REGISTRAR OF SOCIETIES

ROYAL BRUNEI POLICE FORCE

BEING RESILIENT

A GUIDE TO PROTECTING YOUR ORGANIZATION FROM THE THREAT OF TERRORISM FINANCING ABUSE

Introduction

While non-profit organisations (NPOs), like their for-profit counterparts, face numerous risks relating to both money laundering and terrorist financing, some NPOs face risks specific to terrorist financing abuse based on their unique characteristics and the vital activities that they conduct.

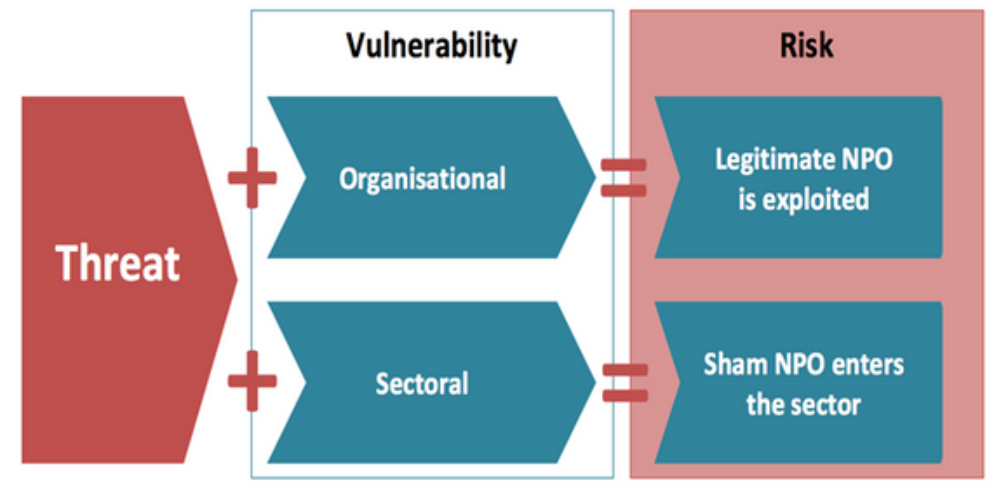
The purpose of this guidance document is to help those NPOs develop resilience to such terrorist financing threats by raising awareness within the sector

By so doing, organizations can ensure they have appropriate due diligence measures in place to counteract the threats posed to them by those terrorist entities that seek to abuse and manipulate the important contributions they make to society.

The Financial Action Task force defines Terrorist Financing Abuse as the exploitation by terrorists and terrorist organisations of NPOs to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support terrorists or terrorist organisations and operations.

Terrorism, and its precursor terrorism financing, are crimes where **PREVENTION IS PARAMOUNT**. A sector resilient to terrorist financing abuse, together with risk-based government oversight, will help prevent terrorist entities from abusing NPOs and their activities.

Risk



The Risk Equation model illustrates the relationship between a threat or threats, vulnerabilities, and the resulting risk posed to NPOs both at the Organizational and the Sectoral levels.

