NON-PROFIT ORGANISATION SECRETARIAT

PROMOTING ACCOUNTABILITY, INTEGRITY AND PUBLIC CONFIDENCE IN THE NPO SECTOR

A Guide to Protecting Ghana Non-Profit Organizations from the Threat of Terrorism Financing Abuse

NPO | DECEMBER, 2025

PROMOTING ACCOUNTABILITY, INTEGRITY AND PUBLIC CONFIDENCE IN THE NPO SECTOR

A Guide to Protecting Ghana Non-Profit Organizations from the Threat of Terrorism Financing Abuse

TABLE OF CONTENT

NON-PROFIT ORGANISATION SECRETARIAT

LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering/ Countering the Financing of Terrorism
FIC	Financial Intelligence Centre
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
JEM	Jaish-e-Mohammed
ML	Money Laundering
NPO	Non-Profit Organisation
PF	Proliferation Financing
TF	Terrorism Financing
UN	United Nations
KYD	Know Your Donor
NRA	National Risk Assessment
STR	Suspicious Transaction Report
NPOS	Non-Profit Organization Secretariat

FOREWORD

Non-Profit Organisations (NPOs) play an indispensable role in Ghana's national development by supporting vulnerable populations and contributing to progress in areas such as social protection, education, health, humanitarian relief, and community development. Through their interventions, NPOs complement government efforts and provide essential services to communities across the country, particularly in areas that may otherwise be difficult to reach.

However, as the NPO sector continues to expand in scope, scale, and operational reach, it has also become increasingly important to safeguard the sector from potential misuse. Global experience and international studies have demonstrated that certain segments of the NPO sector may be vulnerable to exploitation by criminal and terrorist actors seeking to raise, move, or conceal funds intended to support terrorist activities. Such abuse undermines the credibility of legitimate organisations and threatens the trust that communities, donors, and partners place in the sector.

The Government of Ghana remains firmly committed to protecting the integrity of the NPO sector while ensuring that legitimate organisations can continue their valuable work without undue restrictions. In pursuit of this objective, Ghana has strengthened its Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) framework in line with international standards, particularly those established by the Financial Action Task Force (FATF). These efforts include legislative reforms, national risk assessments, and the implementation of regulatory and supervisory measures aimed at addressing terrorism financing risks within the NPO sector.

The establishment of the Non-Profit Organisation Secretariat (NPOS) under the Ministry of Gender, Children and Social Protection represents a significant step toward enhancing coordination, regulation, and support for Non-Profit Organisations in Ghana. The Secretariat is mandated to promote transparency, accountability, and compliance within the sector while facilitating constructive engagement between government and civil society organisations.

This Guide to Protecting Ghana Non-Profit Organisations from the Threat of Terrorism Financing Abuse has been developed as part of these national efforts. The guide is intended to raise awareness among NPOs about the potential risks of terrorism financing abuse and to provide practical guidance on governance, financial transparency, due diligence, and internal controls. By promoting sound management practices and strengthening organisational safeguards, the guide seeks to empower NPOs to protect themselves from misuse while maintaining the trust of the public and the confidence of donors and partners.

The successful implementation of the principles and best practices outlined in this guide will depend on continued collaboration between the NPO Secretariat, Non-Profit Organisations, the Financial Intelligence Centre, development partners, and other relevant stakeholders. Through collective commitment and shared responsibility, Ghana can ensure that the NPO sector remains resilient, transparent, and fully capable of continuing its important contribution to national development.

Government remains dedicated to fostering a vibrant and accountable Non-Profit Organisation sector that operates with integrity, upholds public confidence, and continues to serve the interests of the Ghanaian people.

DR. AGNES NAA MOMO LARTEY (MP)

....

Minister for Gender, Children and Social Protection

NON-PROFIT ORGANISATION SECRETARIAT

01

INTRODUCTION

Non-Profit Organisations (NPOs) play a vital role in providing charitable services to those in need and contributing to constructive debate that is essential to any flourishing society.

While 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 (TF) abuse based on their unique characteristics and the vital activities that they conduct.

Financial Action Task Force through its typology studies has shown that NPOs have been involved in terrorism financing schemes. Terrorist organisations have been known to infiltrate

NPOs to raise funds and use NPOs logistical networks to fund recruitment, travel and the acquisition of weapons.

