GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FIUTT REFERENCE: GN/003/2025

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO

Ministry of Finance

COUNTER FINANCING OF TERRORISM GUIDANCE FOR NON-PROFIT ORGANISATIONS

28 October, 2025

Purpose

This Guidance is intended to provide assistance to Non-Profit Organisations monitored by the Financial Intelligence Unit of Trinidad and Tobago.

CONTENTS

TABLE OF ACRONYMS

ACRONYM	FULL FORM
CFT	COUNTER FINANCING OF TERRORISM
FATF	FINANCIAL ACTION TASK FORCE
FIUTT	FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO
NPOs	NON-PROFIT ORGANISATIONS
NPO ACT	NON-PROFIT ORGANISATIONS ACT, 2019
NRA2	2ND NATIONAL RISK ASSESSMENT
RBA	RISK-BASED APPROACH
RGD	OFFICE OF THE REGISTRAR GENERAL'S DEPARTMENT
TF	TERRORIST FINANCING

1. INTRODUCTION

1. Non-Profit Organisations ("NPOs") are integral to the social, cultural and humanitarian fabric of Trinidad and Tobago. Their invaluable efforts often rooted in altruism and community service, extend across borders and sectors, making them fundamental agents of positive change. NPOs are undoubtedly regarded as pivotal catalysts as they provide indispensable services to underprivileged groups and fervently advocate for human rights. Notwithstanding the significance of this sector, some services and good works have the potential to be exploited by terrorist actors to facilitate and finance terrorist acts and terrorism.

2. Terrorism refers to the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political, ideological, or religious objectives. Terrorist financing ("TF") involves the collection or provision of funds with the intention that they be used to support terrorist acts or terrorist organisations.

3. TF abuse of NPOs refers to 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.[1] While NPOs play a vital role in humanitarian and development efforts, their global reach and financial activities can be vulnerable to abuse by individuals or groups seeking to fund terrorism. It is therefore essential for NPOs to understand these risks and implement safeguards to protect their operations, reputation, and the communities they serve.

4. Not all NPOs are at risk of abuse by terrorists, therefore, when applying counter measures, a "one size fits all" approach cannot be adopted. As such, Trinidad and Tobago has amended its laws to better identify and provide support to NPOs who may be vulnerable to TF abuse, without disrupting legitimate NPO activities.

5. As at 15 August, 2025, NPOs are no longer considered Listed Businesses in Trinidad and Tobago. Additionally, in accordance with section 4 of the Non-Profit Organisations Act, 2019 ("NPO Act")[2], as amended, the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT") is the Oversight Authority responsible for counter financing of terrorism ("CFT") oversight and monitoring of NPOs which have the following characteristics:
    (i) meet the Financial Action Task Force ("FATF") definition; and
    (ii) have been identified as having a risk of TF abuse through an NRA or other risk assessment conducted by the FIUTT.

[1] Paragraph 8, FATF (2023), BPP-Combating the Terrorist Financing Abuse of Non-Profit Organisation, FATF, Paris, www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

[2] The Non-Profit Organisations Act was amended by section 8 of the Miscellaneous Provisions [Proceeds of Crime, Anti-Terrorism, Financial intelligence Unit of Trinidad and Tobago, Securities, Insurance, Non-Profit Organisations, the Civil Asset Recovery and Management and Unexplained Wealth and Miscellaneous Provisions (FATF Compliance)] Act, 2024. This section was proclaimed on 15 August, 2025 via Legal Notice 283 of 2025.

2. DOES THIS GUIDANCE APPLY TO YOU?

6. The NPO Act defines an NPO as a body of persons, whether incorporated or unincorporated, which is established primarily for the promotion of a patriotic, religious, philanthropic, charitable, educational, cultural, scientific, literary, historical, artistic, social, professional, fraternal, sporting or athletic purpose, or some other useful object and raises or disburses funds for that purpose or object. All such NPOs must be registered with the Office of the Registrar General's Department (RGD) pursuant to section 5(3) of the NPO Act.