Risk Equation Model

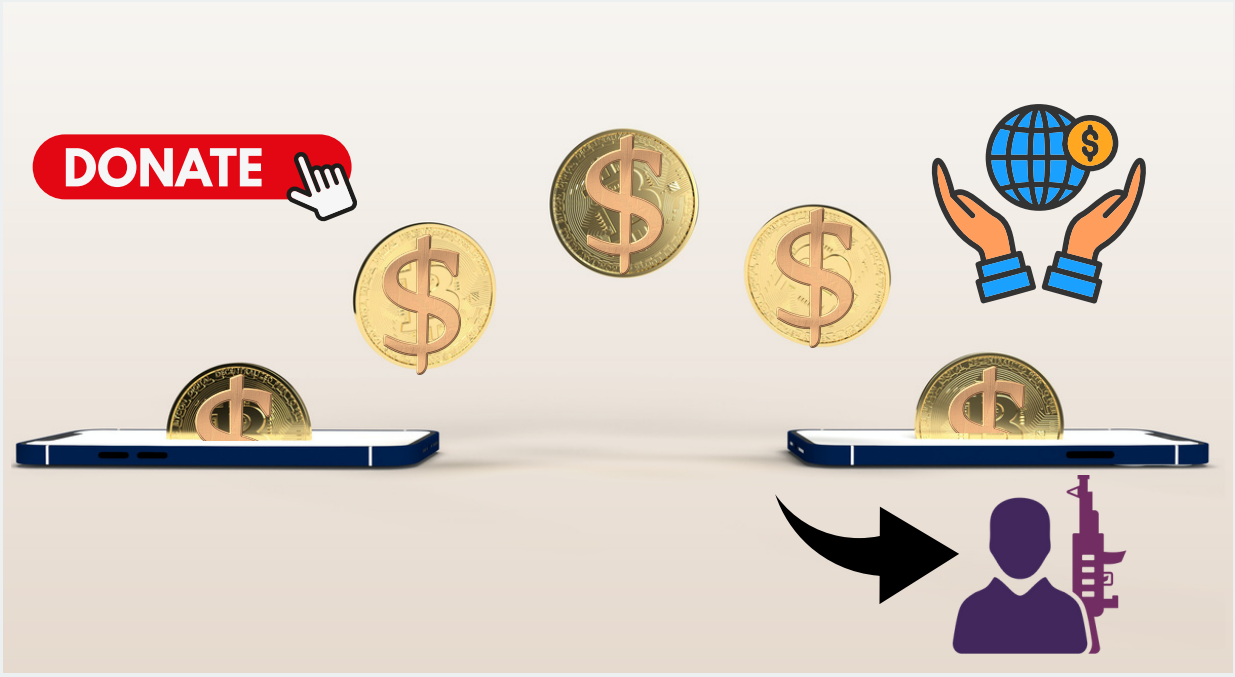
Threat

The Financial Action Task Force defines a Threat as a person or group of people, object or activity, with the potential to cause harm. A threat is dependent on actors that possess both the capability and intent to do harm, in this case, towards the NPO sector.

Vulnerability

The Financial Action Task Force defines a Vulnerability as things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities can exist at the organisational level or at the sectoral level. Organisational vulnerabilities are seen in cases where legitimate NPOs are abused by external actors or deceived by internal actors. Sectoral vulnerabilities are seen in cases where illegitimate organisations (commonly referred to as ‘sham’ NPOs) are allowed to enter the sector and take advantage of its benefits.

Threats posed by terrorist entities



Terrorist financiers engaged in the logistical support of terrorist organisations use funds to meet broad logistical requirements, which include but are not limited to, recruitment, travel and the acquiring of weapons.

The Interpretive Note for Recommendation 8 recognises this, stating that terrorist and terrorist organisations “exploit the NPO sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organisations and operations.

The NPO sector has interconnected vulnerabilities. The threat posed by terrorist entities seeks to exploit more than one type of vulnerability. These threats can be grouped into several categories:.

Threats

01 Diversion of Funds (Internal)

Diversion of funds (internal) occurs when an NPO, or an individual acting on behalf of an NPO who aspires to support terrorism, diverts funds to a known or suspected terrorist entity.

02 Diversion of Funds (External)

Diversion of funds (external) occurs when third-party associates of the NPO, such as external fundraisers or foreign partners, are diverting funds that are destined for, or provided by, an NPO.

03 Affiliation with a Terrorist Entity

Affiliation with a Terrorist Entity occurs when an NPO, or an individual acting on behalf of NPO, maintains an operational affiliation with a terrorist organisation or supporter of terrorism.

Threats

04 Abuse of Programming

Abuse of Programming occurs when NPO-funded programmes meant to support legitimate humanitarian purposes are manipulated at the point of delivery to support terrorism.

05 Support for Recruitment

Support for recruitment occurs when NPO-funded programmes or facilities are used to create an environment which supports and/or promotes terrorism recruitment-related activities.

06 False Representation and Sham NPOs

False representation occurs when under the guise of charitable activity, an organisation or individual raises funds and/or carries out other activities in support of terrorism.

