

**MARCH 2026**



# TERRORIST FINANCING IN HIGH-RISK NON-PROFIT ORGANIZATIONS



+264 61 285 0054



helpdesk@fic.na



<https://www.fic.na>



114 Nickel Street Prosperita

**TABLE OF CONTENTS**

- 1. ACRONYMS AND DEFINITIONS..... 4
- 2. EXECUTIVE SUMMARY ..... 6
- 3. INTRODUCTION..... 8
- 4. OBJECTIVES OF THIS REPORT ..... 8
- 5. METHODOLOGY ..... 9
- 6. UNDERSTANDING NPOs..... 9
- 7. SUMMARY OF STRs AND SARs RELATED TO TF ACTIVITIES REPORTED TO FIC ..... 11
  - Chart 1: Summary of STRs received per Sectors..... 11
  - Chart 2: Classification of STRs received per Sectors ..... 13
  - Chart 3: Summary of potential TF STRs received per Entity ..... 14
  - Chart 4: Classification of potential TF STRs received per annum ..... 17
- 8. HIGH-RISK NPOS IN THE CONTEXT OF ML AND TF ..... 18
  - 8.1 High-level summary of what an NPOs ought to have (FATF and Namibia FIC view)..... 19
  - 8.2 The following NPOs financial bank statement has been analysed..... 21
  - 8.3 NPOs risk of terrorist abuse to include indoctrination / radicalization ..... 22
  - 8.4 NPOs reported to the FIC ..... 23
- 9. POTENTIAL INDICATORS OF TF IN NPOs AND OTHER SECTORS..... 29
- 10. KEY FINDINGS..... 32
- 11. POSSIBLE RECOMMENDATIONS..... 34
- 12. CONCLUSION ..... 34

## 1. ACRONYMS AND DEFINITIONS

Accountable Institution (AI)	Means a person or entity listed in schedule 1 and 3 of the Act. The term “accountable and reporting institutions” in this document refers to all Authorised Dealers and Authorised Dealers with Limited Authority.
Act	Financial Intelligence Act, 2012 (Act No. 13 of 2012) as amended.
Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation framework (AML/CFT/CPF)	Refers to the national (or international) framework which combats and prevents money laundering, terrorism and proliferation financing activities.
Customer due diligence	Means a process which involves establishing the identity of a client and monitoring all transactions of the client against the client’s profile.
FIA	The Financial Intelligence Act, 2012 (Act No. 13 of 2012), as amended (also referred to as the Act).
Customer due diligence	Means a process which involves establishing the identity of a client and monitoring all transactions of the client against the client’s profile.
FIC	Means the Financial Intelligence Centre. It is sometimes referred to as the FIC.
PF	Refers to Proliferation Financing. “the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations”.
ML	Money laundering (ML)” Generally, refers to the act of disguising the true source of proceeds generated from unlawful activities and presenting such in the financial system as sourced from legitimate activities. However, in terms of the Prevention of Organized Crime Act, 2004, as amended (POCA), the definition of ML is broad enough to include engagement, acquisition and concealment of proceeds of crime whether directly or indirectly.

SAR	Refers to a suspicious activity report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.
STR	Refers to a suspicious transaction report submitted to the FIC in terms of sections 33 (1) & (2) of the Act.
TF	“Terrorist financing (TF)” includes “acts which are aimed at directly or indirectly providing or collecting funds with the intention that such funds should be used, or with the knowledge that such funds are to be used, in full or in part, to carry out any act of terrorism as defined in the Organization for African Unity (OAU) Convention on the Prevention and Combating of Terrorism of 1999, irrespective of whether or not the funds are actually used for such purpose or to carry out such acts.”
	“Terrorism” Whilst no acceptable international definition on terrorism exists, it is generally described as the execution of acts of violence against persons or property, or a threat to use such violence, with the intent to intimidate or coerce a Government, the public, or any section of the public to achieve or promote any tribal, ethnic, racial, political, religious or ideological objectives .
Vulnerabilities	When used in a risk assessment, this term comprises of those weaknesses that can be exploited by the threat or that may support or facilitate its activities.
Threat	An activity, person or group of people, object with the potential to cause harm. Threat is contingent on actors that possess both the capability and the intent to do harm.

## 2. EXECUTIVE SUMMARY

The Non-Profit Organisation (NPO) sector is vital in delivering humanitarian and social services but remains vulnerable to terrorist financing (TF) abuse due to its public trust, funding access, and cross-border operations. In Namibia, the Financial Intelligence Centre (FIC) and the 2023 National Risk Assessment (NRA) identified Faith-Based Organisations (FBOs) and charitable entities as the most exposed to TF risks.

Primary risk factors include cross-border financial flows, links to extremist ideologies, and transactions with high-risk jurisdictions. While most Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) filed mostly by banks were later deemed false positives, they have enhanced national understanding of TF typologies and improved detection mechanisms. Key TF red flags for NPOs include:

- Large or unusual “donation” deposits from high-risk jurisdictions.
- International transfers from unverifiable sources.
- Cross-border withdrawals are inconsistent with NPO objectives.
- Weak governance and limited financial oversight.

Although confirmed TF incidents in Namibia are minimal, ongoing vigilance is essential. The sector’s exposure stems from inadequate donor verification, weak internal controls, and activities in high-risk regions.

Key Recommendations:

1. Strengthen regulation, coordination, and oversight among relevant authorities.
2. Enhance financial transparency through recordkeeping, audits, and official banking.
3. Improve governance and compliance within NPOs.
4. Apply due diligence to donors, partners, and beneficiaries.
5. Monitor ideological risks and promote counter-radicalization awareness.
6. Build NPO capacity through AML/CFT training and guidance.
7. Ensure timely reporting and proportionate enforcement.

8. Foster international cooperation and information sharing.

A coordinated, transparent, and risk-based approach is crucial to protect NPOs from terrorist misuse while ensuring they continue their vital humanitarian role.

### **3. INTRODUCTION**

The importance of the NPO sector to the global community cannot be overstated. It is an important sector, providing various services, including vulnerable members of society. In essence, terrorist organisations and NPOs have different objectives, but often rely on similar logistical capabilities to carry out their objectives. In this regard, funds, material, personnel and public influence are key resources for NPOs. Equally, terrorist organisations seek the same resources to further their cause, which makes NPOs vulnerable for abuse by terrorists or terrorist networks.

In the case of Namibia, it has previously been found that services offered by NPOs were abused for ML domestically. This is reflected through cases in the 2015-2023 NPO NRA update. In contrast, the greater concern, however, is combatting the abuse of NPOs to advance TF activities. In this regard, the FIA Amendments are tailored to specifically enhance TF risk management within the NPO sector. The 2020 NRA found religious and faith-based organisations highly exposed to risks of TF while the 2023 NRA update has additionally identified the broader category of service charities as equally vulnerable to TF abuse. Therefore, these findings brought about specific NPOs to which the FIA applies are religious or faith-based organisations and those involved in charitable activities. The importance of the NPO sector to the global community cannot be overstated. For this reason, a risk-based approach is adopted at institutional and supervisory level to restrict both institutional and supervisory expectations to only those areas and operations highly exposed to risks.

### **4. OBJECTIVES OF THIS REPORT**

The primary objective of this report is to assess and better understand the TF risks and vulnerabilities within the NPO sector in Namibia, with a specific focus on changes observed following the 2023 NRA update. The report seeks to provide an evidence-based overview that will guide policy, supervision, and mitigation measures aimed at safeguarding the NPO sector from potential terrorist abuse. Specifically, the report aims to address the following key questions:

#### **1. Who**

- 🚩 Which categories or types of NPOs are most at risk of being abused by terrorist entities?

#### **2. What**

- ✚ What is the nature and form of the threat that terrorist entities pose to the NPO sector?

### **3. When**

- ✚ At what points or stages in their operations are NPOs most vulnerable to potential abuse by terrorist entities (e.g., fundraising, transfers, or programme implementation)?

### **4. Why**

- ✚ Why are NPOs particularly attractive targets for terrorist entities (e.g., due to public trust, cross-border work, or access to funding channels)?

### **5. How**

- ✚ How are NPOs vulnerable to terrorist activities including weaknesses in governance, transparency, or financial controls?
- ✚ How do terrorist entities abuse or exploit the NPO sector to raise, move, or use funds?
- ✚ How have cases of suspected abuse been identified, investigated, and disrupted domestically through the efforts of the FIC and law enforcement agencies?