7. However, in accordance with section 4 of the NPO Act, as mentioned previously, only those NPOs which (i) **meet the FATF definition;** and (ii) have been **identified as having a risk of TF abuse** through a national risk assessment (NRA) or other risk assessment conducted by the FIUTT, will be subject to oversight and monitoring by the FIUTT.

(i) NPOs within the FATF definition

8. The FATF has adopted a definition of NPO premised on the characteristics of the organisation which may make it more susceptible to TF abuse.

> **According to the FATF, an NPO is a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as:**
>
> - **charitable,**
> - **religious,**
> - **cultural,**
> - **educational,**
> - **social or**
> - **fraternal purposes, or**
> - **for the carrying out of other types of *"good works"*.**

Box *1: FATF NPO Definition*

(ii) NPOs identified as having a risk of TF abuse through an NRA or other Risk Assessment conducted by the FIUTT

9. Trinidad and Tobago conducted its 2nd National Risk Assessment (NRA2) and in June 2025, published the Trinidad and Tobago Public NRA2 Report[3]. The results of the assessment showed that the overall NPO sector has a low exposure of terrorism and TF abuse, while charitable, social and religious NPOs were observed to be vulnerable to *potential* misuse for TF abuse.

[3] 2nd National Money Laundering and Terrorism Financing Risk Assessment (NRA), June 2025

10. It is imperative to note that such vulnerability does not mean that these types of NPOs are being misused. Instead, such NPOs should implement measures, on a case-by-case basis, to mitigate these vulnerabilities depending on the level of exposure to the potential misuse by terrorist actors and organisations.

    N.B. Once an NPO submits its application documents to the -RGD- it **does not **need to register with the FIUTT**. The FIUTT will receive the relevant information from the RGD, conduct its assessment of the information, having regard to the two (2) characteristics cited at paragraphs 8 and 9, and determine whether the NPO should be subject to the FIUTT's Oversight. An NPO which is subject to the FIUTT's Oversight will receive a letter of introduction from the FIUTT and will be required to adhere to this Guidance Note.*

11. Once the criteria are met at paragraphs 8 and 9and NPOs determine that this guidance is applicable, NPOs can protect themselves from TF abuse by:
    a. understanding the potential TF risk at an individual NPO level;
    b. understanding the TF risk at the national level (NRA) and at a sectorial level;
    c. applying self-regulatory measures, where available; and
    d. implementing internal controls and good governance measures at an individual NPO level.

3. TAKING A RISK BASED APPROACH TO COUNTER TERRORIST FINANCING

12. TF risk in relation to NPOs refers to the potential of these organisations to be exploited—intentionally or unintentionally—to raise, move, or provide funds that support terrorist activities. Abuse of NPOs can take several forms. For example, funds raised for charitable purposes may be diverted to support terrorist activities, donations may be solicited under false pretences or through deceptive campaigns, terrorist groups may establish sham NPOs or infiltrate NPOs to create a façade of legitimacy and humanitarian aid and services may be redirected to benefit terrorist actors.

13. In order to understand the TF risks faced, NPOs should first identify these risks and conduct an assessment based on the TF threat(s) present and the NPOs natural vulnerability to those threats. This would allow NPOs to apply the appropriate risk-based mitigating measures to reduce the risks identified by their individual NPO.

14. The FATF defines a:

Threat[4]	*A person or group of people, object or activity, with the potential to cause harm.*

[4] FATF (2014a), Risk of Terrorist Abuse in Non-Profit Organisations, FATF, Paris, France, available at www.fatf-gafi.org/topics/methodsandtrends

Vulnerability[5]	*Things that can be exploited by the threat or that may support or facilitate its activities.*

BOX ***2: Threat & Vulnerability definitions***

15. Diagram 1 below describes the steps to be taken when applying a risk-based approach (RBA) by NPOs when they raise and disburse funds in the course of their programme management.

Diagram 1: Applying an RBA to protect against NPO TF abuse

16. When there is a clear understanding of the TF risks faced by NPOs, NPOs can now make informed decisions on the implementation adequate and proportionate risk mitigation strategies.