Criminal organisations use all sectors of the economy, including NPOs, to launder their “dirty” money. By using an NPO as a front, criminals can make their ill-gotten funds appear legitimate.

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

PURPOSE/OBJECTIVE OF GUIDELINE

The purpose of this guidance document is to help NPOs develop resilience to such ML/TF threats by raising awareness within the NPO sector. The more specific objectives are to:

- Promote accountability, transparency and public confidence in the NPO Sector.
- Serve as a tool for preventing TF abuses in the NPO sector.
- Guide NPOs to strengthen their internal controls to guard against TF.
- Create awareness among their employees, volunteers and other
- stakeholders regarding best practices to combat TF.

By implementing the best practices outlined in this document, organizations can ensure they have appropriate due diligence measures in place to counteract the threats posed to them by those criminals and terrorist entities that seek to abuse and manipulate the important contributions NPOs make to society.

NON-PROFIT ORGANISATION SECRETARIAT

03

INTERNATIONAL CONTEXT

The Government of Ghana has been working to strengthen the Non-Profit Organisation (NPO) sector to meet its international anti-money laundering and countering the financing of terrorism (AML/CFT) obligations as defined by the Financial Action Task Force (FATF).

FATF 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.***

FATF requirements for NPO

a. Identify which subset of organizations fall within the FATF definition of NPO.

b. Identify the features and types of NPOs which by their activities or characteristics, are likely to be at risk of terrorist financing abuse

c. Identify the nature of threats posed by terrorist entities to the NPOs that are at risk as well as how terrorist actors abuse those NPOs.

NON-PROFIT ORGANISATION SECRETARIAT

04

NATIONAL EFFORTS

Ghana is committed to combating TF and its negative impact on its citizens. Ghana has adopted a series of legislative and regulatory measures including the Anti-Money Laundering Act (2020) and the Anti-Terrorism Act (2008) and their corresponding regulations that provide the foundation for Ghana's fight against TF.

The government has also published a National Non-Profit Organisation Policy as well as Directives for the Management of Non-Profit Organisations Operations in Ghana which promote accountability, transparency, and public confidence in the NPO Sector which are core components of the fight against TF.

NON-PROFIT ORGANISATION SECRETARIAT

05

KEY AML/CFT ORGANISATIONS IN GHANA

The following organisations play a key role in the fight against TF.

NPO SECRETARIAT

In the context of these efforts to strengthen the NPO sector the government has recently established the Non-Profit Organisation Secretariat. The functions of the NPO Secretariat are as follows:

a. advise the sector minister on policy and the promotion of the non-profit sector;
b. license NPOs;
c. establish standards, guidelines and codes of practice for NPOs;
d. monitor the activities of NPOs in order to ensure observance of the provisions of this Policy;
e. ensure the promotion of NPOs in the public interest and the observance of high standards of accountability, transparency and compliance with law;
f. liaise between NPOs and the government;
g. perform other functions related to the object of the Policy/Directives.

FINANCIAL INTELLIGENCE CENTRE (FIC)

The FIC is the National Centre for the receipt and analysis of suspicious transaction reports and other information relevant to predicate offences of Money Laundering/ Terrorist Financing and Proliferation Financing (ML/TF&PF) and to disseminate actionable intelligence to competent authorities.

NON-PROFIT ORGANISATION SECRETARIAT

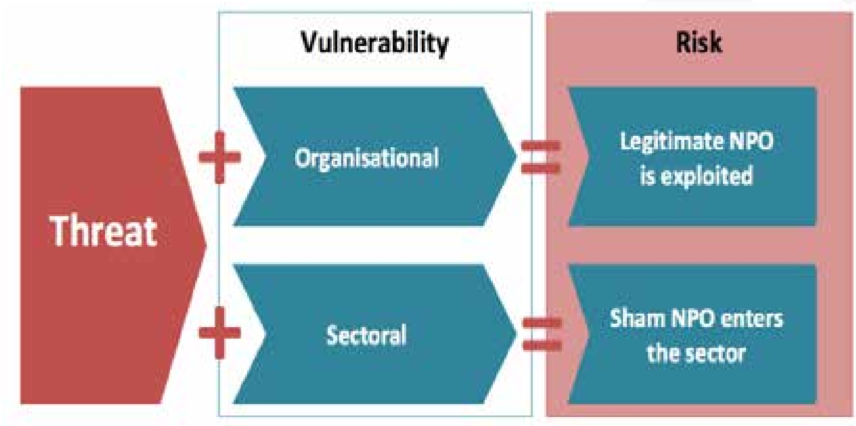
06

UNDERSTANDING TF RISK IN THE NPO SECTOR

The following '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.