## **5. METHODOLOGY**

The FIC analysed relevant data, and various reports at its disposal in an effort to understand potential methodologies, trends, typologies, and other related red flags associated with NPOs which potentially leads to TF activities. The information contained in this report was derived from STRs/SARs data filed with the FIC by various reporting institutions.

Specifically, the sources of data and information analysed primarily include:

- i. Sanitised intelligence emanating from reports and closed databases;
- ii. Competent Authorities' investigation outcomes; and
- iii. Open-source research.

Such data was analysed and the information from such is summarized herein.

## **6. UNDERSTANDING NPOs**

According to the FATF, NPO refers to a legal person or arrangement or an organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of 'good works'<sup>1</sup>.

---

<sup>1</sup>FATF Report: Terrorist Financing Risk Assessment Guidance

It has been anticipated that the NPOs at the highest risk of TF abuse internationally are charities. This is because charities are cash intensive, most operate with reduced governance structures, regularly transmit funds between jurisdictions and have historically operated under less formal regulatory scrutiny than formal profit entities. Such is therefore seen as an ideal vehicle in which to launder money or collect and transmit funds to finance terrorism activities.

It is important to note that not all NPOs are vulnerable to TF and care should be taken to duly supervise the sector without undermining legitimate NPO operations. FATF Recommendation 8 requires countries to assess TF risks facing NPOs and use outcomes of such an assessment to construct or implement risk based preventative measures. Importantly, it requires jurisdictions to undertake a domestic review of their NPO sector or have the capacity to obtain timely information on its activities, size and other relevant features. Such is required to identify the subset of NPOs that fall into the FATF definition. In doing so, jurisdictions are required to use all available sources of information to identify features and types of NPOs that, by virtue of their activities or characteristics, are at risk of being misused for TF<sup>2</sup>. Owing to NPOs receiving significant funds from international stakeholders (cross-border funds remittances), NPOs are inherently vulnerable to advancing TF or being abused for ML purposes. The reduced governance structures in most NPOs further make them attractive to PF abuse.

---

<sup>2</sup> FATF Report: Terrorist Financing Risk Assessment Guidance

## 7. SUMMARY OF STRs AND SARs RELATED TO TF ACTIVITIES REPORTED TO FIC

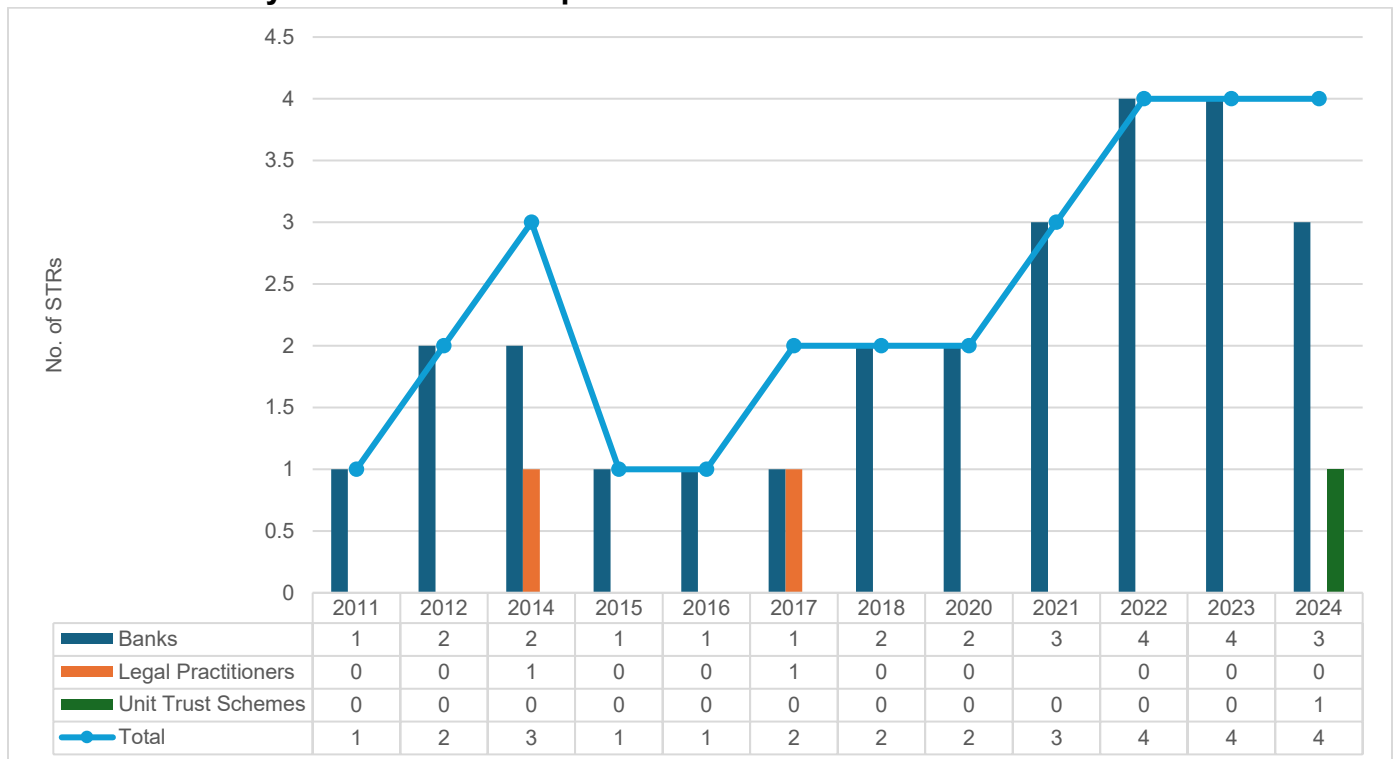
To effectively combat TF and related crimes, it is crucial for all relevant agencies and authorities to fully understand the risks, trends, and pressures associated with this type of criminal activity. Such understanding enables them to prevent and detect predicate offences and address any associated ML activities.

This section provides an overview of STRs, and SARs related to potential TF threats and risks that have been filed by various reporting institutions since the introduction of mandatory reporting in 2009 up to 31 December 2024.

Upon receipt, each report is assessed by the FIC to determine whether additional analysis or investigation is warranted. Reports that meet the criteria for further review are converted into active cases, allowing for deeper analysis and possible referral to LEAs for investigation.

The section also outlines the total number of STRs<sup>3</sup> that progressed into active TF-related cases, highlighting the trends and patterns observed within Namibia’s financial and non-profit sectors.

**Chart 1: Summary of STRs received per Sectors**



<sup>3</sup> Cases within FIC domain.

Chart 1 provides a summary of STRs submitted by the three reporting sectors that have filed reports involving NPOs. Analysis of these reports reveals that approximately 90% of all STRs originate from the banking sector. This trend can be attributed to several factors.

Firstly, the banking sector possesses the most advanced and mature Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of Proliferation (AML/CFT/CPF) compliance frameworks compared to other sectors. Banks generally have robust monitoring systems, trained compliance personnel, and automated transaction monitoring tools, which enhance their ability to detect and report suspicious activities.

