



**Financial Intelligence Centre
Republic of Namibia**

PO Box 2882
Windhoek
Namibia

Phone: + 264 61 283 5286
Fax: + 264 61 283 5918
Helpdesk@fic.na

GUIDANCE NOTE NO. 12 OF 2023

GUIDANCE ON RISK ASSESSMENT AND INDICATORS OF POTENTIAL TERRORISM FINANCING

NON-PROFIT ORGANISATIONS: ALL CHARITIES AND RELIGIOUS OR FAITH BASED ORGANISATIONS

First Issued: 30 JUNE 2023

TABLE OF CONTENTS

- 1. BACKGROUND 6
- 2. COMMENCEMENT 7
- 3. HIGH RISK NPOs 7
- 4. UNDERSTANDING THE RISK BASED APPROACH (RBA) 8
 - 4.1 Elements of Risk Management..... 8
 - 4.2 Foundation of the RBA: Conducting Risk Assessments 10
- 5. RISK ASSESSMENT CONSIDERATIONS 11
 - 5.1 Vulnerabilities Within NPOs That Are Abused 11
 - 5.2 Categories of Risk and Abuse 13
 - 5.3 Checklist of Variables to Assess Risks 24
 - 5.4 Risks Associated with High Risk Jurisdictions 25
- 6. EXTERNAL RISK ASSESSMENTS AND TYPOLOGIES 27
- 7. FURTHER GUIDANCE ON CONTROLS..... 27
- 8. GENERAL..... 27
- 9. NON-COMPLIANCE WITH THIS GUIDANCE 28
- 10. GENERAL..... 28
- ANNEXURE A 29



A. DEFINITIONS AND ABBREVIATIONS

“Beneficiary” a person, group, association (or other entity) who is designated to receive the benefits of services, assets, funds or any other type of benefit from a NPO;

“Beneficial Owner” refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Care needs to be taken to identify those who control or direct operations, affairs or the management of an entity without their names being written in any formal documents of the entity as would be expected;

“Customer Due Diligence” (CDD) means a process which involves establishing the identity of a client, the identity of the client’s beneficial owners in respect of legal persons and monitoring all transactions of the client against the client’s profile;

“Enhanced Due Diligence” (EDD) means doing more than the conventional simplified due diligence or the basic CDD measures mentioned above and includes, amongst others, taking measures as per the FIA to identify, as far as reasonably possible, the source of wealth, funds and any other assets of the client or beneficial owners whose activities may pose a risk of ML, TF or PF;

“Directing official” An individual who holds a leadership position in an NPO and has the ability to direct aspects of the NPO’s activities. This includes directors, officers, trustees, and religious leaders;

“Dual-use equipment” Equipment that has both peaceful and military applications, depending on intent;

“FATF” means the Financial Action Task Force. The FATF is an organization that develops policies to prevent and combat money laundering, terrorist and proliferation financing activities. Like most countries, Namibia’s AML/CFT/CPF regime is aligned to the FATF standards;

“FIA” refers to the Financial Intelligence Act, 2012 (Act No. 13 of 2012);

“FIC” means the Financial Intelligence Centre;

“Humanitarian” in this document, humanitarian refers to the promotion of human welfare and is not limited to activities undertaken following emergency or disaster situations;

“LEAs” means Law Enforcement Authorities such as the Namibian Police, Anti-Corruption Commission or NAMRA;

“ML” means Money Laundering;

“Monitoring” as defined in the FIA, for purposes of Sections 23, 24 and 25 of the Act includes:

- the monitoring of transactions and activities carried out by the client to ensure that such transactions and activities are consistent with the knowledge that the accountable institution has of the client, the commercial or personal activities and risk profile of the client;
- the enhanced monitoring of transactions and activities of identified high risk clients in order to timeously identify suspicious transactions and activities; and
- the screening of the name of a client or potential client, and the names involved in transactions, against the sanctions lists issued by the United Nations Security Council under Chapter VII of the United Nations Charter; for purposes of combating money laundering, the financing of terrorism and the funding of proliferation activities.

“NPO” refers to any type of Non-Profit Organisation. Note however that in terms of the FIA, only some NPOs are highly exposed to TF risks and thus, only such are required to comply with the FIA. This Guidance Note is only addressed to such NPOs, which are religious or faith based organisations and those involved in charitable activities/services;

“PEPs” means Political Exposed Persons (See FIC Guidance Note 01 of 2019);

“PF” means proliferation financing;

“Records” means any material on which information is recorded or marked and which is capable of being read or understood by a person, or by an electronic system or other device;

“Religious leader” means a person who is a member of the governing body of any religious body or a person who is vested with the decision-making authority within the religious body;”

“Regulations” refer to the FIA Regulations unless otherwise specified;

“RBA” refers to the Risk Based Approach. An approach for managing risks based on prioritization of such risks as per the occurrence/frequency/probability and potential impacts/consequences of each identified risk;

“TF” means Terrorist Financing;

“Terrorist entity” In the context of this guidance, a terrorist entity refers to a terrorist and/or terrorist organisation identified as a supporter of terrorism by national or international sanctions lists, or assessed by a jurisdiction as active in terrorist activity;

“Terrorism financing (TF)” The financing of terrorist acts, and of terrorists and terrorist organisations. Includes when a person wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts). TF includes financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. TF as a concept is broad and extends to any funds or other assets whether from a legitimate or illegitimate source;

“Threat” A person or group of people, object or activity, with the potential to cause harm. Threat is contingent on actors that possess both the capability and the intent to do harm;

“Transaction” means a transaction concluded between a client and an accountable or reporting institution in accordance with the type of business carried on by that institution, and includes attempted transactions;

1. BACKGROUND

This guidance note will add to the framework of tools aimed at enhancing Anti-Money Laundering, Combatting the Financing of Terrorism and Proliferation (AML/CFT/CPF) measures at institutional, sectoral and national level. It is common cause that services offered by NPOs have been abused for ML domestically, as reflected through cases in the 2015-20 NPO National Risk Assessment (NRA) updates. The greater concern is however combatting the abuse of NPOs to advance TF activities. The FIA Amendments are tailored to specifically enhance TF risk management within the NPO sector.

