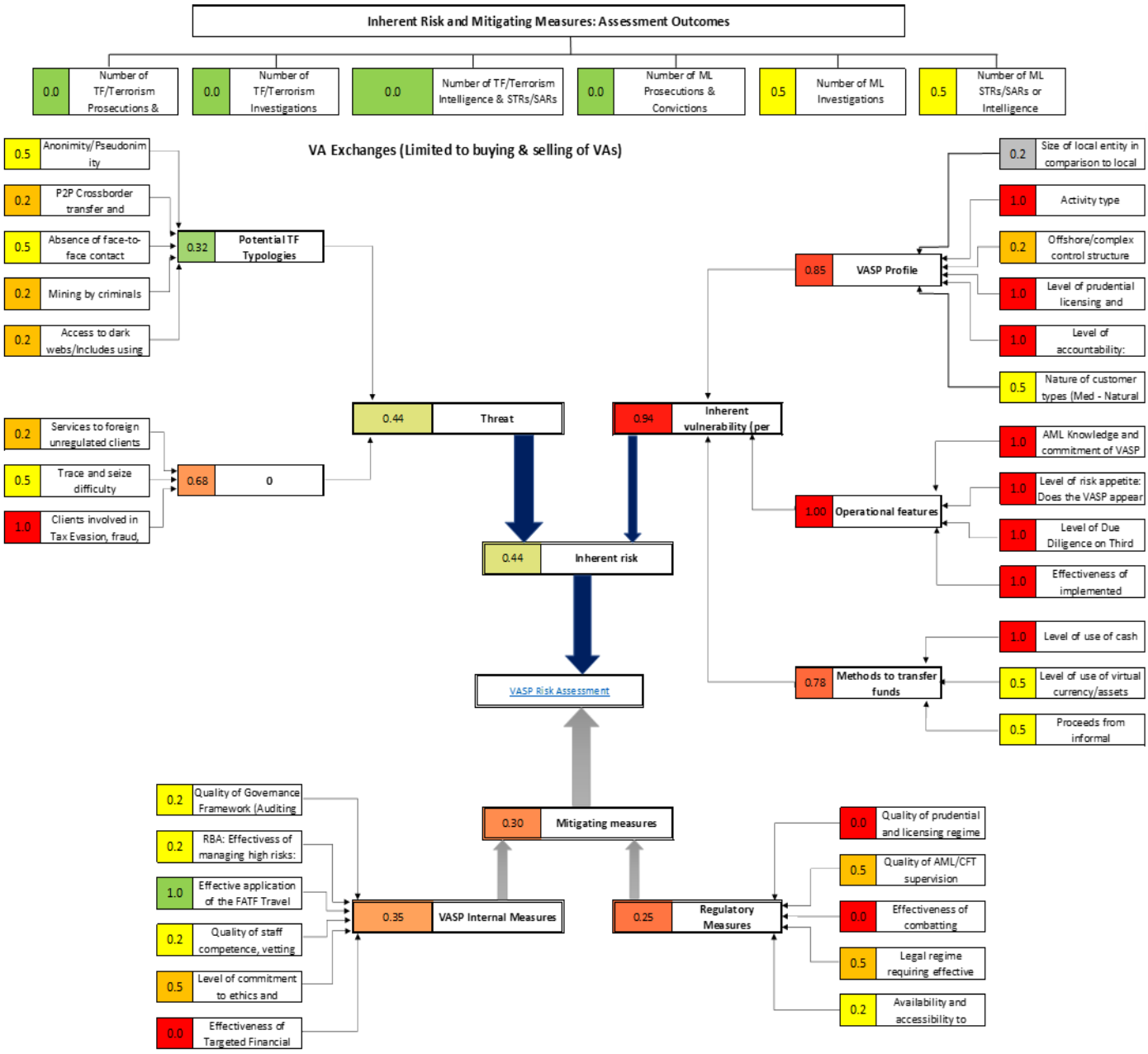
Omphile Masegela said the officers found seven boxes containing more than 114kg of dagga inside the truck. At the time of the arrest, the truck driver was arrested for drug trafficking and was due to appear in court, said Masegela. The bust comes days after Eastern Cape police confiscated 32 blocks of cocaine, with an estimated street value of just under R13 million, at the Port of Ngqura. National police spokesperson Brigadier Athlenda Mathe said border police officers at the port made the discovery on Wednesday, 21 June 2023. The drugs were inside a cargo container destined for the United Arab Emirates.