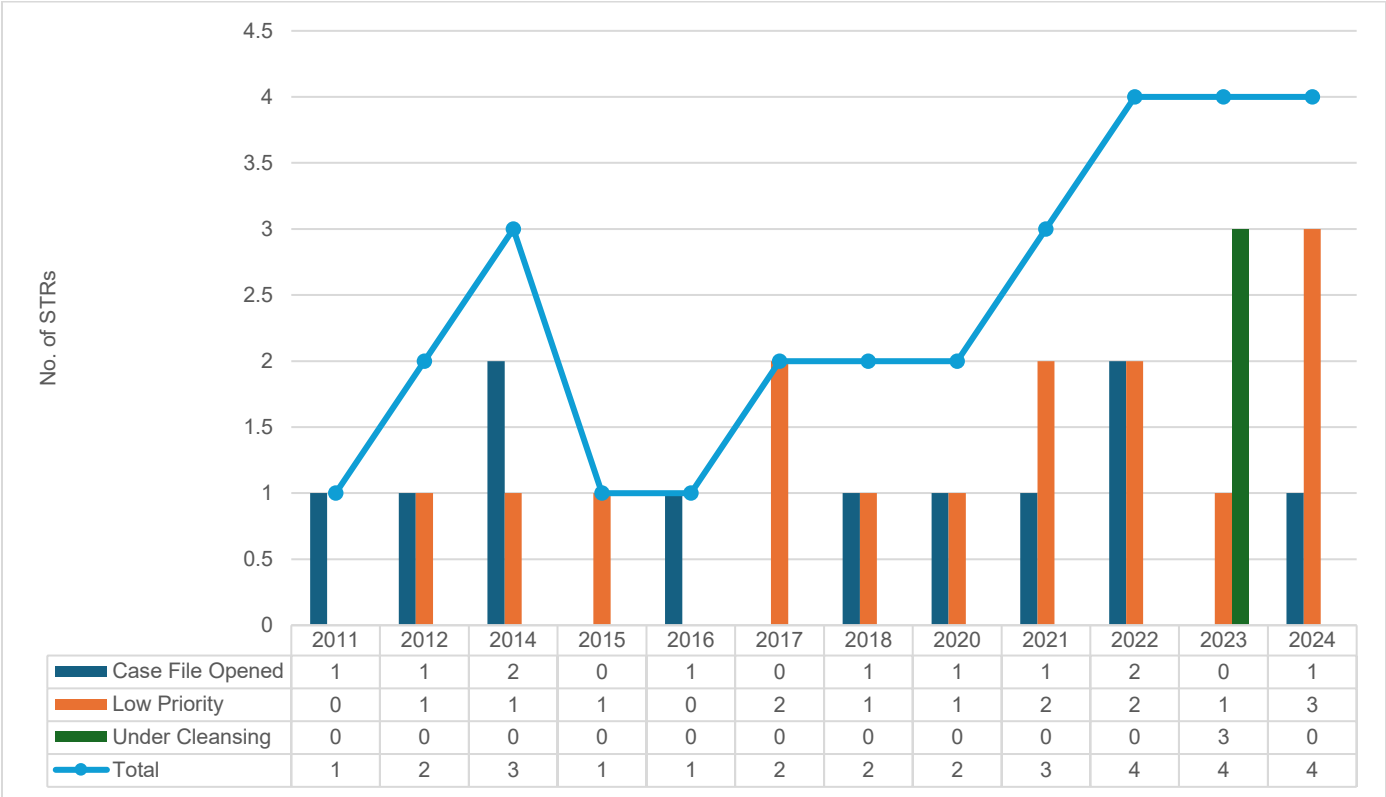
Secondly, the dominance of bank-originated STRs also reflects the fact that almost all financial and non-financial sectors rely on banking services to facilitate their transactions. This makes the banking system inherently more exposed to financial crime risks, including TF, since most illicit financial flows ultimately pass through formal financial channels.

According to the 2023 National Risk Assessment (NRA) update, the NPO sector, particularly Faith-Based Organisations (FBOs) and those engaged in charitable or humanitarian activities, remains highly exposed to terrorist financing risks. These entities are often targeted due to their cross-border operations, access to donor funding, and community influence, which can be exploited to raise or channel funds for illicit purposes. The FIC supports and reiterates the NRA findings, emphasizing that while various factors contribute to NPO risk exposure, the following three variables are the primary drivers of elevated TF risk among domestic NPOs:

1. Cross-border linkages, where NPOs operate, receive, or send funds to foreign jurisdictions, especially those with weak AML/CFT controls.
2. Potential associations with radical or extremist ideologies or organisations: where individuals or groups linked to an NPO may hold or promote beliefs aligned with extremist movements.
3. Financial transactions involving high-risk jurisdictions, including remittances to or from countries identified as posing elevated TF or ML risks by the Financial Action Task Force (FATF) or other international bodies.

Together, these risk variables significantly shape the TF risk profile of the Namibian NPO sector, underscoring the need for enhanced due diligence, targeted supervision, and stronger inter-agency collaboration to mitigate potential abuse.

**Chart 2: Classification of STRs received per Sectors**



Overall, analysis by the FIC revealed that out of the total STRs received involving NPOs, approximately 38% (11 reports) were classified as “high priority” and subsequently escalated for detailed analysis, leading to the opening of formal case files. In contrast, 52% (15 reports) were assessed as “low priority”, indicating limited immediate suspicion but still warranting monitoring.

A common reason in these reports was the presence of frequent cash deposits and international transfers into NPO bank accounts, particularly from high-risk or non-transparent jurisdictions. Such transactions often lacked clear economic or charitable justification and were inconsistent with the NPOs’ stated objectives or operational profiles. These patterns raised concerns about potential TF or ML activity.

Additionally, a notable number of cases involved funds misappropriation, where account signatories or individuals in management positions were suspected of diverting or misusing NPO funds for personal benefit or purposes unrelated to the organisation’s mandate. This reflects weaknesses in internal financial controls, governance structures, and accountability mechanisms within some NPOs.

The FIC’s findings also highlight that the vulnerability of NPOs is closely linked to the nature of their operations and structural characteristics. Many NPOs operate on a cash-intensive basis, often collecting or distributing funds in environments where formal financial systems are limited. Their social and humanitarian purpose can make them attractive vehicles for abuse, as they typically enjoy public trust and less scrutiny than for-profit entities.

Furthermore, there is a lack of a dedicated prudential regulatory authority in Namibia to oversee market entry, licensing, and operational compliance for certain categories of NPOs, especially Faith-Based Organisations (FBOs). This regulatory gap increases the risk that such entities could be established or exploited by individuals or groups with illicit or extremist motives. Strengthening registration, transparency, and ongoing oversight mechanisms for NPOs particularly those with cross-border operations remains a critical step in mitigating these risks.

**Chart 3: Summary of potential TF STRs received per Entity**

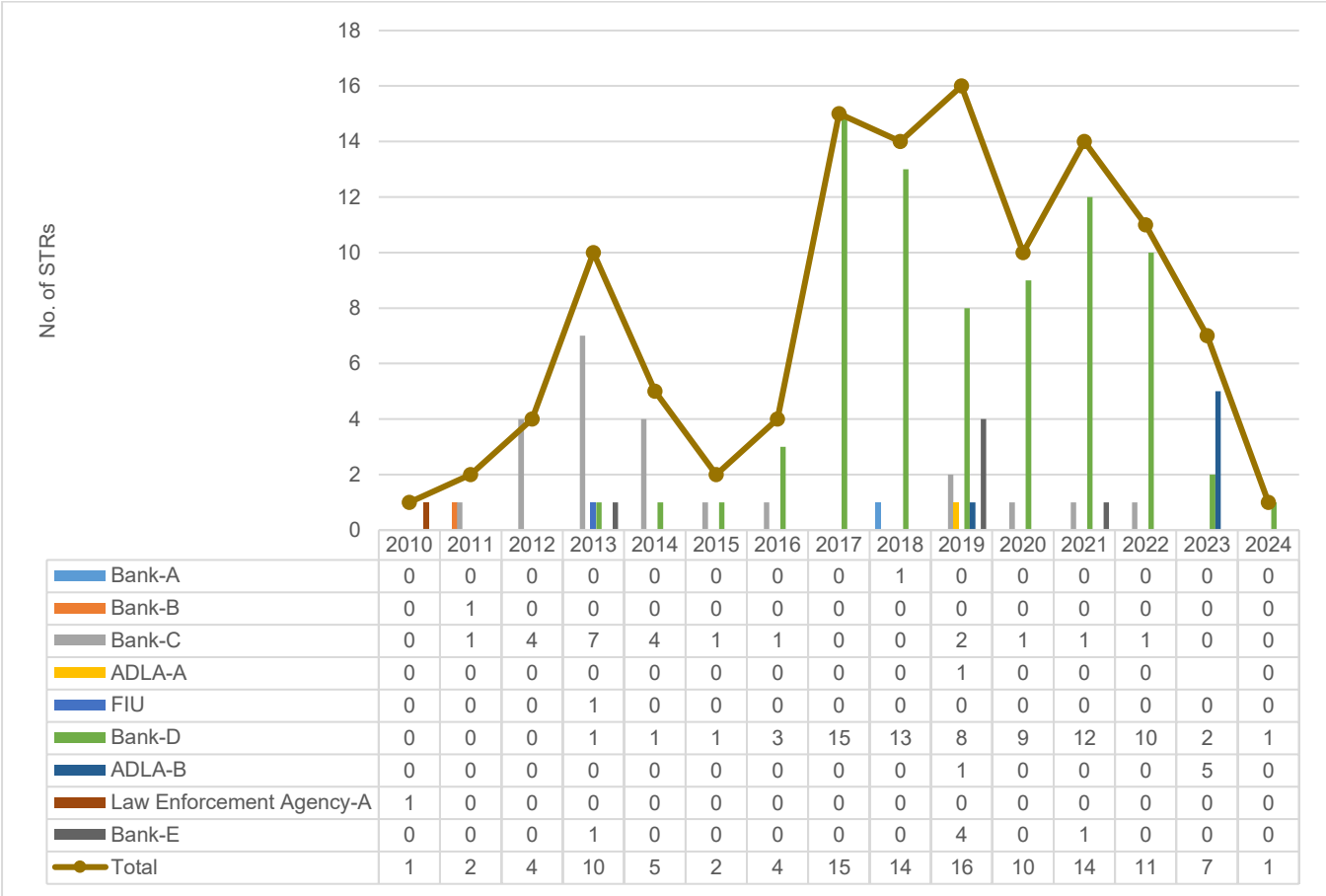


Chart 3 presents a summary of STRs filed by the entities related to potential TF. The year 2019 saw the highest volume of reports related to potential TF offences with 16 STRs. It is worth noting that 93% of the reports originate from the banking sector. Bank-D filed the highest volume