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. In the context of terrorism financing the threat stems for terrorist groups who may be operating in your region or using NPOs to funnel money to finance their operations.

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.



This guidance will be focused on raising awareness of the risk at the organizational level to help individual organizations become resilient to the threat of terrorist financing abuse.

NON-PROFIT ORGANISATION SECRETARIAT

Money Laundering and Terrorism Financing Risk for NPOs in Ghana

Ghana conducted a Money Laundering and Terrorism Financing National Risk Assessment (NRA) in 2018 and 2024, with a view of understanding its ML/TF risks and complying with the FATF Recommendation. Furthermore, a detailed ML/TF risk assessment of the NPO sector was conducted in 2016 in addition to the NRA. The NPO sector was evaluated as having **a medium money laundering and terrorism financing risk.**

The threats facing the NPO sector related to ML are fraud, forgery, stealing, the risk of receiving donor funding from high-risk jurisdictions and suspected tax evasion through an NPO. In the case of suspected tax evasion, sham organizations were incorporated as NPOs to avoid the payment of taxes.

The Terrorism Financing (TF) threat to the sector mainly arises from foreign NPOs linked to high-risk jurisdictions, NPOs operating near Ghana's northern borders, and service-type NPOs in faith-based, humanitarian, and educational fields, which the 2024 NRA identified as FATF-defined NPOs.

METHODS USED BY TERRORIST AND CRIMINAL ORGANISATIONS TO EXPLOIT THE NPO SECTOR

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 FATF 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 methods used and risks posed by terrorist entities seek to exploit more than one type of vulnerability. Most the methods used are linked to breaches of integrity and ethics that can be exploited by terrorist and criminal organizations. These methods can be grouped into the following categories:

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.

Case Study #1: Diversion of Funds by Actors Internal to NPO

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.

Collection Phase

An investigation by the national Financial Intelligence Unit 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.

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.

Case Study #2: Diversion of Funds by Actors External to NPOs

A domestic NPO was established to support charitable work in foreign areas of conflict.

Transfer Phase

An investigation by the national FIU, initiated by suspicious transaction reporting, revealed that locally collected funds were being transmitted to foreign-based charitable organisations. The investigation also uncovered that, once the funds were received by the foreign-based charitable organisations, they were systematically passed on to persons or organisations which were part of, or affiliated with, a known terrorist organisation.
While there were established connections between the foreign-based charitable organisations and the terrorist organisation, direct links between the domestic NPO and the terrorist organisation could not be substantiated.

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.

Case Study #3: Affiliation with a Terrorist Entity

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

Delivery of Programmes Phase

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.

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.

Case Study #5: Abuse of Programming

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.

Delivery of Programmes Phase

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.

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.

Case Study #6: Support for Recruitment

On 4 November 2010, Al Rehmat Trust, an NPO operating in Pakistan, was designated pursuant to Executive Order in the United States for being controlled by, acting on behalf of, and providing financial support to designated terrorist organisations, including al Qaida and affiliated organisations.

Delivery and Transfer Phases

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 United Nations 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 terrorist activities in Afghanistan. Al Rehmat Trust has also been involved in fundraising for JEM, including for militant training and indoctrination at its mosques and madrassas. As of early 2009, Al Rehmat Trust 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.

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.

Case Study #7: False Representation

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.

Collection Phase

The individuals in question did not have the consent of the domestic NPO to solicit donations on its behalf nor did they deliver 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.

OPERATIONAL VULNERABILITIES

Breaches in integrity and ethics

Breaches in integrity and ethics can be present in both for profit and non-profit organisations alike. Terrorist and criminal organisations will exploit weak integrity and ethical practices by providing individuals associated with NPOs with monetary and other incentives then use the NPO as front for their criminal activities.

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 businesses).
Both of these aspects increase the risk that resources can be diverted or that the delivery of programmes can be corrupted.