## ANNEXURE G: TF RISK ASSESSMENT OUTCOMES (FOR OTHER NPO SUBSETS CAN BE AVAILED ON REQUEST)




Evidence of level of terrorist financing abuse of NPO
0.2 Number of TF/Terrorism Convictions
0.2 Number of TF/Terrorism Prosecutions
0.2 Number of TF/Terrorism Investigations
0.2 Number of TF/Terrorism Intelligence
0.2 Number of TF/Terrorism STRs
1.0 Number of TF/Terrorism Allegations in credible
Faith Based Organisations (FBOs)
1.0 Diversion of funds
0.2 Affiliation with a terrorist entity
1.0 Abuse of programming
1.0 Support to recruitment efforts
1.0 False representation/Sham
0.84 TF Typologies
1.0 Collection of funds
1.0 Transfer of funds
1.0 Expenditure of funds
1.00 Proximity to active terrorist threat
0.89 Threat
0.97 Inherent vulnerability (per
0.89 Inherent risk
NPO Risk Assessment
0.98 NPO Profile
0.5 Size
1.0 Activity type
0.5 Offshore/complex control structure
1.0 Level of accountability
1.0 Level of verifiability of fundraising methods
1.0 Level of cash transfers, valuable in-
1.00 Operational features
1.0 Level of risk appetite
1.0 Complexity / length of operational chains
1.0 Reliance on transitory or informal workforce
1.0 Level of professionalism
0.66 Methods to transfer funds
1.0 Use of cash
0.2 Use of virtual currency
0.5 Use of informal money transfer
0.18 Mitigating measures
0.22 NPO measures
0.2 Quality of Governance
0.2 Quality of Financial management
0.5 Quality of Project management
0.0 Quality of staff vetting and oversight
0.2 Level of commitment to ethics and
0.2 Level of self-regulation (incl.
0.14 Government measures
0.2 Quality of outreach and education
0.2 Quality of NPO policies
0.2 Scope of registration of FATF NPOs
0.0 Availability and accessibility of
0.2 Avoiding disruption of NPO activities

# ANNEXURE H: ML/TF/PF VASP RISK ASSESSMENT OUTCOMES



# ANNEXURE I: CHAINANALYSIS API DATADUMP (wallet address screening outcomes)

**Layer 2 are addresses connected to Layer 1 addresses either by receiving funds from Layer 1 addresses or other means**

There are approx 43k layer 2 addresses

Only a small "subset" of layer 2 addresses were cross referenc against the Chainalysis Sanctioned listing due to API speed constraints