of reports related to potential TF offences with 76 STRs. The records show that the high number of reports received from Bank-D could be attributed to various factors, including the fact that they appear to be the largest financial institution in terms of volumes of clients. Equally, through such a larger client base, Bank-D's measures aimed at detecting and reporting suspicions can be said to be aligned to the bank's risk exposure. This is based on volumes of reports and bank size. It does not replace any observations in the relevant supervisory observations around compliance.

NPOs are particularly vulnerable to misuse of TF because of their legal status, public trust, and frequent engagement in cross-border activities. Information reported by reporting entities highlights the following patterns of concern:

### **Raising funds sources of increased risk for NPOs**

- ✚ Large and unusual cash deposits: NPO bank accounts have received significant cash deposits described as "donations." These deposits often originate from individuals in jurisdictions known for higher TF risks. Such deposits may not align with the NPO's stated objectives or normal fundraising patterns, creating a red flag for potential misuse.
- ✚ Inward international transfers from high-risk jurisdictions: Many NPO accounts are credited with funds via EFTs or inward SWIFT transfers from multiple individuals or entities abroad. When these senders are based in high-risk or conflict-affected regions, the probability of TF-related misuse increases, especially if the donors are not known or cannot be adequately verified.
- ✚ Unknown or unverified source of funds: In many cases, the source of funds is unclear or inconsistent with the NPO's profile and past activities. This lack of transparency and due diligence exposes NPOs to heightened TF risks because it undermines the ability to demonstrate that funds are from legitimate and non-criminal sources.

### **Movement of funds - patterns heightening TF vulnerability**

- ✚ Cross-border cash withdrawals: Funds received into NPO accounts are often disbursed through cross-border ATM cash withdrawals or foreign currency withdrawals. This makes the flow of funds harder to trace, increases anonymity, and creates an opportunity for funds to be diverted for TF purposes.

- ✚ International purchases and payments: NPOs have been observed making international purchases or payments inconsistent with their stated objectives or operational needs. Such patterns can mask the redirection of funds to finance terrorism under the guise of legitimate overseas operations or aid distribution.

### **Overall risk implications for NPOs**

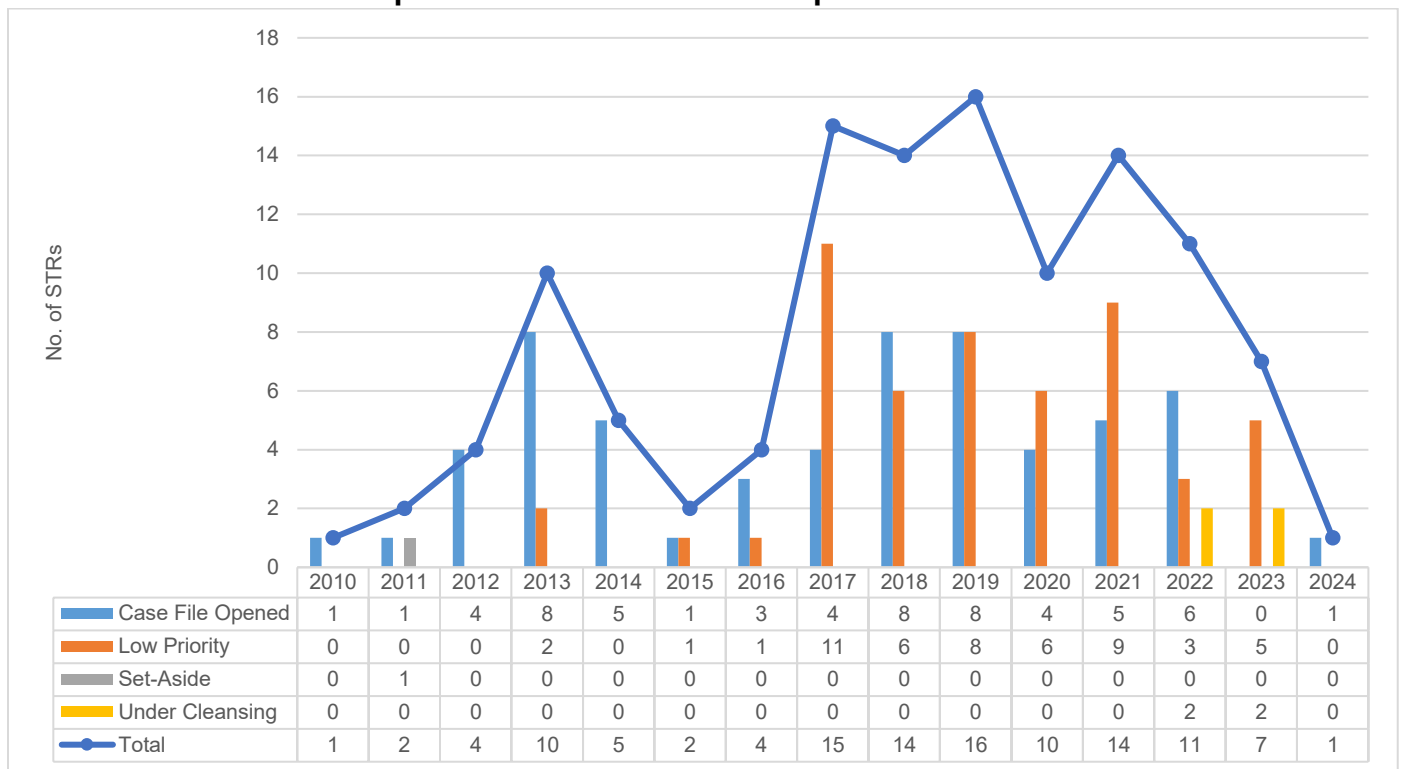
Because NPOs are built on public trust, they are attractive to bad actors who wish to exploit this trust to move and disguise funds for terrorist activities. The following factors magnify their TF exposure:

- ✚ Frequent cross-border transactions in high-risk regions.
- ✚ Reliance on donations from a wide pool of individuals or entities, often without full donor verification.
- ✚ Limited internal controls or monitoring of how funds are raised and disbursed, especially in smaller or informal NPOs.
- ✚ The potential mixing of legitimate charitable donations with illicit funds.

NPOs can face significant risks related to TF, potentially through donations received and the destination of funds. NPOs, especially those involved in charitable or religious activities, can be vulnerable to infiltration or misuse by terrorist groups for fundraising or logistical support, hence is it worth noting the above-mentioned sources and movement of fund within the NPOs.

As mentioned above, many such potential TF reports were deemed false positives within the FIC and not escalated to Law Enforcement Agencies (LEAs) for further investigation. However, those escalated to Namibian Police (NamPol), almost all were deemed false positives for terrorism or TF and not investigated any further.

**Chart 4: Classification of potential TF STRs received per annum**



Overall, as observed in chart-4, 51% of the reports received during the review period were classified as “high priority” and subsequently escalated for further analysis, resulting in the opening of case files. Meanwhile, 45% were categorized as “low priority” and were not pursued beyond initial review.

Among the high-priority cases, several involved foreign individuals or entities transferring funds to high-risk jurisdictions. These transactions were often considered potential indicators of TF and were therefore subjected to comprehensive analysis. In most instances, however, the only red flag identified was the transfer of funds to or from a high-risk jurisdiction, without the presence of additional TF indicators.