The 2020 NRA found religious and faith based organisations as 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, the 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.

This Guidance aims to help NPOs understand how to go about conducting risk assessments and identify indicators of potential TF activities. Risk understanding and documenting is the starting point for implementing risk based mitigation systems at sectoral and institutional level. Risk assessment outcomes are supposed to highlight risk levels in a NPO's operations and services. Such risk levels ought to then inform the prioritization of control implementation. While this guidance focuses on risk understanding, Guidance Note 13 of 2023, issued along with this Guidance, provides essential guidance on how NPOs can effectively implement mitigating controls in line with identified risks.

This Guidance Note is issued in terms of Section 9(1)(h) of the Financial Intelligence Act, 2012 (FIA) and is applicable to only those NPOs stated herein above.

2. COMMENCEMENT

This Guidance Note comes into effect on **03 July 2023**.

3. HIGH RISK NPOs

The type of NPOs supervised as per the FIA are **religious or faith based organisations** and those involved in **charities** (or provision of such ‘good works’). Such NPOs are required to align their risk management measures with the FIA and as simplified in this Guidance Note and Guidance Note 13 of 2023.

In Namibia, as it is around the world, not all NPOs are highly exposed to risks of TF. Only those highly exposed to such risk should be subjected to regulatory and supervisory activities in terms of the FIA and FATF Recommendations. The point of departure is therefore to first identify those within the category of highly exposed NPOs. This ensures due regulation and supervision of NPO activities is risk based and does not undermine legitimate NPO operations.

The FATF Study¹ 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, 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.

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 these organisations are most at risk. The FATF has defined a NPO in its Interpretive Note to Recommendation 8 as “a legal person or

¹ <file:///D:/09%20November%202022/NPOs/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf>

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 that measures to combat TF activity in the NPO sector should “apply to NPOs which account for:

- a. significant portion of the financial resources under control of the sector; and
- b. substantial share of the sector’s international activities.

This 2023 National Risk Assessment update could not find anything within local NPOs that would deviate from the said trend. If anything, faith based activities, particularly those with potential extremist ideologies exhibited the highest level of exposure to TF risks, as found in the 2023 NRA update. The few domestic cases of potential TF shows how locals were allegedly² ideologically radicalised through FBOs, before embarking on their journeys to potentially support or associate with terrorist activities in one way or the other. Charitable activities are similarly found to be highly exposed to TF risks.

4. UNDERSTANDING THE RISK BASED APPROACH (RBA)

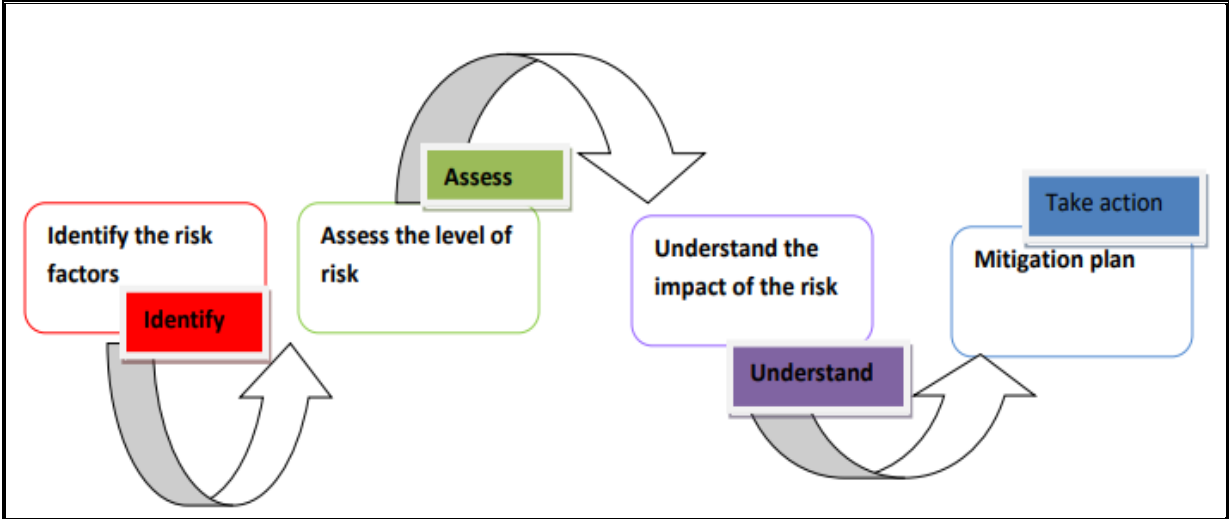
4.1 Elements of Risk Management

The primary intent of supervising and regulating NPOs as per FIA obligations and international standards is to ensure NPO services and operations are not abused to advance or support criminal activities such as ML and in particular TF activities.

The RBA speaks to a control system premised on a NPO’s understanding of risks it may be exposed to. As shown in the diagram below, such understanding is what informs the design, nature and extent of controls implemented to mitigate risks (implementation of controls). The primary RBA elements are: identifying risks, assessing such risks to understand their levels and impact, followed by a mitigation plan aligned to such risk levels. An effective control

² This is not yet proven but the few suspects converted from Christianity to other religions and that is when it is suspected they may have been radicalized. Though they had close ties to FBOs there is no proof that the FBOs directly played any part in extremist radicalization.

implementation is also characterised by documenting ML/TF risk findings (in a risk report) and updating such when the need arises. This enables a platform through which risks are tracked. The figure below outlines the primary elements of the RBA.



Risk Based Approach implementation framework

The primary RBA steps can be explained as follows:

- a. **Identifying ML/TF risks facing a NPO:** this should be done with consideration of its beneficiaries, donors, nature and extent of its services, countries of operation, delivery channels and third parties it is associated with etc. with external factors, NPOs ought to consider the most reliable open source information or information it can obtain from relevant authorities (may include ML/TF risks and typologies information). This process also ensure risks are duly *assessed*, classified or rated to enhance *understanding* of such. The understanding of risks lays the foundation for implementing risk management measures;
- b. **Risk management and mitigation:** identifying and applying measures to effectively and efficiently mitigate and manage ML/TF risks. Guidance Note 13 of 2023, issued along with this guidance explains how to implement risk based controls aligned to the understanding of relevant risks;



- c. **Ongoing monitoring:** implementing policies, procedures and information systems to monitor changes to ML/TF risks across the operations and services of the NPO; and
- d. **Documentation:** documenting risk assessments, strategies, policies and procedures to monitor, manage and mitigate ML/TF risks is essential.