| LAYER_2_Address | LAYER_1_Link | Risk | Risk_Category | Risk_Name | Risk_Description | Risk_URL |
|---|---|---|---|---|---|---|
| 112gk6CVErZYixMtVXzQy6qG77nUdT3FJS | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 116EwAnwT4XWX7cdyFCbMrTKBvzRimci3M | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 122ER3S1zib9uF8EuAF3wCe6XSjBuAS3Xn | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 122XAWCfALACuQRfgGGgqcMdH1Sti1Rgeb | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 123inZrPLE8ajJc3cszaGEt8xQeYQuxSju | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 123qC1TwiENsswkKDmHVXLNz6EnvNRWytd | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 123tWkiLdgrkQXDx1C9mk45JLW959EdP4o | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 1289KctQsEdaCxqW7LKzf5g9oJK355ronL | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 128RX6AZxLRSqbf3encn2yyB6p6hDV6TyV | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 128SVERWagtio9gXcqZaKK3qYZ7GCryKU4 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12ASSBC7rSJLh7BrmTYdukke3r9eqeeCFL | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12AVYVVAmjyv8uf6hnh6ArA2HHkbMa6yDD | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12Ah5SqwN1m11sEhqvkxC11saYAdTbEznR | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12HHHoExucx18SQaFsDXteGGgjAiZLrHLL | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12HXmGddgS35MqK5H9tKhMdMe2kKcEZ2Hd | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12N7jJwjwDtYhAS8uKmjqsTRFLvNs5xEcc | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12QW19xzjcFVCnqJ1pfE7gB6Mq9SiMdFDW | bc1qaz0rqpl5cqeqpq6n2cakqvnrx37zefmyvvj3mg | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12RazbFJaDGV6ZVsYBAy8xnct1utFHV7ca | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12YPwoEfbLvWkeUZ6LHrUZcBw4Qn1RDz7C | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12a8tWHxHSUQrnP22z1QFb9KtpDCUNPo24 | bc1qq4h458snp879d9ep2p8pl0yc54363xpue33jww | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12byBRLce7emi1ZZkcykErqRpiVSQyCRKh | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12cuPS9u4ai9EJdQQyVBMrkosi358T1D8w | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12eBecuVkcN3MndzN9evKNPVYP9CfZE5L5 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12f4PsKWS4h2xFR2eJKL3G3bFbaG2Yp9pp | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12fACtmfkbKbydk3NSRUtWVLudv3MULY5v | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12fZGs3rrS74yPxGBsB3BwL54VcJ74ZKJR | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12gdWKFhp5JbFcztSite9gMgKthffrVYnq | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12grn8ff2jDpxEYXQ1QbGqNPfVzLTn8Gcu | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12hss6tdRFyS2uycWyik6dEw5SAj2uWCSM | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12ib4xE3M4AtvFKxRaoBzfp1YDeQuf3goT | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12jgXRDFPpRYgFRziCBC31rTccoR9nSNbu | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12ktRzyjufDiuz9yQg6j4AvFBkXQdhEPv9 | bc1qgvjurukcqfyp3ak2m7cv5j9vanlez8jdpv037d | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12mCsi4cDJS33WLSrxLJJQ88ZxsHHqRWhB | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12naWvM8SR3sqng6S6B6jzjzwSJC9Kcy5k | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12njR245tnjh38tbUaeoJBRFJiSeASVRVF | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12nudGq7tF69WKDtyd4FG4AWd16vmMkHvt | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12p6YJPvtNAc26CJitNTwPefjSL7GeU4HU | bc1qq4h458snp879d9ep2p8pl0yc54363xpue33jww | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12qMFH21HZG7cDDuQP22DX8Ur81P8ZqD4t | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12rrL7SGV6LcxN5t4KuU4n9UdsgQp5ViPn | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12sf96xj4ySfTa9jdmV6RX8sgWafeU54j9 | bc1qxgmqqvkzc4nwxc2wah0rd48dwxedme0t9ylva9 | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12sqhkFgweeYzUdU5fFE2r3WeyGpCZXvah | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12tmtVCvMcpC4tUSyfJo9CipsArUpxGwYq | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12vNCHz2vKXvvTRqFkLJwjSzVwWQRpx489 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12vmudUc58RHKhnqLeL4y33gQE3DzcYvad | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12xhq8t6g1eRDpJb7GZt7hLzCPv69MKY6a | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12ypmdA74g8K83diKHLL6jG27usykcxdhC | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 12zq2ziYPkAL7FfGJNQzs8cCA32597wJG7 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 1317bg3PAXNP3cLEtC45TqfNz9oYqLrnG1 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 133jJon18ZF1uKjhVzDns7AZatzcepdT31 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 1351HDm3pViQmziXERSegQCTxC3xBKGW4P | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 136CXT3GZrE4KD7Jffwtr7Lr24kmTjzVpe | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 138gj73KwMCLztc5cw6XNmb8qCmHRuBQki | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 13BDABvq3dcTuT1DcN15wxW2p13Etgr3mz | 193DHDtGiidLukNkoc8g7Eqh1aKrWMrf9N | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 13CoZaPnHjXtrrECb15M2kJDxfAWAw2q9x | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 13EvMNf7QRvoHsM3RJtp3ituGmVFj546D8 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |
| 13GayCSfeor3WaVd6TXDMccUtn72v47d55 | bc1qkm0plrnjnfsfspkp92n0jq5swpvym45ck6r3mv | Low Risk | Not Sanctioned | N/A | N/A | N/A |