In numerous cases, the FIC’s analysis led to the generation of actionable intelligence, which was subsequently disseminated to LEAs for investigation. Nevertheless, after further investigation, the Namibia police (AML & CFT Division Crime Investigation Directorate) confirmed that most of these reports were false positives, meaning they were not linked to actual terrorism or TF activities. Only two cases were found to warrant continued investigation.








It is important to note that terrorism risk and TF risk, while often related, are not always identical. An assessment of TF risk requires consideration of both domestic and international terrorist

threats. Jurisdictions experiencing active terrorist activity within or near their borders generally face a higher likelihood of TF occurrences.

In addition, during the period under review, the FIC received only two SARs explicitly related to potential TF offenses. Both were filed in 2021 by Bank-C and were categorized as “low priority”, given the absence of sufficient indicators suggesting credible TF activity.

**8. HIGH-RISK NPOS IN THE CONTEXT OF ML AND TF**

This section presents a summary of analysis high risk NPOs as categorised by the FIC. The purpose is to assess vulnerabilities within such NPOs that may facilitate illicit activities, and to identify characteristics, operational practices and regulatory gaps that make such NPOs susceptible to abuse. Below are the names of NPOs that are categorized as high risk:

-  NPO-A
-  NPO-B
-  NPO-C
-  NPO-D
-  NPO-E
-  NPO-F
-  NPO-G

It is significant to indicate that although the above NPOs have been categorised as inherently high risk, not all of them have been reported to the FIC or other relevant LEAs for illicit activities. It is evident that combating terrorism financing requires a high degree of vigilance from a wide range of role players in government and, critically, the private sector, particularly banks, authorised dealers in foreign exchange, providers of a range of financial services (cross-border payments platforms, providers of remittance services, and crypto currency dealers). Moreover, it also requires the co-operation and oversight of NPOs that provide services in areas affected

by terrorism, and whose systems are at risk of being abused to facilitate the transfer of goods or financing in support of terrorist activities.

## **8.1 High-level summary of what an NPOs ought to have (FATF and Namibia FIC view)**

### **a. Governance and legal identity**

- ✚ Clear legal status and registration documents, Constitution/Articles, certificate of incorporation/registration. (FIC requires these on registration.)

### **b. Board and management structure**

- ✚ Board composition, roles (Chair, Treasurer), meeting schedule, minutes and delegation (who can authorize funds). (Expected by both FATF best practice and FIC guidance.)

### **c. Risk assessment and written AML/CFT / TF policy**

- ✚ Periodic risk assessment (geography, programs, delivery channels, donors). A written policy and procedures to mitigate risks (donor screening, beneficiary controls, cash handling, PEP/sanctions checks). FATF stresses risk-based measures; FIC guidance expects NPOs to implement such controls.

### **d. Beneficiary, partner and donor due diligence (DD)**

- ✚ Basic KYC for large donors; vetting for partner organisations and high-value beneficiaries; document source-of-funds for suspicious or large donations. (FIC Guidance Note for donors and NPOs.)

### **e. Financial controls and record-keeping**

- ✚ Segregation of duties, bank account(s) in NPO name, approved signatories, receipts and invoices, accounting records for at least 5–7 years, annual audited financials (if size/requirements demand). FIC registration asks for bank account(s) and accounting contact details.

### **f. Reporting and registration obligations to FIC and other authorities**

- ✚ Register (if required), file annual returns to FIC, promptly update registration on material changes.

#### **g. Internal controls for programs and cash/asset management**

- ✚ Standard Operating Procedures (SOPs) for cash distributions, procurement, asset inventories, fuel/vehicle use, vouchers, beneficiary lists, field receipts, dual authorization for payments.

#### **h. Training and awareness**

- ✚ Regular training for staff/volunteers on AML/CFT, donor screening, whistleblowing and sanctions. NPO must maintain staff training records.

#### **i. Transparency and public-facing information**

- ✚ Up-to-date websites and public documents (mission, activities, audited financials, annual report), to reduce reputational risk and increase donor confidence.

#### **j. Suspicious activity reporting (SAR) channels**

- ✚ A named compliance focal point, procedure to escalate suspicious transactions to the FIC (and to law enforcement where required), and internal threshold triggers for review. FIC has channels for reporting and provides guidance.

It is significant to indicate that FATF sets the global risk-based approach and clarifies a subset of NPOs that may need supervision; implementation must be proportionate to the NPO's risk profile. FIC applies this in Namibia via its registration process and Guidance Notes (e.g., Guidance Note 13 on risk-based controls and Guidance Note 18 for donors).

## 8.2 The following NPOs financial bank statement has been analysed

### NPO-A

The account number 000-1 held at Bank-F in the name of the above entity for the period of 01 January 2022 to 04 March 2025, reflects the accumulation of credit amounting to N\$ 620,312.19. Subsequent to the above credit, a total amount of N\$ 3,10.00 was debited from the account bearing the name "Maintenance fee" during the above stated period. The majority of deposits were made with description as "contribution".

### NPO-B

It is reported that such NPO is relating to various organizations in the Republic of Namibia which are suspected to be involved in the indoctrination and radicalization of Namibian nationals within the borders of the Republic of Namibia. The entity has two accounts at Bank-D, the first account no: 00022 has a balance of N\$26,556.29 as of 03 March 2025. This account reflected the accumulation of credit amount mostly described "00000." Such a source of funds is not established at this stage. The second account, no: 00023, has a balance of N\$590,096.98 in the same period. Such accumulated funds were deposited by various individuals. Most significant amounts were deposited with description "M0000III".

### NPO-D

The account number 00044 held at Bank-D in the name of the above entity for the period of 01 January 2022 to 04 March 2025, reflects the accumulation of credit amounting to N\$ 2,236,673.05. The majority of deposits were made with description as ""DONATION" and "BankdCOLLECTION" amongst others. The account has also received EFTs and various deposits from various individuals. Further, this NPO has also an account with Bank-E, account no: 00045. Unestablished significant amounts were deposited into this account by various entities and individuals.

### NPO-G

The entity has two accounts with Bank-D, the first account no: 00055 has account balance of N\$ 91,188.06 as of 04 March 2025. This account reflects the accumulation of credit amount deposited by various individuals and entities. The second account no: 00056 has a balance of N\$ 5,221.80. The amounts were deposited with description "J00012". Similarly, such sources of funds are not established at this stage.

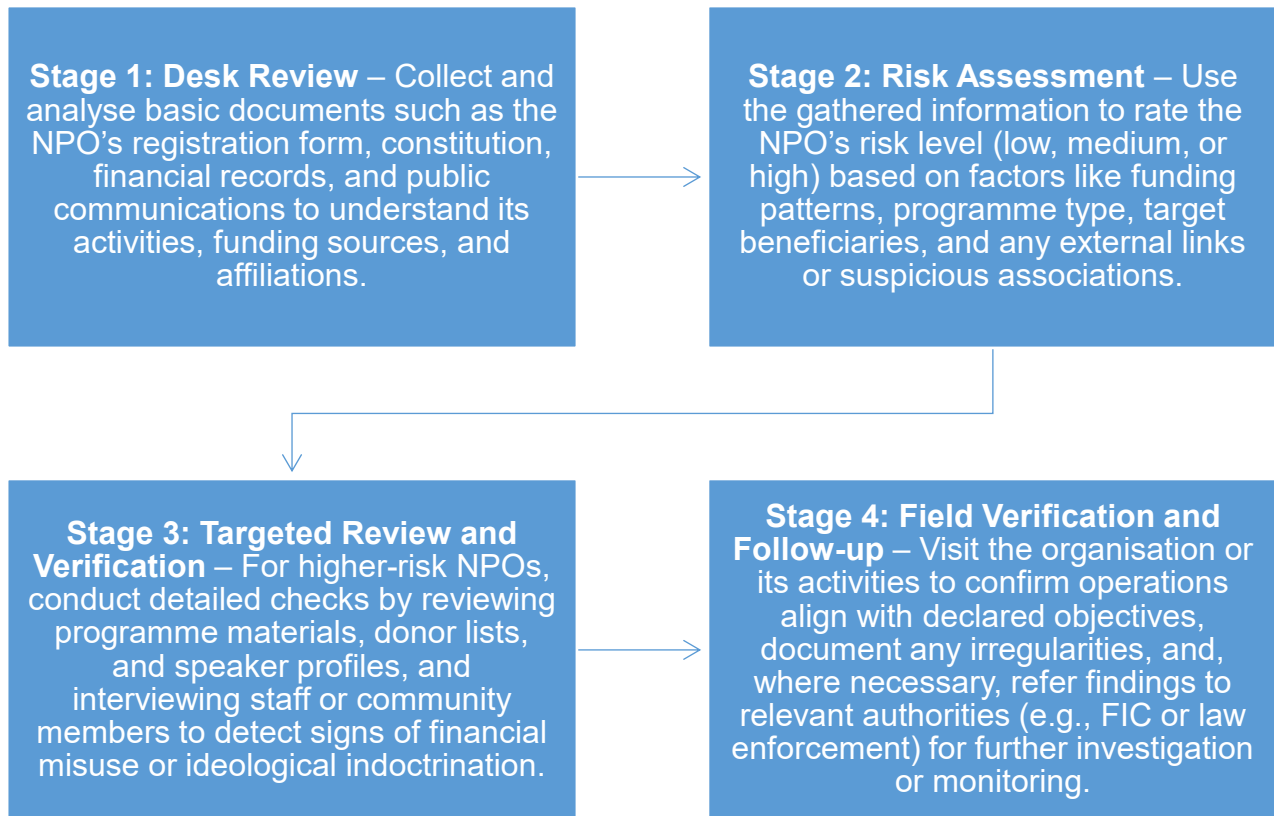
It is important to indicate that the cases analysed show that other higher risk NPOs highlighted above have no account with commercial banks and some which had accounts are now closed. Given the difficulties in assessing the true scale and scope of the sector, the risks associated with ML/TF must be assessed as high, particularly religious associations, which operate unregistered and unregulated. There is no direct evidence that implicates any part of the sector, but greater certainty of this can only be achieved by greater transparency.