The above suggests that access to accurate, timely and objective information on ML/TF/PF risks is a prerequisite for an effective RBA. If duly implemented, the RBA ensures prudent balancing of compliance costs to business and customers by prioritising and directing controls to where they are most needed, in a prudent manner. This ensures high risk clients and services are accorded controls which are commensurate to such risk levels while lower risk clients and services are not burdened with unwarranted stringent customer due diligence.

4.2 Foundation of the RBA: Conducting Risk Assessments

The object of understanding client and transaction risks is to help the NPO determine the level of due diligence that beneficiaries, donors, certain transactions and if need be, third parties or associates should be subjected to. The principle in AML/CFT due diligence is that low risk services, operations, donors or beneficiaries making use of low risk services should be subjected to minimum or simplified due diligence. On the other hand, higher risks should be subjected to enhanced risk management measures as outlined in Guidance Note 13 of 2023. The nature and extent of risk management measures is dependent on the level of assurance/comfort that a NPO needs to gain in reducing its ML/TF risk exposure.

NPOs, like all other sectors are best placed to understand their risk exposure and thus implement relevant controls to manage same. This next sections hereunder avail guidance around understanding risk exposure and carrying out risk assessments as a starting point for implementing the RBA.

5. RISK ASSESSMENT CONSIDERATIONS

While no cases of NPO abuse for terrorist purposes were observed in Namibia to date, THE principal *methods of operation* in the abuse of NPOs are universal as documented in the FATF Report³ on Risk of Terrorist Abuse. The said report provides a comprehensive presentation of how NPO TF abuse can occur and talks to indicators that may help in detection of same. The 2015-20 NPO risk assessment updates highlight poor governance, controls and risk management framework in NPOs, especially religious and Faith Based Organisations. Such were exploited to advance fraud and ML. The said risk management and governance shortcomings within NPOs can be similarly exploited to advance TF activities. For this reason, the cases studies and examples cited herein, sourced from international studies, are used to merely demonstrate how risks within NPOs can materialise.

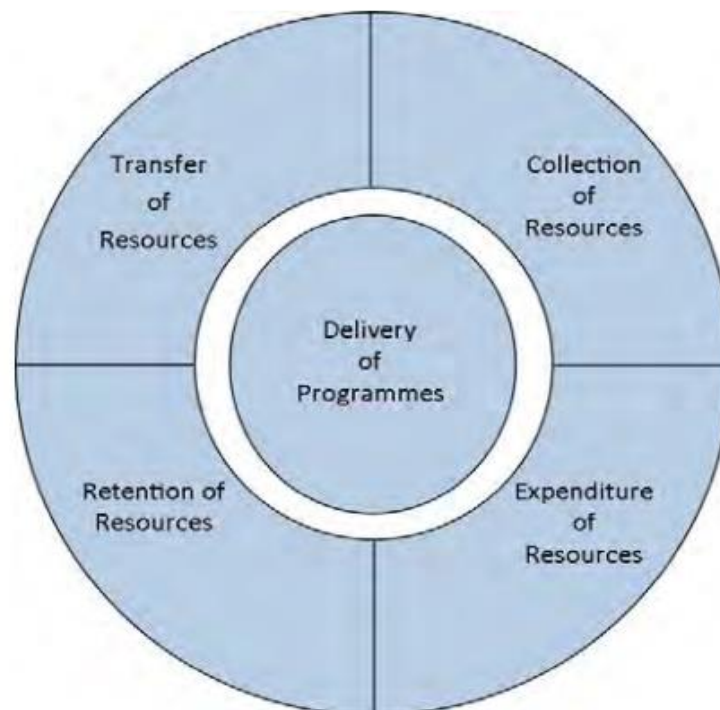
5.1 Vulnerabilities Within NPOs That Are Abused

In the FIC's workshops held with the NPO sector since the last quarter of 2020, a common question raised in different ways is: What makes NPOs vulnerable (or attractive) to abuse in advancement of terrorism? NPOs, being legitimate international actors, can easily capture many operational advantages from globalisation, including:

- a. General trust and goodwill that NPOs enjoy as entities the service social interests;
- b. Increased mobility;
- c. Interconnectedness of NPO networks which makes it easier to move values from one NPO to another or otherwise;
- d. Expanded and deepened access to areas of conflict or low-governance which is not easily seen with other types of arrangements or similar vehicles ;
- e. Diversified financial services and logistical networks;
- f. Decentralised communications and management; and
- g. Increased ability to engage the public.

³ <file:///F:/09%20November%202022/NPOs/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf> (2014)

In an effort to establish how abuse can occur in the NPO sector, it is necessary to outline the model of NPO operations that is generally applicable, particularly to the service activity organisations as such are highly vulnerable. Note that domestically, religious or Faith Based Organisations and charitable activities are the most vulnerable for TF activities. Within the context of understanding NPO abuse, it is generally accepted that NPO operations can be reduced to five general elements as per below:



- a. The **collection of resources** refers to any activity undertaken by an NPO to acquire resources either directly or through third parties such as volunteers;
- b. The **retention of resources** refers to the storage or maintenance of resources by an NPO. Retention includes activities ranging from the maintenance of funds within bank accounts to the management of property or facilities;
- c. The **transfer of resources** can occur at multiple instances during NPO operations and refers to any point at which the resources of the NPO are transferred between different actors;

- d. The **expenditure of resources** refers to any point at which an NPO's resources are exchanged in return for goods or services; and
- e. All of the above revolve around the **delivery of programmes**. The delivery of programmes refers to the point at which an NPO is carrying out programme activities. This could include activities such as the distribution of aid, the provision of medical treatment, the holding of fundraising events, or the hosting of a guest speaker.