## ANNEXURE J: Data on ties to high risk jurisdictions

| High Risk Jurisdiction: FATF BLACK LIST | No. of banking clients | | | ADLA Remittances | Travellers from such Jurisdiction to Namibia | | | Travellers from Namibia to such Jurisdictions | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Natural Persons | Legal Persons | Trust | | 2020 | 2021 | 2022 | 2020 | 2021 | 2022 |
| Democratic People's Republic of Korea (DPRK) | 3 | 0 | 0 | 0 | 0 | 2 | 3 | 0 | 2 | 6 |
| People's Republic of Iran | 4 | 0 | 0 | 0 | 8 | 15 | 37 | 8 | 15 | 41 |

| High Risk Jurisdiction: FATF GREY LIST | No. of banking clients | | | ADLA Remittances | Travellers from such Jurisdiction to Namibia | | | Travellers from Namibia to such Jurisdictions | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Natural Persons | Legal Persons | Trust | | 2020 | 2021 | 2022 | 2020 | 2021 | 2022 |
| Albania | 3 | 0 | 0 | 1 | 2 | 2 | 9 | 1 | 1 | 11 |
| Barbados | 1 | 0 | 0 | 2 | 0 | 10 | 4 | 1 | 10 | 4 |
| Burkina Faso | 0 | 0 | 0 | 17 | 9 | 15 | 22 | 7 | 16 | 21 |
| Cayman Islands | 83 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Democratic Republic of Congo | 442 | 0 | 0 | 2530 | 274 | 600 | 1122 | 286 | 644 | 1045 |
| Gibraltar | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Jamaica | 3 | 0 | 0 | 16 | 18 | 23 | 36 | 15 | 25 | 37 |
| Jordan | 2 | 0 | 0 | 4 | 11 | 10 | 24 | 0 | 10 | 23 |
| Mali | 10 | 0 | 0 | 61 | 59 | 13 | 43 | 60 | 13 | 45 |
| Mozambique | 63 | 0 | 0 | 232 | 306 | 402 | 923 | 305 | 380 | 865 |
| Panama | 2 | 0 | 0 | 8 | 1 | 5 | 14 | 1 | 5 | 12 |
| Philippines | 68 | 0 | 0 | 449 | 555 | 1018 | 1237 | 560 | 906 | 1221 |
| Senegal | 3 | 0 | 0 | 101 | 56 | 112 | 116 | 56 | 110 | 106 |
| South Africa | 11915 | 336 | 38 | 50 | 59,339 | 104,139 | 164,700 | 57,610 | 96,300 | 154,774 |
| South Sudan | 7 | 1 | 0 | 3 | 12 | 25 | 37 | 13 | 22 | 34 |
| Türkiye | 13 | 0 | 0 | 316 | 88 | 179 | 246 | 72 | 173 | 239 |
| United Arab Emirates | 11 | 2 | 0 | 280 | 6 | 24 | 36 | 3 | 23 | 36 |
| Uganda | 174 | 0 | 0 | 1181 | 291 | 303 | 600 | 272 | 306 | 599 |
| The below jurisdictions chose to defer[1] FATF progress reporting from June 2023: | | | | | | | | | | |
| Haiti | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Nigeria | 448 | 6 | 0 | 488 | 348 | 1081 | 1405 | 293 | 884 | 1457 |
| Syria | 19 | 1 | 0 | 0 | 7 | 11 | 36 | 6 | 16 | 35 |
| Tanzania | 250 | 0 | 0 | 1456 | 345 | 520 | 1118 | 311 | 515 | 1001 |
| Yemen | 0 | 0 | 0 | 2 | 5 | 4 | 5 | 0 | 6 | 4 |
| FATF Further identified the following jurisdictions post reporting: | | | | | | | | | | |
| Cameroon | 85 | 1 | 0 | 434 | 94 | 208 | 269 | 73 | 161 | 275 |
| Croatia | 6 | 0 | 0 | 1 | 109 | 142 | 254 | 122 | 136 | 234 |
| Vietnam | 6 | 0 | 0 | 18 | 39 | 16 | 86 | 30 | 16 | 74 |