### **8.3 NPOs risk of terrorist abuse to include indoctrination / radicalization**

FIC adopt a risk-based approach (RBA) to identify which NPOs are most vulnerable to terrorist abuse, apply proportionate measures, protect legitimate civil society, and use targeted mitigations rather than broad bans or heavy-handed blanket rules. In this regard, the FATF's concern is not only about funds, it also covers use of NPOs for recruitment, radical messaging, training, and mobilization (i.e., ideological/operational abuse).

Another key aspect is indoctrination which refers to organized efforts to instill a set of beliefs or ideology in a targeted audience, often by repeated messaging, training, recruitment or educational activities. On the other hand, radicalization is a process by which an individual adopts extreme political, social or religious beliefs that may (in some cases) lead to support for, or participation in, violence or illegal activity. Radicalization is a process (not a single event) and can be social, ideological, or operational.

The review of NPOs can be conducted through four key stages to ensure both financial and ideological risks including indoctrination are properly assessed.



Together, these stages ensure a balanced, risk-based approach that identifies potential terrorist abuse or radicalization within NPOs while protecting legitimate charitable work.

#### 8.4 NPOs reported to the FIC

Below are the NPOs which have been reported by NamPol to the FIC involved in various activities such as Terrorist Activities by means of recruitment, inciting to and Financing of Terrorist Activities, foreign nationals working as Imams in Namibia, practices of orthodox ideologies on Christ and witchcraft amongst others. Such NPOs were reported to the FIC under one SAR-0959/24-JUN-20 and subsequently, Case No-1975/24-FEB-21 was opened. It is further reported that such NPOs are relating to various religious organizations in the Republic of Namibia which are suspected to be involved in the indoctrination and radicalization of Namibian nationals within the borders of the Republic of Namibia. Their case studies have been illustrated below for demonstration purposes.

- a. NPO-001
- b. NPO-002
- c. NPO-003
- d. NPO-004

- e. NPO-005
- f. NPO-006
- g. NPO-007
- h. NPO-008
- i. NPO-009
- j. NPO-0010
- k. NPO-0011

### **Case Study: 1: Terrorism Investigation: Windhoek CR 2019-00001**

There is one active case of terrorism reported as per Windhoek CR 2019-00001, involvement in Terrorist Activities by means of Recruitment, Inciting to and Financing of Terrorist Activities.

It was reported that a certain Namibian male is believed to have been radicalized and is trying to incite and recruit other people mostly Namibians of Islamic faith/religion to join the Islamic State in Country-S. He is approaching them in person or through Social Media platforms such as Facebook and WhatsApp.

The subject's activities were interrupted when he was arrested by the authorities during March 2019 whereby his cellphones were confiscated. He was released on bail a few days later and has been off-air after his release until July 2019, when he renewed his contact number. However, the subject restricted all his known social media address from the public view to only be viewed or accessed by selected contacts.

Apart from the cases mentioned above, there was another similar incident of involvement in terrorism which was reported during 2015 and 2016, where two Namibian brothers joined I-001 and travelled, at different moments, to Country-S to receive military training and join the military wing of I-001. The whereabouts of the two brothers is unknown, but information so far has revealed that they were both killed in a battlefield in Country-S.

### **Case Study: 2: NPO-B**

#### **Imams at NPO-B expressed displeasure about foreign nationals working as Imams in Namibia**

Information revealed that on Monday, 07 November 2016, Imams at NPO-B expressed unhappiness about foreign nationals who were sent to Namibia to work as Imams at NPO-B. These foreign nationals were from Malawi, Uganda, Kenya, Egypt, Tanzania and Iran who are

posted to different parts of the world, including Namibia. They are said to receive salaries from Country-A<sup>4</sup>.

According to the information, none of these foreign nationals had a required standard for the work they were doing in Namibia, and that although there were Namibians who were more qualified than expatriate Imams, they were not given opportunity to work.

The information further revealed that the foreign nationals came to Namibia under the pretext of preaching the Islamic religion, yet they were engaged in dubious, corrupt and criminal activities such as car dealership, selling and issuing fake foreign passports and dealing in drug trafficking. Their aim was to make money out of illegal activities in Namibia for possible financing of terrorism. Such Imams do not concentrate on religious affairs of Muslims in Namibia as stipulated on their applications.

It was further stated that a certain Mr-A who was in Namibia for a couple of years but relocated to the Country-B was involved in printing and issuing of fake passports but when he left for the Country-B, this business was still being carried out by these foreign nationals.

The subjects were also receiving payments when conducting marriages and this is reportedly against Islamic belief, as marriages are supposed to be solemnized free of charge.

It was further reported that most of the subjects do not have proper documentation, and some were on work permits which are renewed after every three months by the Ministry of Home Affairs and Immigration.

Further, the subjects are reported to be in possession of more than one passport with different names. An example given is that of Mr-C, who was denied entry to Namibia at one point when he came back from Kenya because his work permits expired. His wife indicated at the time that they had arranged for another passport for her husband to come to Namibia.

It was further stated that the subjects were engaging in marriages with Namibian women for the purpose of acquiring citizenship as such marriages are regarded as marriages of convenience, which guarantee their permanent status to stay in Namibia and makes it difficult for the Government to deport them.

Lastly, the Imams at NPO-B made an appeal to the Government of the Republic of Namibia to intervene and stop the illegal activities that are taking place at NPO-B. They Said they were

---

<sup>4</sup> As per report filed by FIC

ready to provide information to law enforcement in order to remedy the situation at the organisation.

### **Case Study: 3: NPO-0012:**

#### **Practices of orthodox ideologies on Christ and witchcraft**

An investigation conducted since 23 April 2020 revealed that a certain individual, who was reported missing by her father, was not missing but was distanced from her family by one Pastor of NPO-0012.

Father-S claimed that the Church negatively influenced his daughter, turning her to practices of orthodox ideologies on Christ and witchcraft. The church, which is situated in Katutura, is guarded by security and has a right of admission sign posted at the entrance, thus restricting access.