5.2 Categories of Risk and Abuse

Generally, five categories of abuse or risk can be established from the FATF study⁴, which are generally applicable across all NPOs. These are not mutually exclusive categories and can be summarised as follows:

- a. The **diversion of funds** is a significant method that focused on the substantial financial resources within the sector. Actors inside an NPO, or external actors such as foreign partners, were responsible for the diversion. The corrupt use of NPO resources or theft and fraud (though ML and not TF) related thereto presents a generally higher risk in terms of diversion as per case studies highlighted in 2020 NRA;
- b. In other cases of abuse, **NPOs or directing officials maintained 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;
- c. In several cases, **NPOs were abused to provide support to recruitment efforts** by terrorist entities;
- d. NPOs were also targeted for **abuse of programming**. In these instances, the flow of resources was legitimate, but NPO programmes were abused at the point of delivery; and
- e. Finally, some **terrorist entities abused 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.

⁴ As per cases reviewed in terms of the FATF Report on Risk of Terrorist Abuse in NPOs, July 2014.

The primary method of understanding how terrorists may abuse NPOs is through the examination of case studies. Domestically, there have been no indications of terrorist abuse of the NPO sector. The case studies cited in the 2015-20 NPO risk assessment updates largely showed ML and fraud. TF occurs in preparation for subsequent serious criminal acts, as opposed to ML which follows from serious criminal acts. Until the risk environment is fully understood, it will not be possible to implement measures to effectively address the risk of terrorist abuse of the NPO sector. The case studies analysed by the FATF⁵ demonstrated that abuse and risk of terrorist abuse of the NPO sector was commonly the result of:

- a. a lack of robust internal governance; and/or
- b. inadequate or absence of appropriate external oversight.

Additionally, just under half of the case studies analysed involved some form of affiliation with a known terrorist entity or one suspected of supporting terrorist activity, and the majority of NPOs that appeared in the case studies were legitimate organisations as opposed to ‘sham’ NPOs started purely for the purpose of supporting terrorist entities. The table below summarizes methods and risks of NPO abuse in terms of frequency observed.

Methods and Risks of Abuse	Frequency Observed
Diversion of Funds	54%
Affiliation with a Terrorist Entity	45%
Abuse of Programming	10%
Support for Recruitment	26%
False Representation	14%

Methods and Risks of Abuse – Frequency Observed

The subsections below explain the methods of such potential risk abuse.

⁵ FATF, Risk of Terrorist Abuse in NPOs, June 2014.

5.2.1 Diversion of Funds

From the cases showing the diversion of funds typology, an overwhelming majority involved actors internal to the NPO. Diversion of funds by internal actors occurs when a portion of the funds raised by an NPO, for a charitable purpose, is syphoned off and diverted to a terrorist organisation for different purposes. The NPO risk assessment updates of 2015-20 showed how those managing or in charge of directing NPO affairs diverted funds by mostly for fraudulent or self-enrichment purpose. The lack of controls in such instances shows how same can be abused to advance TF. There are examples wherein funds raised by third-parties (ostensibly for charitable purposes) were channelled through the NPO to a terrorist organisation. The use of the NPO to facilitate such transactions has the effect of obscuring an audit trail, severing or distancing any link to a terrorist entity, and decreasing the likelihood of detection by authorities.

It is almost a given that internal actors within the NPO are most likely to be involved in the diversion of funds. Internal personnel are well positioned during the collection, retention, and transfer phases of NPO operations to divert funds for nefarious purposes using a variety of techniques. This particular vulnerability, paired with the threat of insiders who aspire to support terrorism, present considerable risk to the NPO sector. The severity of this risk is supported by the fact that almost half of all the cases submitted involved an element of diversion of funds by internal actors.

During the collection phase, diversion of funds involves the interception of cash prior to the deposits into NPO accounts, while during the retention and transfer phases, the funds are diverted by a variety of means, ultimately ending up in the control of terrorist organisations. Cases involving the diversion of funds by internal NPO actors demonstrate that the following means are used:

- a. wire transfers;
- b. cash transactions and cash couriers;
- c. unrelated persons and personal accounts;
- d. unrelated businesses and business accounts;
- e. money services businesses; and/or

- f. travellers' cheques and cashiers' cheques, though cheques are no more used in Namibia.

The following case study shows an NPO directing official taking cash donations intended for the NPO and depositing them into an unrelated company account. From there, the funds were believed to be transferred to a foreign terrorist organisation.

Diversion of Funds by Actors Internal to NPOs (Collection Phase)

A domestic company was established with very broad commercial purposes. Numerous small deposits were made to the company's account by the individual who had signing authority on the account. The funds were immediately transferred to foreign-based companies. An investigation by the national FIU revealed that the individual with signing authority on the company's account was also a directing official of an NPO.

It was suspected that the small deposits made on the company's account originated from fundraising by the NPO. Law enforcement information indicated that the NPO was known to have ties to a terrorist group. A second directing official of the NPO, who was also a manager of the company, also had ties to the terrorist group. The investigation concluded that the domestic company was a front company being used as a conduit to transfer funds on behalf of the NPO linked to a foreign terrorist group.

In the case below, NPO officials willingly worked with foreign organisations in controlled areas that were suspected of supporting terrorism in order to gain access and provide humanitarian assistance.

Diversion of Funds by Actors Internal to NPOs (Transfer Phase)

A domestic NPO was established to provide a place of religious worship for a diaspora community that had come from an area of conflict, and to raise and disburse funds for humanitarian causes. The national NPO regulator became suspicious when the NPO's mandatory reporting indicated that it had sent funds to organisations that were not legally prescribed beneficiaries. These funds were sent ostensibly in response to a natural disaster that had affected the diaspora community's homeland. One of the beneficiary organisations, however, was believed to be the domestic branch

of an international front organisation for a foreign terrorist group operating in the diaspora community's homeland. The regulator audited the NPO and discovered that it had sent funds to five organisations or individuals that were not legally prescribed beneficiaries. This included USD 50 000 sent to the international front organisation through the domestic branch, and USD 80 000 sent directly to the front organisation's headquarters branch located in the area of conflict.

While the audit was ongoing, the regulator received two leads from the public regarding the NPO. Both leads cited concerns regarding the opacity of the NPO's leadership, and that decisions to send funds overseas had circumvented normal accountability procedures set out in the NPO's governing documents. One of the leads indicated that a shift in the demographic of the diaspora community had meant a new faction had gained control of the NPO's board of directors.