A. Identifying TF Risks

17. Each NPO must undertake a basic risk assessment to better understand its ***individual and unique*** exposure and vulnerability to TF threats. These threats may present differently for each NPO. In assessing unique risks, an NPO should consider factors which involve the nature of the NPO's activities, source of funding and areas of operation. For example, international activities including international donations or cross-border fundraising, operations in regions with heightened TF threats,

[5] FATF (2014a), Risk of Terrorist Abuse in Non-Profit Organisations, FATF, Paris, France, available at www.fatf-gafi.org/topics/methodsandtrends

partnerships with high-risk counterparts or intermediaries, engagement with unfamiliar third parties are some key factors that should be considered.

18. Table 1 below provides examples of the above and are intended to be used as a guide only.

Risk Factor	Example of Vulnerability
Membership and Governance: Risks related to the governance structure and membership of the NPO.	• Poor oversight • Lack of internal controls These can create opportunities for misuse.
The nature of the NPO activities: Emphasis must be placed on the services offered by the NPO.	• NPOs that rely heavily on cash donations or disbursements may lack transparency and traceability, making them attractive for TF abuse. • Certain services provided may be attractive to terrorist entities for misuse. One example of this is the exploitation of youth engagement programmes to recruit individuals into extremist ideologies under the guise of community development.
Geographic location: Risks associated with the location of the NPO's head offices, sub offices, region known for TF threats.	Operating: • in or near conflict zones or regions with active terrorist networks increases the risk of coercion or infiltration. • in jurisdictions with weak CFT frameworks or limited enforcement capacity can also increase vulnerability.
Legal and Regulatory Environment – The adequacy of a country's laws, regulations and policies relating to the operations and governance of NPOs.	• Operating in jurisdictions with weak CFT frameworks or limited enforcement capacity can increase vulnerability.
Financial Assistance: Risks related to providing financial assistance such as voluntary contributions, donations and humanitarian aid, international donations or cross-border fundraising.	• Receiving anonymous donations or • Transferring funds to high-risk jurisdictions, • Transferring funds especially via informal or unregulated channels can obscure the origin and destination of funds raised.
Promotional Activities: Risks associated with fundraising and promotional events.	• Data Breaches. e.g. Online fundraising campaigns are hijacked by terrorist sympathisers who use social media platforms to redirect donations to sham

	NPOs or fraudulent causes linked to terrorism.
Cooperation with Other Organisations: Risks related to partnerships and collaborations with other organisations whether it is local or international.	• Collaborating with other organisations that have weak controls or questionable reputations can expose an NPO to indirect risk.
NPO Beneficiaries: Risks which may occur from a failure to identify and obtain information from associate NPOs and NPO Beneficiaries.	• If there are unverified beneficiaries, without proper identification, funds or resources may be diverted to individuals or groups linked to terrorism, including those on sanctions lists. • Providing services to individuals from high-risk countries or vulnerable populations may inadvertently support terrorist actors.
Procurement: Risks associated with procurement processes.	• Fake or Front Companies: e.g. Procurement contracts for goods and services can be awarded to shell companies controlled by terrorist networks, enabling them to launder money and finance operations under the cover of legitimate business. • Diversion of goods. For example, procured items, especially dual-use goods like vehicles, medical supplies, or communications equipment, may be stolen or redirected for terrorist use.

Table 1: List of TF Risk Factors and Vulnerability examples

19. An Internal Vulnerability Assessment Checklist should be implemented to ensure all relevant factors are considered when identifying TF Risks. A Sample Checklist is provided at Appendix I.

B. Assessing TF Risks

20. After an NPO identifies the potential scenarios that may expose the NPO to TF threats and vulnerabilities, those risks should be assessed based on the probability of each threat occurring and the potential consequences.

21. In assessing the probability of each threat occurring, an NPO should take into account past experiences, the country's NRA results and any other NPO sectoral risk assessment which the FIUTT may have published. This includes any typologies or notices affecting NPOs or the financial sector which have been published by the FIUTT and other competent authorities.

22. In assessing the potential consequences of each threat, an NPO should consider what impact the threat may have on the its mission, activities, beneficiaries, donors and the jurisdictions which may be involved in the NPOs activities.