Operational Vulnerabilities

Extended Logistical Networks

Logistical networks are the linkages through which NPOs collect, retain, transfer, and deliver resources related to their operational activities. Extended logistical networks give the NPO sector greater reach, allowing NPOs to deliver programmes in multiple areas through multiple partners.

Conversely, because of their scope, extended logistical networks also increase vulnerability. With more individuals, wider ranges of activities, and possibly substantial geographic distances involved, it can be challenging to maintain adequate control of resources.

For NPOs engaged in humanitarian work, logistical networks often flow through geographic areas of conflict or low governance. Also, there is an increased risk that resources will have to flow through other sectors where governance may be less stringent (for example, unregulated money service businesses). Both of these aspects increase the risk that resources can be diverted or that the delivery of programmes can be corrupted.

Operational Vulnerabilities

Large Transitory Workforce

TThe NPO sector also relies heavily on a large transitory workforce. Volunteers make up a significant and important portion of this workforce. The nature of the NPO sector workforce can make it difficult to scrutinise staff, particularly volunteers or foreign partners.

Additionally, for small and medium-sized NPOs, this type of workforce can make it difficult to attract and retain personnel that have technical expertise in risk assessment, compliance, and legal matters. These personnel pressures can lead to NPO activities going forward without adequate due diligence and safeguards in place, increasing the risk of abuse.

Operational Vulnerabilities

Operational Capacity

The NPO sector also possesses high operational capacity. The FATF noted that NPOs may be vulnerable because they "have access to considerable sources of funds and are often cash intensive. Furthermore, some NPOs have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity." The NPO sector is resource intensive and transnational in nature. These resources and associated logistical networks are valuable to terrorist movements if they can be exploited.

NPOs have a unique ability to reach people, particularly those in conflict areas or diaspora populations. Exploiting this unique access presents terrorist movements with an opportunity to recruit for their movements through the abuse of NPO recourses and programmes. A further important aspect of the operational capacity of NPOs is the public trust afforded to the sector. Because the sector has generally enjoyed high public trust, scrutiny of NPO activities has often been less consistent and robust than in other sectors.

For terrorist entities looking to minimise risk to their own operations and logistical networks, piggybacking on, or mimicking, legitimate NPOs has presented an attractive solution.

Operational Vulnerabilities

Organisational Culture

The final area of vulnerability pertains to organisational culture. The emphasis placed on values in some NPOs could contribute to poor decision-making and risk management.

Studies have examined the importance of values in non-profit organisations, and identified that for some organisations, value calculations represent the real 'bottom line.'

While this is not a consistent vulnerability, the tendency to trust external and internal actors may leave some NPOs vulnerable to abuse.

Best Practices to Protect Yourself

Organizational Integrity

NPOs are established and operate in accordance with a governing document, for example, articles of incorporation, a constitution, or bylaws that outline purposes, structure, reporting practices, and guidelines for complying with local laws.

Members of the governing board understand and act in the interest of the organisation. The governing board maintains oversight over the organisation by establishing strong financial and human resource polices, meeting on a regular basis, and actively monitoring activities.

Partner Relationships

To prevent the abuse of funds by partners, NPOs carry out appropriate due diligence on those individuals and organisations that the NPO receives donations from, gives money to or works with closely before entering into relationships or agreements.

NPOs verify partner reputations through the use of selection criteria and searches of publicly available information, including domestic and UN sanctions lists.

Written agreements can also be used to outline the expectations and responsibilities of both parties, which include detailed information as to the application of funds and requirements for regular reporting, audits and on-site visits.

Financial Transparency and Accountability

NPOs prevent financial abuse and misuse of resources and funds by establishing strong financial controls and procedures. For example:

- The governing board approves an annual budget and have a process in place to monitor the use of funds.
- NPOs keep adequate and complete financial records of income, expenses, and financial transactions throughout their operations, including the end use of the funds.
- NPOs clearly state programme goals when collecting funds and ensure that funds are applied as intended.
- Information about the activities carried out is made publicly available.
- NPOs are informed as to the sources of their income and establish criteria to determine whether donations should be accepted of refused.