This faction was more sympathetic to the cause of the foreign terrorist organisation. While these issues had already been noted through the regulator's audit, the leads supported the regulator's concerns regarding the NPO's management. The NPO leadership replied to the regulator's concerns by stating that the urgent need to respond to a natural disaster had led the NPO to bypass some internal procedures and to work with whichever organisations could operate in the affected areas. Taking this into consideration, the NPO retained its registration but was forced to pay penalties. The NPO also entered into a compliance agreement with the regulator that would enforce strict due diligence and accountability standards.

5.2.2 Affiliation with a Terrorist Entity

According to the FATF study, the second most commonly observed method and risk of abuse in the submitted case studies relates to the existence of, or suspicion of, an operational affiliation between an NPO and a terrorist entity. This affiliation translates into activity that is meant to financially or otherwise support activities carried out by one or both parties. Affiliations observed range from informal personal connections involving NPO directing officials and terrorist entities, to more formalised relationships between NPOs and terrorist entities. 45% of cases considered in the cited FATF Report involved an element of affiliation between an NPO and a terrorist entity.

Affiliation cases uncovered connections between NPOs and terrorist entities relating to every element of NPO operations: the collection, transfer, retention and expenditure of resources, as

well as the delivery of programmes. In many cases, affiliations encompassed all of these elements.

The case studies in this group demonstrate two main types of affiliation resulting in abuse and/or risk. The first type of affiliation is where NPOs' internal actors, namely directing officials and staff, have established or suspected links to a terrorist entity. The cases where NPOs are abused by internal actors affiliated to terrorist entities demonstrate that these individuals are able to exercise influence over the operations of the NPO that ultimately support terrorist entities. In the case study below, an individual who was on a terrorism watch-list used fake identification to gain employment with an NPO established to advance education.

Affiliation with a Terrorist Entity (Delivery of Programmes Phase)

A boarding school, registered as a religious NPO, hired an individual on a terrorist watch-list. Unbeknownst to the NPO, this individual was responsible for harbouring fugitive perpetrators involved in a terrorist bombing.

Using fraudulent identification, the individual obtained residence and employment as an English language teacher at the boarding school. The director of the school was unaware of the individual's true identity or that he was on the terrorist watch-list.

The individual was subsequently charged and convicted of terrorism-related offences.

The second type of affiliation is where a more formalised relationship exists between the NPO and a terrorist entity. Characteristics that make NPOs effective international actors can also make them particularly vulnerable to abuse. This type of affiliation shows that terrorist entities that operate regional NPO branches can broaden their operational support network. Typologies show that these branches are being used to carry out activities relating to fundraising, the diversion of funds, the procurement of weapons, the recruitment of supporters, military training, and other operation tasks.

In the case below, the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was operating as a foreign outpost of the Sri Lankan-based LTTE.

Affiliation with a Terrorist Entity

(Collection, Retention, Transfer, Expenditure, and Delivery of Programmes Phases)

In January 2005, the Australian Federal Police (AFP) received a letter of complaint from the Sri Lankan High Commission, requesting that the AFP investigate alleged fundraising activity in Australia by the Liberation Tigers of Tamil Eelam (LTTE). The letter contained references to an international network of 'special task forces' fundraising for the LTTE under the guise of the Asian tsunami disaster relief, involving persons in Australia, Denmark, France, Germany, Italy, the Netherlands, Norway, Sweden, Switzerland, and the United Kingdom. As a result of the letter, the AFP Joint Counter Terrorism Team in Melbourne began an investigation into the allegations. The investigation determined that the Tamil Coordinating Committee (TCC), a Melbourne-based NPO run by a small committee, was a cover organisation for the LTTE. The TCC solicited funds from, and coordinated radio and print material for, the Tamil community in Australia. It also lobbied politicians regarding Tamil independence in Sri Lanka and procured electronic and marine equipment on behalf of the LTTE. Hundreds of Australian-based Tamils were persuaded to contribute monthly directdebit payments to the TCC. The TCC also used charity tins to collect money roadside and in shopping centres.

Reportedly, the Australian arm of the LTTE was run by three men: courier Aruran Vinayagamoorthy, Tamil community newspaper editor Sivarajah Yathavan and accountant Arumugan Rajeevan. The same men were also involved in directing the operation of the TCC. Raids on their homes uncovered video footage of Rajeevan and Yathavan firing a machine gun on board an LTTE gunboat in Sri Lanka and visiting one of the group's terrorist training camps. Also uncovered were photographs of Vinayagamoorthy and Rajeevan posing with LTTE founder Velupillai Prabhakaran. Vinayagamoorthy was recorded telling an associate that "[the] TCC are the Tigers and the Tigers are TCC." Vinayagamoorthy and Yathavan ultimately pleaded guilty to providing the LTTE with more than USD 1 million. Vinayagamoorthy also admitted to providing the LTTE with electronic devices, at least one of which was used to make and detonate a bomb used in a terrorist attack.

From an NPO regulatory perspective, the TTC case encompassed multiple (red flag) indicators of risk: it facilitated the transfer of funds to a developing country with an established presence of terrorism; it collected funds in relation to disaster situations; and it was an ethnocentric organisation whose members and supporters did not approve of the listing of an organisation. This case involved the use of financial intelligence from Australian Transaction Reports and Analysis Centre (AUSTRAC) to monitor the flow of funds out of Australia.

5.2.3 Abuse of Programming

Another observed method in which terrorists may abuse NPOs is through the abuse of their programming. The cases in this typology demonstrate that deviations to benevolent NPO-funded programmes, at the point of delivery, can result in abuse intended to support terrorism. There can be varying levels of involvement of actors both internal and external to NPOs in abuse. Studies in the cited FATF Report suggest that while activities relating to this typology were carried out at a domestic level, affected parties were commonly more widespread.

In the following case study, an NPO was exploited by an internal actor who had been empowered to manage the NPO's online presence. While maintaining a website to further an NPO's purposes is appropriate, maintaining a website that promotes terrorism is not.

Abuse of Programming (Delivery of Programmes Phase)

A domestic NPO was the subject of negative open source information suggesting it was condoning suicide bombers on its website. A review of the NPO's website by the national NPO regulator found that the NPO had published a list of 'martyrs' online, including a number of suicide bombers.