23. A risk matrix can be developed by an NPO to meet its unique needs. There is no particular format for assessing risk because it will vary depending on the size, structure and nature of activities, etc. For example, if an NPO is larger with branch offices in different countries and geographical area, the assessment will vary compared to smaller NPOs.

24. Based on the risk assessment, an NPO should compile a list of its risks in order of priority. All risks are important but emphasis and resources must be focused on addressing the factors which pose a higher risk.

Risk Matrix Explanation:

25. Once you have identified the risks your NPO faces, each risk needs to be assessed and measured in terms of the chance (likelihood) it will occur and the severity or amount of loss or damage (impact) which may result if it does occur.

26. The risk level associated with each event is a combination of the likelihood that the event will occur and the impact it could have.
Therefore: **Likelihood x Impact = Risk level**

Likelihood

27. Likelihood refers to the potential of a particular risk occurring in your NPO. Three levels of likelihood are provided as examples, but you can have as many as you need for your NPO.

    a) **Very likely**: Almost certain – it will probably occur several times a year
    b) **Likely**: High probability it will happen once a year
    c) **Unlikely**: Unlikely but not impossible.

Impact

28. Impact refers to the seriousness of the damage which could occur if the risk happens. You know your NPO, and are in the best position to know how it would be affected by any impacts. What impacts may affect the NPO and how those impacts would affect the NPO. Some examples of impacts to think about could include:

    a) How your NPO would be affected by a financial loss from a crime.
    b) The risk that a particular donation or transfer of funds abroad may result in a terrorist act and loss of life.
    c) The risk that donations may result in funds being used for any of the following: corruption, bribery, tax evasion, drug trafficking, human trafficking, illegal arms trading, terrorism, theft, or fraud.

Note that these do not cover every scenario and are not prescriptive.

29. Three levels of impact are shown here, but you can have as many as necessary for your NPO:

    a) **Major**: Severe damage
    b) **Moderate**: Moderate level of damage
    c) **Minor**: Minimal damage.

30. Once you assess the likelihood and impact of each risk, you can determine the risk level based on these two factors. Following is an example of how you could use a risk matrix and risk score to determine the risk level posed by donors.

Risk matrix and Risk score

31. You can use a risk matrix to combine the **likelihood** and **impact** to obtain a **risk score**. The risk score may be used to aid decision making and helping you in deciding what action to take in view of the overall risk. A sample Risk Matrix and Risk Scoring model is provided at Appendix II for example purposes only.

    **N.B. risk matrices will differ depending on the nature and operations of each NPO and it is not expected that all NPOs under the FIUTT's Oversight will implement the same Risk Matrix and Scoring model. More guidance will be provided to NPOs based on their individual needs.*

C. Defining the Mitigating Measures

32. Once risks have been identified and assessed, an NPO must develop mitigating measures to reduce the negative impacts of these risks. The mitigating measures should be incorporated as part of the NPO's internal measures and policies.

33. The mitigating measures implemented by an NPO must be proportionate to the risks identified and the impact on the NPOs activities. Risk mitigation measures include:
    a. **Avoidance:** Stopping the risky activity. If the risk can be avoided, what measures will you put in place to prevent the NPO from being exposed.
    b. **Reduction:** Changing the activity to reduce the risk.
    c. **Mitigation:** Implementing actions to minimise the impact of the risk.
    d. **Insurance:** Implementing measures to compensate for potential risks, depending on the nature of the project or activity. For example, an NPO might secure event liability insurance for a public fundraiser or property insurance for a donated facility used for youth programs.
    e. **Acceptance:** Accepting the risk if it is mission-critical and cannot be mitigated.

34. A combination of risk mitigation strategies can create a robust risk mitigation plan tailored to specific needs of an NPO.