Large transitory workforces

The NPO sector also relies heavily on a large transitory work-force. 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 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 diasporas. 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, leveraging or mimicking, legitimate NPOs has presented an attractive solution.

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.' In their desire to make a contribution some NPOs might put less of a priority on financial integrity and good governance.

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

The following section outlines best practices that can assist NPOs in protecting themselves. The best practices are grounded in principles of integrity and ethics. A best practices checklist has been included at Annex A that summarises the practices outlined in this section.

Good Governance

At the heart of protecting yourself from abuse is the implementation of good governance practices. The foundation of good governance starts with the board and senior management clearly expressing its commitment to transparency and prevention of terrorism financing. Best practices include:

- Establishing adequate measures to clearly identify every board member, both executive and non-executive.
- Commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the AML/CFT objectives.
- Based on a risk-based approach, consider forming an independent oversight committee of its operations recognizing that each NPO must select the oversight structure which best suits its needs.

NON-PROFIT ORGANISATION SECRETARIAT

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 policies, meeting on a regular basis, and actively monitoring activities.

Know your employees

NPOs maintain records of particulars of its employees (both from Ghana or foreign nationals), including but not limited to permanent address, present address, copy of national identification card, passport number, nationality, personal email, phone or mobile number, past experience, etc.

Every potential employee should be screened, whether permanent or temporary. NPOs check the work history of employees by taking up references, calling referees and probing their previous jobs. For senior-level and finance positions, NPOs carry out enhanced checks, including criminal history and financial background.

Finally, management should be alerted to changes in employee's lives which might put them under increased pressure from terrorist financiers or other criminal organisations.

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.

Know Your Beneficiaries and Partners

NPOs should have a good understanding of their beneficiaries and partners. They should ascertain correct and complete identification particulars of their beneficiaries (person, group of persons or organization etc.) who receives cash or services or in-kind contributions.

In case the beneficiary is an organization/ group of persons, donor NPOs must have knowledge of detailed profile and particulars of such organization. The NPOs should ensure that the beneficiaries are not linked with any suspected terrorist activity or any link with terrorist support networks.

In instances where the projects are implemented through partnership agreements with other partners, NPOs should make it a part of their project agreements that partners maintain and share beneficiaries' information. They may also share insights about beneficiary organizations or sectors.

NPOs should also ensure that the partner organizations have not had their license revoked by the NPO Secretariat or registration cancelled by other authorities.

Know Your Donors

Knowing your donors and the origin of funds you received is an important component of ensuring your NPO is not being misused. Before receiving funds from a donor, NPOs should establish that the donor is not placed on the United Nation's list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo exists.

NPOs should undertake best efforts to document the identity of their significant donors including collecting and maintaining identification details of major donors.

NPOs should conduct, on a risk-based approach, a reasonable search of public information, including information available on the Internet, to determine whether the donor or their key employees, board members or other senior managerial staff are suspected of being involved in activities relating to terrorism, including terrorist financing.

NPOs may refuse a donation or offer if they are unsure about its legitimacy.

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 or 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

NON-PROFIT ORGANISATION SECRETARIAT

27

GENERAL 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. These indicators can assist you in determining whether a transaction is suspicious and should be reported to the NPO Secretariat.

General risk indicators identify potential support to terrorism where it is necessarily the only possible means is 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 toalternative explanations.

Reporting to the NPO Secretariate NPOs should report to the NPOS when they suspect that a donation or activity may be related to money laundering or terrorism financing.

NON-PROFIT ORGANISATION SECRETARIAT

General risk Indicators

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, such as:

- 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.
- NPO expenditures are not consistent with its programmes and activities.
- NPO is unable to account for the final use of all of its resources.
- NPO is unable to account for the origin of its income.
- NPO has inconsistencies in its accounting and/or mandatory reporting.
- NPO facilities conceals criminal activities.

Donation risk indicators

- Unusual or substantial one-time donations are received from unidentifiable or suspicious sources
- A series of small donations are received from sources that cannot be identified or checked

- Conditions attached to a donation are as such that NPO would merely be a vehicle for transferring funds from one individual or organization to another individual or organization
- There are strange, inappropriate or illegal conditions
- Where donations are made in a foreign currency or foreign sources where financial regulation or the legal framework is not as rigorous
- Where there are complex banking or transfer arrangements
- Where donations are conditional to be used in partnership with particular individuals or organizations where the NPO has concerns about those individuals or organizations
- Where an NPO is asked to provide services or benefits on favorable terms to the donor or a person nominated by the donor
- Where payments received from a known donor but through an unknown party
- Where donations are received from unknown or anonymous bodies
- Where payments received from an unusual payment mechanism where this would not be a typical method of payment.