Engagement by the NPO regulator resulted in the removal of inappropriate content from the website.

The investigation by the NPO regulator concluded that the NPO had inadequate governance procedures and an ineffective risk management system in place. The NPO was directed to review its governance structure to effectively manage the risks to the NPO.

In another abuse of programming case, an NPO was established to advance religion and education, both charitable purposes in the jurisdiction in which it operated. However, this activity was manipulated by advancing philosophies designed to promote recruitment to a terrorist organisation.

Abuse of Programming (Delivery of Programmes Phase)

An NPO was carrying out religious and educational activities domestically, with no foreign activities.

Information provided by the national FIU indicated that the NPO had received over USD 13 000 from a foreign organisation known to provide support to a foreign terrorist group.

Subsequent open source research indicated that the NPO's education programs espoused an ideology that was shared by several foreign terrorist groups. Concerns arose that this shared ideology was being exploited for recruitment purposes for a terrorist organisation.

It was subsequently revealed that a former student of the NPO's school had been charged in another country with terrorism offences. The student had also met with several other individuals who were later convicted of terrorism offences. The NPO was audited by the national regulator, and the audit found that the NPO could not account for the origin of much of its income and expenditures.

Based on this, the NPO was deregistered.

5.2.4 Support for Recruitment

NPO-funded programmes or facilities can be abused to promote recruitment by terrorist movements. Out of 102 case studies analysed by the FATF, as per cited report, 27 are known to have included the abuse of the NPO sector to support recruitment by terrorist movements.

The existence of activities or material that supports recruitment by terrorist movements is a signal that NPO funds are being, or are in danger of being, intentionally misappropriated. Recruitment-related activities are, in themselves, a form of support to terrorist organisations and often an indicator of a wider intent to support terrorism. Additionally, the existence of such activities or material can represent the corruption of NPO programmes at the point of delivery. An NPO may have a legitimate educational programme, devote resources to it, and hire teachers, all of which are legitimate activities. However, if the teachers then engage in recruitment for terrorist causes, the educational programme and the resources devoted towards it become corrupted.

Support for recruitment cases included instances of abuse and risk where existing terrorist entities were using, or believed to be using, NPOs to promote and recruit for their activities. This method of abuse concerns instances where NPO resources were used to promote causes directly associated with terrorist violence. NPO-funded activities in support of recruitment were

observed at the collection, transfer and delivery phases of NPO operations, both domestically and internationally, as per the FATF study. Cases of support for recruitment demonstrate NPO involvement in the following:

- a. transferring funds to terrorists;
- b. providing financial support to families of terrorists;
- c. carrying out of a fire bomb attack (by an NPO directing official);
- d. organising and hosting events that support terrorism or terrorist entities; and
- e. publishing materials, online or otherwise, supporting terrorism or terrorist entities.

Cases also demonstrate that NPO facilities were used to:

- a. recruit and train individuals to engage in acts of terror such as bomb manufacturing and suicide bombing;
- b. provide a meeting place for terrorist entities; and
- c. host speakers that advocate terrorism.

Support for Recruitment (Delivery and Transfer Phases)

On 4 November 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to U.S. Executive Order (E.O.) 13224 for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including al Qaida and affiliated organisations. Al Rehmat Trust was found to be serving as a front to facilitate efforts and fundraising for a UN designated terrorist organisation, Jaish-e Mohammed (JEM).

After it was banned in Pakistan in 2002, JEM, a UN 1267 designated Pakistan-based terrorist group, began using Al Rehmat Trust as a front for its operations. Al Rehmat Trust has provided support for militant activities in Afghanistan and Pakistan, including financial and logistical support to foreign fighters operating in both countries. In early 2009, several prominent members of Al Rehmat Trust were recruiting students for terrorists had initiated a donation program in Pakistan to help support families of militants who had been arrested or killed. In addition, in early 2007, Al Rehmat Trust was raising funds on behalf of Khudam-ul Islam, an alias for JEM.

Al Rehmat Trust has also provided financial support and other services to the Taliban, including

financial support to wounded Taliban fighters from Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas.

5.2.5 False Representation and Sham NPOs

False representation occurs when, under the guise of charitable activity, organisations and individuals raise funds, promote causes and carry out other activities in support of terrorism. Specifically, the false representation cases can be divided into two categories. The first category involves ‘sham NPOs’ where the NPO is created as a front to support terrorist activity and its stated purposes are false. The second category involves situations where individuals or groups of individuals falsely claim to be acting on behalf of existing legitimate NPOs.

The cases demonstrate that sham NPOs and individuals falsely claim to be acting on behalf of existing legitimate NPOs, scheme to collect funds to support terrorism, and/or deliver programmes in support of terrorism.

In the following sham NPO case, an NPO claiming to be a school was actually established solely to recruit students for attacks against local police, prosecutors and judges, and to manufacture bombs.

False Representation (Delivery of Programmes Phase)

A bomb blast occurred at a religious boarding school being operated as an unregistered NPO. The ensuing investigation found that the school was being used by members of a terrorist group to recruit students for attacks against local police, prosecutors and judges and for the manufacture of homemade bombs. The director of the school was convicted of terrorism-related offences.

In the case study below, two individuals were observed falsely representing themselves as members of a well-known NPO in order to raise funds to support a militant fighting abroad.

False Representation (Collection Phase)

Two individuals were raising funds domestically for a family member who was fighting alongside a listed terrorist organisation abroad. The individuals, claiming to be representatives of a well-known domestic humanitarian aid NPO, were raising the funds by way of public street collections. The collection efforts were in breach of the domestic law.

The individuals in question did not have the consent of the domestic NPO to solicit donations on its behalf nor did they deliver to funds raised to the NPO. Once a sizeable amount of money had been collected, it was sent to the family member abroad using wire transfers.

As a result of a joint investigation between the FIU, NPO regulator, and law enforcement authorities, the two individuals were arrested and convicted of terrorist fundraising and sentenced to jail.