It was established that the Church is indeed owned by the above-mentioned Pastor, a Country-F national, who is married to a Namibian national. According to information, the Pastor was a former Country-F Ambassador to various countries. During the investigation, former Church members were interviewed, and they revealed the following:

- a. Pastor's intentions in the church are alleged to be aimed at destroying good relationships, for instance marriages, family and friendships. Once you become a member of the Church, you are not allowed to freely attend funerals, weddings and visiting friends or relatives because anyone not from his church is regarded as evil or a witch.
- b. Further, that Pastor had called on his congregants to burn valuable properties/belongings and documents (i.e. furniture, vehicles, bibles, wedding rings, qualifications, ID documents) citing that they are possessed with evil or witchcraft, and refusal by members lead to the Pastor breaking marriages by imposing forced separation and eventually causing divorce.
- c. According to Mrs-M, a former member of the said church, Pastor told her to bring the umbilical cords of her newborn twin babies so that they can be burned in the church, which she refused to do. After she refused, the Pastor claimed that both her babies would die. She decided to stop attending the church service.

d. Mrs-M further stated that when she refused the Pastor's demand, her husband, Mr-T, stopped to share the matrimonial bed with her and he was sleeping on the couch in their room. She further revealed that she found a paper suspectedly written by Pastor implicating and accusing her of being a witch suggesting that her husband must not eat her food and not sleep with her.

e. The former church members are said to be willing to give information secretly, as they do not want their names to be revealed to Pastor or to be confronted in court because he is believed to be a dangerous man in witchcraft.

f. According to the interview conducted with different former Church members, the majority suggested that the church be closed down or that Pastor be deported, because he is alleged to be practicing witchcraft or is causing disunity amongst the congregants; that he creates separation within their families or relationships, as he even advises them (congregants) to keep a distance from their family by not visiting them.

Right of admission to church premises raises questions for a place of religious purposes.

#### **Case Study: 4: Mushrooming of Pentecostal Churches and suspicious activities**

Zambezi Region is faced with the mushrooming of many charismatic churches, most of which are headed by foreigners. Types of churches operating in the region are as follows: Roman Catholic, ELCIN, Seventh Day Adventist, New Apostolic, Pentecostal Churches, Enlightened Christian Gathering (ECG), Universal Church, Jehova's Witnesses, Dutch Reformed, Assemblies of God and one Mosque.

The security assessment that was conducted during 2019 revealed that some Churches are having suspicious activities that are affecting the community. These activities range from the way they are conducting their business in terms of sourcing money from the congregants to the end use of such contributed money.

It was observed that these Churches are having a system of requiring congregants to contribute 10% of their monthly income to the church on a monthly basis as tithe. The money is donated in envelopes that are placed in a basket in church, whereby the Pastor will collect all the money, and nobody knows exactly where this money is ending up. There is a sign of indoctrination on the part of the churches as the members are made to believe that whatever they are donating will increase the ties between them and God. Some of the congregants ended up contributing

almost everything that they have to the church to apparently increase their ties with God. The radicalization activities were not detected in these churches so far.

Indoctrination was observed in one church, the followers are made to believe that the more contribution they give to the church, the closer they will be to God. People are having three different contributions in church:

Donation made for Pastor every Sunday offering;

Offering every Sunday; and

Tithes every Sunday, the amount depends on what one is having that day.

The most suspicious organization in the region is the NPO-0013 situated in Katima Mulilo. The Mosque is headed by Mr-D, Country-I businessman and it is located inside his residential premises which makes it difficult for the police to monitor the activities. Information at hand revealed that the Mosque leaders who are all businesspeople in Katima Mulilo, have recruited several Namibians as employees and turned them to certain religion. The conversion of workers starts immediately at the job application in which they put a requirement that anyone who needs employment in that business or domestic work should be of such religion.

Although no sign of radicalization was observed in the region from the religious organizations, the possibility cannot be ruled out. The region has a sensitive political situation coupled with the ongoing struggle of seceding the region from the rest of Namibia by Mr-MS and his group. This group of Caprivi Liberation Army (CLA) was observed to try to join hands with the Group-Z Western Country-Z, in efforts to secede the so-called Barotseland which they claim to include three neighboring countries.

Current information revealed that there is a radical group from Country-MZ currently operating in Country-Z's Western Province trying to assist the Barotse in fighting for their "independence". Based on this information, considering the ties between Muyongo group and the Barotseland, it cannot be ruled out that the two (02) groups can still cooperate to radicalize people in Western Province of Country-Z as well as in Zambezi Region. The police are working on the information to establish whether Zambezi Region is also affected at this stage.

Radicalization generally targets the marginalized communities as soft targets; therefore, Zambezi Region cannot be spared as a target since it housed many Barakwena communities,

who can be easily turned into religious radicals due to their level of civilization. Currently no signs of radicalization are observed in the region.

## 9. POTENTIAL INDICATORS OF TF IN NPOs AND OTHER SECTORS

There are few known cases of NPOs being criminally misused, and most involve charities raising or hiding funds to support terrorist activities. Like other crimes, there are red flag indicators that can help identify potential terrorist financing (TF) or related offences. These indicators are observable signs that, on their own, may not confirm wrongdoing, but when combined with other evidence or patterns, they can reveal a higher risk or likelihood of criminal activity. The indicators serve only as a guideline and are not exhaustive, meaning investigators should use them together with other relevant information and context. The indicators are grouped into five main categories such as financial, operational, governance, partnerships, and behavioral to support structured analysis.

<b>1. Financial Red Flags</b>
These indicate possible misuse of funds or financial systems to channel money toward terrorism:
<ul style="list-style-type: none"><li>• Unexplained or sudden increases in donations without clear source or donor details.</li></ul>
<ul style="list-style-type: none"><li>• Frequent cash deposits or withdrawals, especially just below reporting thresholds.</li></ul>
<ul style="list-style-type: none"><li>• Transfers to or from high-risk jurisdictions, conflict zones, or countries with known terrorist activity.</li></ul>
<ul style="list-style-type: none"><li>• Use of personal or third-party accounts instead of the organisation's official bank account.</li></ul>
<ul style="list-style-type: none"><li>• Donations made in foreign currencies or through informal money transfer systems (e.g., hawala).</li></ul>
<ul style="list-style-type: none"><li>• Unusual patterns of remittances that don't match the stated purpose of the NPO.</li></ul>
<ul style="list-style-type: none"><li>• Circular fund movements (money returning to sender or linked entities).</li></ul>
<ul style="list-style-type: none"><li>• Inadequate or missing records for incoming or outgoing funds.</li></ul>

<ul style="list-style-type: none"> <li>• Funds transferred to individuals rather than registered partner organisations.</li> </ul>
<ul style="list-style-type: none"> <li>• Multiple small donations from unknown donors that cumulatively form large sums.</li> </ul>
<ul style="list-style-type: none"> <li>• Rapid disbursement of donations soon after receipt, without proper accounting or verification.</li> </ul>
<ul style="list-style-type: none"> <li>• Payments to persons or entities unrelated to the declared NPO activities.</li> </ul>
<ul style="list-style-type: none"> <li>• Use of multiple bank accounts across different institutions without operational need.</li> </ul>
<p><b>2. Operational Red Flags</b></p>
<p>These points to suspicious activities within the NPO's projects or programmes:</p>
<ul style="list-style-type: none"> <li>• NPO runs programmes in high-risk or conflict areas without proper due diligence.</li> </ul>
<ul style="list-style-type: none"> <li>• Activities inconsistent with the stated mission or registration purpose.</li> </ul>
<ul style="list-style-type: none"> <li>• Lack of verifiable evidence of projects or beneficiaries (e.g., no receipts, photos, or lists).</li> </ul>
<ul style="list-style-type: none"> <li>• Frequent changes in project locations or beneficiaries without clear justification.</li> </ul>
<ul style="list-style-type: none"> <li>• Programmes targeting youth or vulnerable groups with little transparency or oversight.</li> </ul>
<ul style="list-style-type: none"> <li>• No physical presence or legitimate office despite active fundraising.</li> </ul>
<ul style="list-style-type: none"> <li>• High administrative expenses with little spending on actual charitable activities.</li> </ul>
<ul style="list-style-type: none"> <li>• Outsourcing of projects to unregistered or informal groups.</li> </ul>
<ul style="list-style-type: none"> <li>• Events or gatherings that include unvetted external speakers or ideological messaging.</li> </ul>
<p><b>3. Governance and Structural Red Flags</b></p>
<p>These relate to weak internal controls or suspicious leadership arrangements:</p>
<ul style="list-style-type: none"> <li>• Unknown or unverifiable board members or trustees.</li> </ul>
<ul style="list-style-type: none"> <li>• Frequent changes in leadership or signatories without explanation.</li> </ul>