D. Implementing the Mitigating Measures

35. As part of the implementation procedure, the NPO should document its risk mitigating measures clearly, and make this document available to all the relevant persons to the NPOs operations. This is to ensure that all persons in the NPO understand what measures should be taken to manage TF risks. Factors that can assist with successful implementation are:
    a. **Training:** Ensure all staff, volunteers, and board members receive regular training tailored to their roles.
        i. Training should cover how TF can affect the NPO, its legal obligations, risk mitigation measures, and how to identify unusual activity/transactions.
        ii. Refresher sessions should be scheduled periodically and keep detailed records of all training activities, including attendance and topics covered.
    b. **Monitoring:** Regularly monitor the NPO's activities and transactions to ensure compliance with mitigation measures. Use internal audits to review financial transactions and assess risk management strategies.
    c. **Know Your Beneficiaries and Partners:** where possible it is important to demonstrate that reasonable measures are taken to identify Beneficiaries and Partners in High-Risk circumstances**.** The measures taken should not be intrusive to the extent that they restrict or delay the NPO's activities, but such that they encourage transparency where it is needed.[6]
    d. **Know Your Donors:** The NPO must collect general information from the donor or take steps to identify the donor where possible. This measure should be implemented especially in circumstances where large donations, over TT$50,000.00 or equivalent value, is received.
    e. **Reporting:** Establish procedures for reporting unusual activities, complaints and concerns. Ensure that staff and volunteers know how to report issues confidentially and without fear of retaliation.
    f. **Coordination and partnership with Authorities-** members of the NPO must ensure that they stay updated with legal obligations and partner with FIUTT and the Registrar General Department to keep updated on the latest publications and news.
    g. **Record Keeping**: Establish and maintain organised systems to securely record financial transactions, donations, disbursements, and project activities. Records should clearly show where funds come from, how they are used, and who benefits. Keep these records for at least six years and ensure they can be promptly accessed when needed. Good record keeping helps demonstrate transparency, supports oversight, and protects your organisation from misuse.
    h. **Use of Regulated Financial Channels:** NPOs that handle funds should maintain and keep their funds in an account held at a regulated bank, and utilise regulated financial institutions to conduct financial transactions, especially when transferring funds overseas. NPOs should require dual signatures to accounts, whether chequing, savings, or investments, and establish a reasonable threshold above which prior authorisation from the governing board is mandatory. The use of "cash" or alternative remittance services to transfer funding should only be used as a last resort.

[6] NPOs are not required to conduct customer due diligence as they do not have customers to whom they provide services. Obtaining information on beneficiaries and partners should be undertaken as a mitigating measure where TF risks are probable.

NPOs should comply with cash declaration and/or cash disclosure requirements in the law to promote greater transparency and accountability of the funds.

E. Review Periodically and Make Revisions

36. An NPO must establish protocols for effective monitoring of risk over time and adapting strategies as necessary to ensure that the organisation remains resilient. It must also ensure that occasionally, the NPO reviews the assessed risks and the effectiveness of the mitigation measures and adjust the mitigating measures where necessary. The review process entails:
    a) **Context Changes:** Reviewing changes in the overall context, such as levels of terrorist risk, corruption, fraud, and criminality.
    b) **Programme Changes:** Assessing changes in the NPO's programmes, focus, and types of beneficiaries.
    c) **Effectiveness:** Evaluating the effectiveness of the mitigation measures and making adjustments as needed.

37. The changing nature of TF threats and vulnerabilities will require NPOs to continuously assess its individual NPO risk, since the relevant information will change over time, depending on your activities, programmes and nature of the NPO. This plays a significant role for protecting your individual NPO from abuse.

4. SELF REGULATORY MEASURES

38. Self-regulatory measures refer to those measures taken by NPOs when they work together to control and manage TF risks, and protect their NPOs reputation from abuse. The FATF has indicated that such measures may include rules and standards which are applied by self-regulatory organisations and accrediting institutions. Such organisations may exist as umbrella organisations or other representational organisations for NPOs in the jurisdiction. These organisations can engage in the development and promulgation of good practices in several ways:
    a) Providing standards by which the sector should abide, including codes of conduct which can be tailored for both small and large NPOs;
    b) Creating a certification or accreditation system which requires NPOs to adhere to a set of standards, e.g. fundraising expenses thresholds. These standards are then enforced by the withdrawal of such accreditation; and
    c) Providing training and raising awareness.

39. The existence of a self-regulatory organisation, however, does not preclude the ability for NPOs to work together, especially those in similar fields or locations, to:
    a) develop a unified approach to identifying and managing TF and other risks,
    b) help banks and financial institutions understand their risk management systems, and
    c) support smaller NPOs by allowing them to share resources (e.g., joint staff training, shared financial control procedures, or auditing practices).