5.3 Checklist of Variables to Assess Risks

The following checklist, though not exhaustive, helps NPOs, especially charities identify vulnerabilities to terrorist abuse. As part of a broader risk assessment activity, NPOs may thus consider answering the following questions:

- a. Do you know about the individuals and entities associated with terrorism, which are listed as such by the United Nations Security Council (UNSC), and other authorities such as OFAC?
- b. Are you aware of the Financial Intelligence Act, 2012, in particular its application to financing and supporting terrorism—and the consequences of breaching the provisions?
- c. Do you have a good understanding of the background and affiliations of your board members, employees, donors, fundraisers, and volunteers? This document contains guidance which should be considered in evaluation whether the said persons or stakeholders are fit and proper (i.e, do not expose the NPO to abuse).
- d. Do you have appropriate, sound, internal financial and other oversight and verification controls? For example, appropriate delegations and separations of authority over the collection, handling, and depositing of cash and the issuing of receipts?

- e. Do you transfer money using normal banking mechanisms, wherever possible? When it is not, do you use reputable alternative systems, and have strong additional controls and audit trails to protect your NPO's funds and show how and when they were used?
- f. Do you know who uses your facilities and for what purpose? For example, your office or meeting space, name, bank account, credit cards, website, social media platforms, computer system, telephone etc. Do you know what they are saying, and what materials they are distributing or leaving behind?
- g. Do you try to find out who else might be supporting a person or cause that you are endorsing in public statements, and who uses your name as a supporter?
- h. For religious and FBOs, do you conduct internal risk assessment of your leaders and members around the nature of socio-political ideologies they may subscribe to? Are there mechanisms to proactively detect the FBO's members' support of terrorist groups, ideologies or activities? Is your organisation able to report such persons/activities to authorities, upon detection, without delay?
- i. Do you know where your donations and other support really come from?
- j. Do you know who has ultimate control over the project that your NPO's money and resources are benefiting? Do you know what the money and resources are used for, including after the particular project is finished?
- k. Do you know your partners in delivering the work you are doing, and their affiliations to other organisations?
- l. Do you have clear written agreements with agents/contractors/other partners, in Namibia and abroad, covering what activities will be undertaken and how they will be monitored and accounted for? Do you check that the agreements are being followed?

5.4 Risks Associated with High Risk Jurisdictions

All risk considerations and assessments as explained herein have to be mindful of jurisdictional risk levels. NPOs are required to consider the risk levels of jurisdictions which their members, donors, beneficiaries, directing staff or leaders, as well as destination of benefits (perhaps through delivery channels).

Jurisdictions have different risk levels which is informed by the prevalence of ML and TF threats on the one hand and vulnerabilities in control frameworks on the other. High risk jurisdictions may for example not have a NPO registration/licensing regime, or may not have otherwise introduced the full spectrum of preventive and combatting measures as required by the FATF Recommendations. The table below explain variables which influence the risk level of jurisdictions.

What increases jurisdictional TF risk?

Information about high-risk jurisdictions is widely available, which is detailed from several reliable open-source documents and media. The following are indications, based on credible sources, which may escalate the risk of a country that clients to a transaction may be associated with. Amongst other considerations, these are jurisdictions:

- a. that have been found by organisations such as FATF, World Bank, Organisation for Economic Cooperation and Development (OECD) and the International Monetary Fund as **not having effective AML/CFT/CPF measures** in place;*
- b. has been identified by domestic, regional or international body as a **jurisdiction that do not have or apply insufficient measures to counter the illicit dealing in arms or ammunitions**;*
- c. is subject to a **sanction, embargo or similar measure** issued by the United Nations Security Council*
- d. identified to be **uncooperative in extraditions and providing beneficial ownership information** to competent authorities, a determination which may be established from reviewing FATF Mutual Evaluation reports or reports by organisations that also consider various co-operation levels such as the OECD Global Forum reports on compliance with international tax transparency standards; and*
- e. **Identified higher risk countries**: this may include conflict zones, countries with active terrorism, countries subject to sanctions, embargoes issued by the international community including the UN, OFAC, EU etc. Also includes FATF greylisting or blacklisting.*

6. EXTERNAL RISK ASSESSMENTS AND TYPOLOGIES

The considerations and indicators herein are not exhaustive. NPOs are required to consider observations from typologies, sectoral risk assessment and NRA reports issued by the FIC. Local⁶ and international trends and typology reports issued by bodies such as ESAAMLG⁷ and FATF⁸ (available on their websites), equally help highlight changing risks broadly and related to the sector. To the extent possible, this guidance has incorporated lessons and best practices from international publications. ML and TF trends are dynamic, it is thus essential to keep abreast of updated publications in this regard.

7. FURTHER GUIDANCE ON CONTROLS

This Guidance Note deals with risk assessments as a foundational step for the implementation of an effective Risk Based Framework within NPOs. NPOs are further required to duly study Guidance Note 13 of 2023, amongst others, which speaks to the practical implementation of controls to mitigate ML/TF/PF risks at institutional level.

The FIC website contains several other Directives, Guidance Notes, Circulars and Regulations which avail helpful guidance on measures to combat ML/TF in terms of the FIA.

8. GENERAL

This Guidance may contain statements of policy which reflect the FIC's administration of the legislation in carrying out its statutory functions. This guidance is issued without prejudice to the FIA and its complementing Regulations. The information contained herein is intended to only provide a summary on these matters and is not intended to be comprehensively exhaustive.

⁶ Published on the FIC website under Risk Assessments folder while trends and typology reports are under Publications folder.

⁷ https://www.esaamlg.org/index.php/methods_trends

⁸ <https://www.fatf-gafi.org/en/publications.html>

9. NON-COMPLIANCE WITH THIS GUIDANCE

This document is a guide. Effective implementation is the sole responsibility of NPOs. Should a NPO fail to adhere to the guidance provided herein, it will be such NPO's responsibility to demonstrate alternative risk management controls implemented which are effective to the satisfaction of the FIC as supervisory authority in terms of the FIA.