| High Risk Jurisdiction: Global Terrorism Index | No. of banking clients | | | ADLA Remittances | Travellers from such Jurisdiction to Namibia | | | Travellers from Namibia to such Jurisdictions | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Natural Persons | Legal Persons | Trust | | 2020 | 2021 | 2022 | 2020 | 2021 | 2022 |
| Niger | 11 | 0 | 0 | 8 | 11 | 9 | 46 | 11 | 9 | 45 |
| Afghanistan | 0 | 0 | 0 | 0 | 2 | 7 | 14 | 1 | 7 | 5 |
| Iraq | 1 | 0 | 0 | 0 | 0 | 2 | 1 | 0 | 2 | 1 |
| Somalia | 5 | 0 | 0 | 0 | 28 | 47 | 75 | 50 | 50 | 73 |
| Pakistan | 196 | 1 | 0 | 206 | 106 | 215 | 288 | 114 | 195 | 271 |
| Ethiopia | 66 | 0 | 0 | 38 | 86 | 269 | 393 | 60 | 148 | 361 |
| Kenya | 337 | 0 | 0 | 634 | 516 | 698 | 1641 | 499 | 697 | 1568 |

| High Risk Jurisdiction: As per Banks' Internal Risk Assessments | No. of banking clients | | |
|---|---|---|---|
| | Natural Persons | Legal Persons | Trust |
| Angola | 591 | 0 | 0 |
| Balarus | 1 | 0 | 0 |
| Benin | 1 | 0 | 0 |
| Bosnia and Herzegovina | 4 | 0 | 0 |
| Botswana | 14 | 0 | 0 |
| Burundi | 10 | 0 | 0 |
| Cambodia | 2 | 0 | 0 |
| Central African Republic | 2 | 0 | 0 |
| China | 94 | 1 | 0 |
| Congo | 21 | 0 | 0 |
| Cuba | 21 | 0 | 0 |
| Egypt | 0 | 0 | 0 |
| Eritrea | 3 | 0 | 0 |
| Eswatini (The Kingdom Of) | 1 | 1 | 0 |
| Germany | 1 | 0 | 0 |
| Ghana | 8 | 0 | 0 |
| Guinea - Bissau | 0 | 0 | 0 |
| Labanon | 3 | 0 | 0 |
| Liberia | 2 | 0 | 0 |
| Libya | 40 | 0 | 0 |
| Madagascar | 1 | 0 | 0 |
| Maritius | 4 | 3 | 0 |
| Morocco | 15 | 1 | 0 |
| Myanmar/Burma | 0 | 0 | 0 |
| Portugal | 1 | 0 | 0 |
| Russian Federation | 36 | 0 | 0 |
| Serbia | 1 | 0 | 0 |
| Sierra Leone | 2 | 0 | 0 |
| South Africa | 8 | 0 | 0 |
| Sudan (North) | 2 | 0 | 0 |
| Thailand | 1 | 0 | 0 |
| Tunisia | 0 | 0 | 0 |
| Ukraine | 16 | 0 | 0 |
| Venezueela | 4 | 0 | 0 |
| Republic of Bolivia | 1 | 0 | 0 |
| Venezuela | 1 | 0 | 0 |
| Zambia | 66 | 0 | 0 |
| Zimbabwe | 3091 | 1 | 0 |

## ANNEXURE K: NAMPOL statistics[60] on ML & other commercial crimes

| Period | CCs | Companies | Trusts | Natural Persons | Namibian Nationa | Foreign National | Amount (NAD) |
|---|---|---|---|---|---|---|---|
| Sep-21 | 1 | 1 | 0 | 1 | 0 | 1 | 436,500.00 |
| | 0 | 0 | 0 | 4 | 4 | 0 | 241,261.36 |
| | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 46500 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 62,828.00 |
| **Total** | **1** | **1** | **0** | **10** | **8** | **2** | **787,089.36** |
| | | | | | | | |
| Oct-21 | 0 | 0 | 0 | 1 | 1 | 0 | 240,000.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 7,187,723.90 |
| | | | | 4 | 4 | 0 | 490,925.65 |
| **Total** | **0** | **0** | **0** | **6** | **5** | **0** | **7,918,649.55** |
| | | | | | | | |
| Nov-21 | 0 | 0 | 0 | 1 | 1 | 0 | 2,000,000.00 |
| **Total** | 0 | 0 | 0 | 1 | 1 | 0 | 2,000,000.00 |
| | | | | | | | |
| Dec-21 | 1 | 0 | 0 | 1 | 0 | 1 | 67,000,000.00 |
| | 0 | 0 | 0 | 7 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 4,338,145.00 |
| **Total** | **1** | **0** | **0** | **9** | **1** | **1** | **71,338,145.00** |
| | | | | | | | |
| Jan-22 | 0 | 0 | 0 | 5 | 5 | 0 | 162,000.00 |
| Total | 0 | 0 | 0 | 5 | 5 | 0 | 162,000.00 |
| | | | | | | | |
| Feb-22 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 169500 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 620000 |
| | | | | | | | |
| Mar-22 | 1 | 0 | 0 | 1 | 0 | 0 | 20,600.00 |
| | 1 | 0 | 0 | 1 | 1 | 0 | 17,000,000.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | - |
| | 0 | 0 | 0 | 1 | 0 | 0 | 896,589.98 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 102,783.97 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 284,550.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 135,058.00 |
| **Total** | **2** | **0** | **0** | **7** | **3** | **0** | **18,439,581.95** |
| | | | | | | | |
| Apr-22 | 0 | 0 | 0 | 1 | 0 | 0 | 5,400.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 215,000.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | - |
| | 0 | 0 | 0 | 1 | 0 | 0 | 18,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | - |
| | 0 | 0 | 0 | 1 | 1 | 0 | 13,346.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 1,378,984.03 |
| **Total** | **0** | **0** | **0** | **7** | **2** | **0** | **19,612,730.03** |