Programme Planning and Monitoring

NPOs establish internal controls and monitoring systems to ensure that funds and services are being used as intended. For example:

- NPOs clearly define the purpose and scope of their activities, identify beneficiary groups, and consider the risks of terrorist financing and risk mitigation measures before undertaking projects.

- They maintain detailed budgets for each project and generate regular reports on related purchases and expenses.

- NPOs establish procedures to trace funds, services, and equipment, and carry out transactions through the banking system when possible, to maintain transparency of funds and mitigate the risk of terrorist financing.

- Project performance is monitored on a regular basis by verifying the existence of beneficiaries and ensuring the receipt of funds.

- NPOs take appropriate measures, based on the risks, to account for funds and services delivered

Risk Indicators

Indicators can increase forewarning, helping to mitigate risks before they become reality, or help to detect existing abuse. Not all indicators however carry an equally strong certainty of a terrorism-related risk.

Risk Indicators

Identify potential support to terrorism where it isn't necessarily the only possible explanation.

Terrorist Abuse Indicators

Identify a smaller sub-set of indicators, that denote a stronger relationship with terrorism-related activities.

The presence of terrorist abuse indicators would lead to a stronger certainty that the abuse or risk is terrorism-related, as opposed to alternative explanations.

Examples of Risk Indicators

01 NPO funds are transferred to entities not associated with declared programmes or activities.

NPO transfers resources or conducts activities in an area where terrorist entities are known to have a substantial presence. 02

03 NPO expenditures are not consistent with its programmes and activities.

NPO is unable to account for the final use of all of its resources. 04

05 NPO is unable to account for the origin of its income.

NPO has inconsistencies in its accounting and/or mandatory reporting. 06

07 NPO facilities conceal criminal activities.

Examples of Terrorist Abuse Indicators

01 NPO funds are transferred to other entities believed to be engaged in, or supporting, terrorist activities.

02 NPO receives funds from entities believed to support terrorist activities.

.

03 Resources of an NPO are transferred to an entity known to be engaged in, or supporting, terrorist activity.

04 NPO receives resources from an entity believed to support or be engaged in terrorist activities.

05 NPO shares property with another organisation believed to support terrorist activity.

06 The identities of proscribed terrorist entities are found to match the identities of NPO directing officials or employees.

07 Directing officials of an NPO are, or have been, directing officials of other organisations believed to support terrorist activity.

Examples of Terrorist Abuse Indicators

08 NPO suffers from an internal conflict, where one faction is known to be sympathetic or actively supportive towards terrorist entities.

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

.

10 Criminal activities consistent with terrorist operations are concealed in NPO facilities.

11 NPO directing officials or employees are engaged in other criminal activities consistent with terrorist operations.

Please Note: These are not exhaustive lists of Risk Indicators and Terrorist Abuse Indicators. For a more comprehensive list, please refer to the FATF typologies report entitled Risk of Terrorist Abuse in Non-Profit Organisations – June 2014.

Summary

The importance of the NPO sector to domestic and international communities cannot be overstated. It is a vibrant sector, providing innumerable services to millions of people. However, after nearly 20 years since the abuse of NPOs by terrorists and terrorist organisations was formally recognised as a concern, the threat of terrorist financing abuse to the sector remains and NPOs continue to be misused and exploited by terrorist entities. The exploitation of a sector devoted to good works by entities intent on harming innocents is a particularly egregious form of abuse that fundamentally undermines public trust in the sector.

Governments are challenged to develop appropriate and risk-based mechanisms of oversight to protect NPOs from terrorist financing abuse. This guidance is focused on raising awareness of the threat so that organizations themselves can put their own operational safeguards in place to ensure resilience to terrorist financing abuse

This guidance document was put together by relying on the FATF's typologies report on the Risk of Terrorist Abuse in Non-Profit Organisations – June 2014. and the FATF's Best Practices paper on Combating the Abuse of Non-Profit Organisations (Recommendations 8) – June 2015