<ul style="list-style-type: none"> <li>• Family members dominate management or board positions.</li> </ul>
<ul style="list-style-type: none"> <li>• Absence of internal financial controls (no segregation of duties, no audits).</li> </ul>
<ul style="list-style-type: none"> <li>• Failure to maintain proper records or submit required reports to FIC or line ministry.</li> </ul>
<ul style="list-style-type: none"> <li>• Non-cooperation with supervisory or law enforcement requests.</li> </ul>
<ul style="list-style-type: none"> <li>• Dormant or inactive boards, while operations continue under different names.</li> </ul>
<ul style="list-style-type: none"> <li>• Failure to register with the FIC or update details (Annexure A incomplete or outdated).</li> </ul>
<ul style="list-style-type: none"> <li>• NPO shares address or contact details with known high-risk entities or persons.</li> </ul>
<p><b>4. Partnership and Donor Red Flags</b></p>
<p>These relate to suspicious relationships with other organisations or funding sources:</p>
<ul style="list-style-type: none"> <li>• Partnerships with foreign organisations are not subject to regulation or oversight.</li> </ul>
<ul style="list-style-type: none"> <li>• Donors or partners unwilling to provide full identification or documentation.</li> </ul>
<ul style="list-style-type: none"> <li>• Anonymous or disguised funding, including cryptocurrency donations.</li> </ul>
<ul style="list-style-type: none"> <li>• Links with individuals or groups under sanctions or of law enforcement interest.</li> </ul>
<ul style="list-style-type: none"> <li>• Use of intermediaries or shell entities to channel funds.</li> </ul>
<ul style="list-style-type: none"> <li>• Repetitive use of the same foreign donor without transparency on purpose or reporting.</li> </ul>
<ul style="list-style-type: none"> <li>• “Front” organisations used to move funds under the cover of humanitarian aid.</li> </ul>
<ul style="list-style-type: none"> <li>• NPO receives or sends funds to organisations with radical, extremist, or political agendas.</li> </ul>
<p><b>5. Behavioural / Ideological Red Flags (Indoctrination or Radicalization Focus)</b></p>
<p>These reflect potential non-financial abuse of NPOs for recruitment or ideological influence:</p>
<ul style="list-style-type: none"> <li>• Teachings, sermons, or programmes promoting intolerance or extremist narratives.</li> </ul>
<ul style="list-style-type: none"> <li>• Closed or secret gatherings with restricted attendance lists.</li> </ul>

<ul style="list-style-type: none"> <li>• Guest speakers or trainers with known extremist affiliations or past inflammatory rhetoric.</li> </ul>
<ul style="list-style-type: none"> <li>• Youth camps or training where activities are undisclosed or lack adult supervision.</li> </ul>
<ul style="list-style-type: none"> <li>• Use of coded or symbolic language in communications that suggest extremist messaging.</li> </ul>
<ul style="list-style-type: none"> <li>• Beneficiaries pressured to adopt certain beliefs or practices as a condition for aid.</li> </ul>
<ul style="list-style-type: none"> <li>• Isolation of participants from family or community oversight.</li> </ul>
<ul style="list-style-type: none"> <li>• Foreign nationals or trainers involved in unregistered educational or religious programmes.</li> </ul>
<ul style="list-style-type: none"> <li>• Distribution of literature or media that glorifies violence or martyrdom.</li> </ul>
<ul style="list-style-type: none"> <li>• Resistance to oversight by regulators or community leaders, citing “religious freedom” as a shield.</li> </ul>

## 10. KEY FINDINGS

Importantly, STRs and SARs submitted by reporting institutions have played a vital role in helping the FIC and LAEs to identify, investigate, and disrupt individuals and entities involved in potential TF activities.

These reports provide valuable intelligence that supports ongoing investigations, enables the tracing of financial flows, and helps uncover networks that may be using legitimate systems or organisations for illicit purposes.

It has also been observed that legal persons or entities present a higher risk of TF compared to individual clients (natural persons), particularly when their ultimate beneficial owners (UBOs) are not clearly identified or verified. The lack of transparency around ownership structures makes it easier for criminals or terrorist financiers to conceal their identities and misuse such entities for funding or operational support.

The following section therefore outlines the key findings on terrorist financing risks and vulnerabilities identified within the NPO sector and other high-risk sectors, based on STR/SAR analysis and supervisory assessments.

- a. 116 STRs involved TF potential predicate offenses were reported to the FIC. Importantly, 59 STRs were accorded “high priority” status and escalated for further analysis;
- b. Bank-D filed the highest volume of reports related potential TF offences with 76 STRs;
- c. The banking sector was found to have the highest TF risk levels with 93% of the reports originating from this sector. It is further imperative that almost all transactions nationally, from all sectors, pass through the banking sector. The banking sector has comparatively matured AML/CFT/CPF control systems. Despite this, the huge volumes of clients and transactions in the sector escalate the risks as control frameworks in banks are under strain to effectively combat TF;
- d. It is understood that beneficial owners who may launder the proceeds of crime will most likely use complex ownership structures that hide their identification or representation. From the FIA compliance assessment activities conducted in the banking sector, the FIC observed that in most cases, beneficial owners’ information was not adequately obtained when business relationships were established. These findings can similarly be exploited for TF within NPOs;
- e. 29 STRs were received involving NPOs, of which 90% of the reports originate from the banking sector;
- f. From the 29 STRs received, 38% of reports were classified as ‘high priority’ and escalated for further analysis;
- g. Amongst others, funds misappropriation whereby account signatories are suspected of misusing the NPO’s funds for their own good featured as the primary reason in these cases;
- h. The study revealed that funds misappropriation within an NPO features as the leading common reason in the STRs reported;
- i. The study has confirmed conclusively that there are no SARs filed that involve NPO’s;
- j. A certain subject and his entities have been reported on various reports to the FIC with the possibility that he may be linked to TF;
- k. Foreigners are the main perpetrators when it comes to crimes associated in NPOs; and
- l. The study cannot confirm the link between NPOs and terrorist financing.

## 11. POSSIBLE RECOMMENDATIONS

To reduce the risk of TF through NPOs, Namibia should apply a risk-based and balanced approach that strengthens oversight while protecting legitimate charitable work.

1. **Strengthen Regulation and Coordination:** Maintain a central NPO register, ensure annual reporting, and enhance cooperation between the FIC, line ministries, and law enforcement.
2. **Improve Financial Transparency:** Require NPOs to use official bank accounts, keep proper records, disclose all donors, and undergo audits or reviews.
3. **Enhance Governance:** Appoint compliance officers, ensure active and accountable boards, and train staff on AML/CFT obligations.
4. **Apply Due Diligence:** Screen donors, partners, and beneficiaries, verify foreign funding sources and ensure aid reaches legitimate purposes.
5. **Manage Ideological Risks:** Monitor programmes, guest speakers, and youth activities to prevent radicalization or indoctrination.
6. **Build Capacity and Awareness:** Provide training, guidance, and support to help NPOs comply with FATF standards.
7. **Strengthen Reporting and Enforcement:** Encourage timely reporting of STRs and SARs to the FIC and apply proportionate penalties for non-compliance.
8. **Foster International Cooperation:** Share information and typologies with regional FIUs and partners through ESAAMLG and Egmont Group.

Overall, the focus should be on transparency, accountability, and collaboration, ensuring NPOs remain protected from misuse while continuing their vital social and humanitarian roles.

## 12. CONCLUSION

NPOs, while serving important humanitarian and social functions, are inherently exposed to higher TF risks due to their fundraising activities and cross-border operations. Without robust due diligence on donors, strong governance, and strict controls over how funds are received and moved, NPOs can inadvertently become conduits for TF. Financial institutions and regulators must therefore apply enhanced monitoring and risk-based measures to NPOs, particularly those operating in or receiving funds from high-risk jurisdictions.

The risk of the NPO sector is a product of factors related to organisational structure, methods of operation, assets/fund distribution networks and financial management practices. However, there is also significant risk their social role and the inherent trust the sector holds within the community. Embedding operations into the activities of an organisation that commands responsibility and trustworthiness is the ideal cover for criminal activities.

The analysis in this report considered the overall risks of the NPOs structures established in Namibia being misused for financial crimes. It is important that the Compliance Monitoring and Supervision Division takes effective measures to enhance report quality or value adding STRs/SARs which can lead to effective investigations, prosecutions, asset forfeitures and asset/tax recoveries. It is within this spirit that this report is shared. This report or similar studies on the TF risks and within NPO sector will be updated periodically when the need arises.

This report is produced by the FIC's Strategic Analysis Section. For inquiries and communication, please contact [helpdesk@fic.na](mailto:helpdesk@fic.na). Similar studies on potential insurance fraud-related offences will be updated periodically when the need arises.



**Ms. Melintha Fleermuys**

**Acting GM: Analysis and Law Enforcement Department**