[60] The Companies cited herein are Private Companies. No record of Public Companies to date. Trusts referred to herein are inter vivos trusts only. Note however that record keeping to this detail was recently commenced and this may change over time.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| May-22 | 0 | 0 | 0 | 1 | 1 | 0 | 100,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 1 | 277,000.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 19,650.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 11,000.00 |
| **Total** | **0** | **0** | **0** | **4** | **2** | **1** | **407,650.00** |
| | | | | | | | |
| | | | | | | | |
| Jun-22 | 0 | 0 | 0 | 1 | 0 | 0 | 103642 |
| | 0 | 0 | 0 | 2 | 2 | | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 359953.7 |
| | 0 | 1 | 0 | 1 | 1 | 0 | 150,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 100000 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 269993.63 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 306000 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 2,000,000.00 |
| **Total** | **0** | **1** | **0** | **10** | **8** | **0** | **153,139,589.33** |
| | | | | | | | |
| | | | | | | | |
| Jul-22 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 2,074,140.50 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 144,884.63 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 399,090.38 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 122,765.42 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 70,037.14 |
| | 1 | 0 | 0 | 0 | 0 | 0 | 1,178,119.00 |
| | 1 | 0 | 0 | 0 | 0 | 0 | 570,690.83 |
| | 1 | 0 | 0 | 0 | 0 | 0 | 7,276,855.94 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 144,884.63 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 399,090.38 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 3,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 180,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 92,519.19 |
| **Total** | **4** | **0** | **0** | **12** | **9** | **0** | **195,473,078.04** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Aug-22 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 2,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 1,011,896.61 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 263,564.35 |
| | 0 | 0 | 0 | 11 | 11 | 0 | - |
| | 0 | 0 | 0 | 1 | 0 | 0 | 21,720.90 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 36,819.09 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 143,347.50 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 77,931.56 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 77,439.22 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 72,136.32 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 178,761.19 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 216,144.18 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 35,094.61 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 23,655.94 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 36,715.70 |
| **Total** | **0** | **0** | **0** | **29** | **24** | **0** | **4,195,227.17** |
| | | | | | | | |
| **Sep-22** | 0 | 0 | 0 | 4 | 4 | 0 | 0 |
| | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| | 0 | | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 4 | 4 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 1,055,813.21 |
| | 1 | 0 | 0 | 0 | 0 | 0 | - |
| | 0 | 0 | 0 | 1 | 1 | 0 | 109,737.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 9,000,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 246,776.56 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 39,771.90 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 89,020.74 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 15,660.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 133,146.98 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 73,904.65 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 36,388.65 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 31,700.00 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 100,678.80 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 158,896.62 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 80,760.43 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 100,540.64 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 89,512.54 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 76,136.21 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 30,970.48 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 50,228.66 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 96,601.44 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 66,091.67 |
| **Total** | **1** | **0** | **0** | **32** | **19** | **0** | **11,682,337.18** |
| | | | | | | | |
| Oct-22 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 5 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 6 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 157,790.81 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 73,904.68 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 246,776.56 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 155,898.05 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 15,660.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 101,823.80 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 97,876.97 |
| | 0 | 0 | 0 | 0 | 0 | 0 | 97,535.49 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 32,151.12 |
| | **0** | 0 | 0 | 1 | 1 | 0 | 152,578.97 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 83,833.50 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 102,547.12 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 77,611,796.65 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 58,261.18 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 117,139.94 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 7,000,000.00 |
| | 0 | 0 | 0 | 4 | 0 | 0 | 100,000.00 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 7,187,723.90 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 32,055.90 |
| **Total** | **0** | **0** | **0** | **35** | **15** | **0** | **93,425,354.64** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nov-22** | 0 | 0 | 0 | 11 | 11 | 0 | 0 |
| | 2 | 0 | 0 | 0 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 2,700,000.00 |
| **Total** | **2** | **0** | **0** | **12** | **12** | **0** | **2,700,000.00** |
| | | | | | | | |
| | | | | | | | |
| **Dec-22** | 1 | 0 | 0 | 2 | 2 | 0 | 25,303,268.00 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 4,338,145.00 |
| | 0 | 0 | 0 | 2 | 2 | 0 | 121,573.38 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 25,254.10 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 70,762.47 |
| **Total** | **1** | **0** | **0** | **8** | **7** | **0** | **29,859,002.95** |
| | | | | | | | |
| | | | | | | | |
| **Jan-23** | 1 | 0 | 0 | 2 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| **Total** | **1** | **0** | **0** | **3** | | | **0** |
| | | | | | | | |
| | | | | | | | |
| **Feb-23** | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | 0 | 1 | 0 | 0 | 2,713,000.00 |
| | 0 | 0 | 0 | 4 | 0 | 0 | - |
| **Total** | **0** | **0** | **0** | **6** | **0** | **0** | **2,713,000.00** |
| | | | | | | | |
| | | | | | | | |
| **Mar-23** | 0 | 0 | 0 | 1 | 1 | 0 | 8,670,581.60 |
| | 0 | 0 | 0 | 1 | 1 | 0 | 572,175.50 |
| | 0 | 0 | 0 | 1 | 0 | 1 | 3,826.00 |
| **Total** | **0** | **0** | **0** | **3** | **2** | **1** | **9,246,583.10** |
| | | | | | | | |
| **Apr-23** | 0 | 0 | 0 | 1 | 0 | 0 | 9,797,720.91 |
| | | | | | | | |
| **Total** | **26** | **4** | **0** | **402** | **246** | **10** | **9,797,720.91** |