Beneficiary risk indicator

- Where NPO provides financial assistance, services or support on the basis of a certain sum of money per beneficiary and the numbers are relatively high
- Where an NPO provides services to large numbers of beneficiaries, where it may be easier to disguise additional beneficiaries

- Where there may appear signs that people may have been placed on distribution and aid lists by providing kickbacks and bribes to officials
- Lists of beneficiaries contain multiple manual corrections, multiple names may appear, may contain more family members
- Evidence that third parties or intermediaries have demanded payment for recommending or nominating beneficiaries
- Fake or suspicious identity documents
- Beneficiaries with identical characteristics and addresses or multiple identical or similar names and signatures
- Unexpected changes to beneficiaries details, for instance, sudden change of bank account or contact person or sudden toppage in replying to correspondence
- Significant increase in costs or amounts being claimed against the donation
- Attempting to trigger a phased payment through submission of incomplete documents
- Failure of beneficiary to account for all or most of the funds spent and failure to provide sufficient proof of expenditure
- Failure of beneficiary to maintain sufficient financial controls in place

Partnership risk indicators

- The project proposal is vague or lacks adequate financial or technical details
- The structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details
- The proposals include delegating work to other unknown partners or newly formed organizations

- It is difficult to contact the partner at their main address, or their telephone numbers are not working
- The project involves unusual payment mechanisms, or requests for cash, or for money to be paid into an account not held in the name of the partner, or in a country in which the partner is not based and not where the project is being carried out
- Partners request unnecessary or unusual levels of privacy and secrecy
- Requests by partners to use a particular auditor or accountant
- Employee risk indicators
- Indications that staff may be living beyond their means or appearing at unusual times
- Staff carrying out tasks or jobs they should not be, or other unusual staff behavior or conduct
- Sudden or increased staffing costs
- Exaggerating or falsifying expenses or overtime
- An aggressive or bullying manner that makes colleagues unwilling to challenge their behaviour
- An unwillingness to take holidays or be away from the office for more than a day or two at a time
- Asking to use someone else's log-in details because they have forgotten their password
- Monitoring of project risk indicators
- Invoices and paperwork have been tampered with, altered in
- crucial aspects with handwritten amendments
- Inventory shortages
- There is a lack of evidence to show fair and transparent tendering or procurement procedures

- Invoices and papers recording a higher cost for goods or s ervices than expected or agreed
- Missing key documents or only copies can be produced, which raise suspicions perhaps because they are poor copies or because key details are illegible or have been altered
- Signatures confirming receipt or payment are missing or the invoice is unsigned or undated
- Receipts have been signed and dated a long time after the goods or services should have been delivered
- Particularly late or early invoicing
- Repeated excuses of system crashing, losing records or paperwork
- Relief, goods, or items provided by the NPO in connection with the project have been tampered with
- Documents accompanying goods and items are missing
- The local community is receiving aid or assistance by other unexplained or unexpected means
- Unexpected transactions, where commission charged, or no receipts are available
- Figures in documents or records that look familiar or may be repeated
- Discrepancies between budgeted needs and payments requested
- Requests for payment in cash to be made to an unknown third party or other organization
- Payment of administration costs not appearing to relate to the project, or which appear unusually high taking into account the nature of the project.
- Cash advances and payments that are unusually frequent and/or have not been recorded or approved
- Funds are not being banked or accounted for

TERRORIST ABUSE INDICATORS

Terrorist abuse indicators

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, such as:

- NPO funds are transferred to other entities believed to be engaged in, or supporting, terrorist activities.
- NPO receives funds from entities believed to support terrorist activities.
- Resources of an NPO are transferred to an entity known to be engaged in, or supporting, terrorist activity.
- NPO receives resources from an entity believed to support or be engaged in terrorist activities.
- NPO shares property with another organisation believed to support terrorist activity.
- The identities of prescribed terrorist entities are found to match the identities of NPO directing officials or employees.