10. GENERAL

The Guidance Note can be accessed at www.fic.na

DATE ISSUED: 30 JUNE 2023

DIRECTOR: FINANCIAL INTELLIGENCE CENTRE

FIC CONTACT DETAILS

All correspondence and enquiries must be directed to:

The Director, Financial Intelligence Centre

P.O. Box 2882

No. 71 Robert Mugabe Avenue, Windhoek

helpdesk@fic.na

ANNEXURE A: INDICATORS OF POTENTIAL HIGH RISKS

11. BACKGROUND



Indicators are used extensively in sectors where prevention is paramount, such as the business and medical sectors. Indicators can increase forewarning, helping to mitigate risks before they become reality, or help to detect existing abuse. While no cases of NPO abuse for terrorist purposes were observed in Namibia to date, principal *methods of operation* in the abuse of NPOs are universal as documented in the FATF Report⁹ on Risk of Terrorist Abuse. The report provides a comprehensive presentation of how NPO abuse can occur, and indicators of how such can be detected.

The elements that indicate existing abuse of an NPO, or substantial risk of abuse. Are listed herein below to help all stakeholders, including NPOs, competent authorities, government bodies, financial institutions, and designated non-financial businesses or professions (DNFBPs) identify and investigate possible cases of abuse within a particular NPO or the larger NPO sector. While the list of indicators presented here is substantial and transnational in nature, it is not complete; there are likely additional indicators that are unique to particular contexts.

12. THE NATURE OF INDICATORS

Indicators are ultimately leads that require further investigation to assess the nature or risk of abuse. This said, not all indicators carry an equally strong certainty of a terrorism-related risk. For many of the indicators identified, referred to as ‘risk indicators,’ support to terrorism is a possible explanation, but not necessarily the only possible explanation. ‘Terrorist abuse indicators’, a smaller sub-set of indicators, denote a stronger relationship with terrorism-related activities. The table below provides further details on these two types of indicators.

⁹ <file:///F:/09%20November%202022/NPOs/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf> (2014)

 Risk Indicator	 Terrorist Abuse Indicator
<p>An aspect of an NPO's activities that suggests abuse or a risk of abuse that may be terrorism-related, but also has possible alternative explanations.</p>	<p>An aspect of an NPO's activities that suggests abuse or a risk of abuse that is directly related to terrorist activity. The presence of these indicators would lead to a stronger certainty that the abuse or risk is terrorism-related, as opposed to alternative explanations.</p>

12.1 General 'Risk Indicators'

Conventionally the general risk indicators herein below may suggest potential for risks such as fraud and theft of an NPO's assets though they cannot be completely discounted from potential TF.

12.1.1 Indicators Related to General Operations and Governance:

- a. NPO has unreported activities, programmes, or partners;
- b. NPO uses an unusually complex financial network for its operations;
- c. NPO avoids mandatory reporting requirements;
- d. NPO programmes and activities are vaguely explained to oversight or regulatory bodies;
- e. Third parties are used to open NPO bank accounts or carry out some transactions;
- f. NPO expenditures are not consistent with its programmes and activities;
- g. NPO is unable to account for the final use of all of its resources;
- h. NPO is unable to account for the origin of its income;
- i. NPO has inconsistencies in its accounting and/or mandatory reporting;
- j. NPO has opaque leadership or decision-making structures;
- k. NPO or NPO representatives use falsified or conflicting documentation;
- l. NPO transfers resources or conducts activities in an area where terrorist entities are known to have a substantial presence;
- m. NPO has unreported activities, programmes, or partners; and
- a. Falsified or conflicting documentation is used by an NPO or by NPO representatives.

12.1.2 Indicators Related to Financial Support to known or Suspected Terrorists:

- a. Use of cash couriers to transfer NPO funds into areas with known terrorist activity;*
- b. NPO transactions are structured to avoid transaction reporting;*
- c. Requests to transfer NPO funds are accompanied by vague justifications;*
- d. NPO uses a shell organisation as a funding conduit;*
- e. NPO representatives fail to declare large currency amounts at international borders;*
- f. NPO bank accounts are used by entities whose own accounts are under restrictions;*
- g. NPO funds are comingled with personal or private business funds;*
- h. Bank accounts related to some programmes or activities are concealed; and*
- i. NPO funds are transferred to entities not associated with declared programmes or activities.*

12.1.3 Indicators Related to Material Support to known or potential Terrorists:


- a. NPO procures dual-use equipment; and*
- b. NPO facilities are frequented by individuals believed to support terrorist activities.*

12.1.4 Indicators Related to Support for Recruitment:

- a. Individuals involved in terrorist activities are linked to an NPO; and*
- b. NPO publications or speakers support terrorism or terrorist entities.*

12.2 'Terrorist Abuse Indicators'

12.2.1 Indicators Related to General Operations and Governance:

- a. A lead from the public alleges that an NPO is engaged in activities related to terrorism;*
 - b. NPO merges with another organisation believed to support terrorist activities;*
- 

- c. *NPO humanitarian assistance is targeted towards supporting individuals directly linked to terrorist entities;*
- d. *Directing officials of an NPO are, or have been, directing officials of other organisations believed to support terrorist activity; and*
- e. *NPO suffers from an internal conflict, where one faction is known to be sympathetic or actively supportive towards terrorist entities.*
- a. *Existence of reliable information indicating an NPO or its representatives are linked to third parties that support or are engaged in terrorist activities; and*
- b. *Advertised NPO is fictitious.*

12.2.2 Indicators Related to Financial Support to known or Suspected Terrorists:

- a. *NPO funds are transferred to other entities believed to be engaged in, or supporting, terrorist activities;*
- b. *NPO receives funds from entities believed to support terrorist activities;*
- c. *Use of cash couriers to transfer NPO funds into areas with known terrorist activity;*
- d. *NPO transactions are structured to avoid transaction reporting;*
- e. *Requests to transfer NPO funds are accompanied by vague justifications;*
- f. *NPO uses a shell organisation as a funding conduit;*
- g. *NPO representatives fail to declare large currency amounts at international borders; and*
- h. *NPO bank accounts are used by entities whose own accounts are under restrictions.*

12.2.3 Indicators Related to Material Support to known or potential Terrorists:

- a. *Resources of an NPO are transferred to an entity known to be engaged in, or supporting, terrorist activity;*
- b. *NPO receives resources from an entity believed to support or be engaged in terrorist activities; and*
- c. *NPO shares property with another organisation believed to support terrorist activity.*

12.2.4 Indicators Related to Support for Recruitment:

- a. *Directing officials or employees of an NPO engage in activities that support recruitment to violence.*