## ANNEXURE L: Anti-Corruption Commission (ACC) ML statistics

| No. | Date IRD Received from FIC | ACC Case number allocated or detail if no case was opened (No case opened) | Details of Predicate offence being investigated | Short summary of the case/incident | Value of proceeds of crime | Particulars of the suspect(s) 1.Natural Person 2.Legal Person 3. Sector of Legal person | Status/Results of the investigation in detail: 1.Predicate offence; 2.Corruption/ML investigations; 3.Asset Recovery |
|---|---|---|---|---|---|---|---|
| 1 | 09/10/2021 | ACC-X | Fraud | Alleged that the former manager of XXX collected debts meant for a local academic institution for his own personal benefits by providing his personal account detail as that of the academic institution. | 585,869.47 | X1 Natural Person | Transferred to Nampol |
| 2 | 20/10/2021 | ACC-XX | Illegal financial Scheme | It is alleged that the subject could have been a partner to the owner of an entity as significant funds were transferred into the account. | 310,000.00 | X1 Natural Person | Matter closed as it was found out that the funds were indeed the subjects funds and had no relations to the owner of project 1 million. |
| 3 | 13/01/2023 | ACC-XXX | Corruption | Allegations are that, there were loans and contracts submitted to a lending institution and 80% of the companies awarded contracts are related to employees of the lending institution; and other contracts are non-existing contracts | 600,000.00 | X4 Natural persons and X1 CC | Ongoing investigation |
| 4 | 16/03/2023 | ACC-XXC | Corruption | Allegation that someone employed by tax authority created suspicious certificate of good standing on behalf of a CC. | 5,599,000.00 | X1 Natural Person and X1 CC | With PG for decision |
| 5 | 14/09/2023 | ACC-XXX | Fraud | It is alleged that three (3) former employees of the National Assembly (NA) stole funds from their employer | 1,205,710.83 | X4 Natural persons | |