- Directing officials of an NPO are, or have been, directing officials of other organisations believed to support terrorist activity.
- NPO suffers from an internal conflict, where one faction is known to be sympathetic or actively supportive towards terrorist entities.
- Directing officials or employees of an NPO engage in activities that support recruitment to violence.
- Criminal activities consistent with terrorist operations are concealed in NPO facilities.
- 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 – November 2023.

NON-PROFIT ORGANISATION SECRETARIAT

CONCLUSION

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 as it continues to be misused and exploited by terrorist entities and criminals. 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 NPO sector.

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

Annex A. Non-Profit Organisation Best Practices Checklist

Internal controls and policies and procedures
• Policies and procedures have been established
• The level of detail in the policies and procedures reflect the complexity of operation of the NPO
• The policies promote accountability, integrity and public confidence
• Policies and procedures are fully understood by staff and volunteers
• Policies and procedures cover all applicable NPO requirements (for higher risk sub-sectors)
• A policy on knowing your employee (including criminal history and financial background) has been developed
Procedures on managing partnerships include: - Verifying UN/third party lists https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list - Record keeping on major partners - Public information verification - Policy to refuse donations
• Senior management understand what the legislative measures and directives for the NPO sector require
• Policies and procedures indicate how changes in legislative and regulatory requirements will be integrated

• Policies and procedures indicate how often they will be updated
• Policies and procedures are adopted by operations located outside of the head office
• Policies and procedures are adopted regarding on-going monitoring of transactions for higher risk NPOs
• The NPO clearly define the purpose and scope of its activities, identify beneficiary groups, and consider the risks of terrorist financing and risk mitigation measures before undertaking projects.
• The NPO maintain detailed budgets for each project and generate regular reports on related purchases and expenses
• The NPO 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
• The NPO monitors project performance on a regular basis by verifying the existence of beneficiaries and ensuring the receipt of funds
• The NPO take appropriate measures, based on the risks, to account for funds and services delivered?

Financial Controls
• Governing Board approves the annual budget and has a process in place to monitor the use of funds
• The NPO makes information about the activities carried out publicly available
• The NPO keeps adequate and complete financial records of income, expenses, and financial transactions throughout their operations, including the end use of the funds
• The NPO clearly state programme goals when collecting funds, and ensure that funds are applied as intended
• The NPO is informed as to the sources of their income and establish criteria to determine whether donations should be accepted or refused

Reporting to Non-Profit Organisation Secretariat (NPOS)
• The NPO uses ML/TF criteria to detect Suspicious Activity
• Suspicious Transaction Reports are immediately reported to the NPOS
• STR are reported in the prescribed manner
• STR are accompanied by copies of all documentation directly relevant to the suspicion
• The NPO responds in a timely manner to requests made by the NPOS.
• The NPO has procedures to ensure that there is no tipping off that an STR has been reported
• Higher risk NPOs have established on-going monitoring of transactions

NON-PROFIT ORGANISATION SECRETARIAT

Corporate Governance
• NPO has a functioning oversight body (Board, steering committee)
• The Board/Committee meets at least 3 times a year
• The minutes of Board/Committee meetings are comprehensive
• Audited statements are submitted annually and are comprehensive
• Activities are in line with stated purpose and objectives
• Beneficial ownership information on senior officers, board members and trustees is kept up to date

TF/PF Sanctions Monitoring
• NPO monitors watch lists related to terrorism financing, money laundering and proliferation financing https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
• Policies and procedures are developed for watch list monitoring
• Funds and assets related to terrorism or proliferation financing are frozen and reported to the FIC.
• Countermeasures and enhanced due diligence is applied to countries listed by the FATF http://www.fatf-gafi.org/countries/#high-risk

This guidance document was put together by relying on the FATF's typologies report on the Risk of Terrorist Abuse in Non-Profit Organisations – November 2023 and the FATF's Best Practices paper on Combating the Abuse of Non-Profit Organisations (Recommendations 8) – November 2023

UK International Development
Partnership | Progress | Prosperity

SOC-G
TACKLING SERIOUS AND ORGANISED CRIME - GHANA

Non-Profit Organisation Secretariat
Ministry of Gender Children and Social Protection
P.O.Box MBO 186
Ministries-Accra
Website: npos.mogcsp.gov.gh
Email: info.npos@mogcsp.gov.gh
Tel: +233 36 219 6905