40. While informal collaboration among NPOs is considered a formal "self-regulatory" measure, it can play a valuable role in promoting good governance, transparency, and public confidence in the NPO sector. NPOs should note that informal collaboration can support the implementation of proportionate, risk-based approaches to mitigate TF risks, especially when formal regulatory mechanisms are limited or evolving. However, the onus remains on each NPO to implement effective internal controls and risk mitigation measures to protect itself from potential TF abuse.

5. INTERNAL CONTROLS AND GOOD GOVERNANCE

41. NPOs are encouraged to implement internal controls and good governance practices that promote the integrity of the NPO, transparency, accountability, and resilience to abuse, including TF abuse. These measures should be commensurate with the size, nature, and risk exposure of the NPO.

42. Importantly, an NPO should be established and operate according to its governing document(s), e.g., articles of incorporation, a constitution, or bylaws that outline purposes, structure, reporting practices, and guidelines for complying with local laws.

43. An example of an internal control mechanism relates to an NPO's relationships with its partners and donors.

    a. An NPO should make a decision to use reliable open source or publicly available information to confirm the reputation of its donors and partners, when deciding on these relationships.
    b. There can also be selection criteria when establishing relationships with donors and partners.
    c. Selection criteria may include:
        i. alignment with the NPO's priorities and values;
        ii. proven track record showing results;
        iii. strong financial management systems;
        iv. willingness to form strong partnerships with other NPOs.
    d. After selection, an NPO may decide to have written agreements with the partner.
    e. Where higher risks are identified, an NPO could also implement measures to conduct targeted screening of beneficial owners of their partners and staff when establishing relationships, including through targeted financial sanctions related to terrorism and terrorist financing screening, using domestic and UN sanctions lists, which may be found on the FIUTT's website using the Targeted Financial Sanctions Search Tool.

44. Examples of internal controls and good governance practices include:
    a. **Clear Governance Structures**: Establish well-defined roles and responsibilities, especially for financial oversight, board oversight/governance, and programme management and monitoring.
    b. **Transparency Measures**: Share key information with stakeholders, including your mission, sources of funding, and how funds are used. Keep adequate and complete financial records of income, expenses, and financial transactions throughout the operations, including the end use of

the funds, both nationally and internationally, and carry out transactions through the financial system when possible.

c. **Internal Policies and Procedures**: Develop internal controls such as financial management policies, conflict of interest declarations, partner due diligence, and procurement standards.
d. **Internal Reporting Channels**: While there are no legal requirements for an NPO to have systems to identify and report suspicious transactions, where there is a suspicion, NPOs should encourage staff or volunteers to report any unusual or suspicious activity to the FIUTT or the Police in a secure and confidential manner. Reports to the FIUTT can be submitted voluntarily[7] in accordance with section 52 of the Proceeds of Crime Act. A Typology of suspected NPO abuse for TF is provided at Appendix III for information purposes.
e. **Ongoing Stakeholder Engagement**: Foster open communication with donors, beneficiaries, and partners to reinforce mutual accountability and flag reputational or operational risks early.

6. ENGAGEMENT WITH OVERSIGHT AUTHORITY

45. Active engagement with the Oversight Authority, the FIUTT, is a critical part of safeguarding an NPO's operations, strengthen its internal controls and demonstrate a proactive stance against TF threats and abuse. Such engagement includes:
    a. maintaining open lines of communication[8].
    b. regularly consulting the FIUTT to understand evolving risks, compliance expectations, and reporting obligations.
    c. participating in joint outreach and awareness sessions, sharing sector-specific vulnerabilities, and adopting best practices.
    d. cooperate fully during Oversight Reviews and Risk Assessments which may be conducted by the FIUTT from time to time. This includes providing timely access to records, documents outlining governance structures, and donor information, while ensuring there is transparency with respect to funding sources and programmatic activities.
    e. staying informed about regulatory updates, such as changes in laws and regulations, guidance documents, and risk indicators, enables NPOs to align their operations with national and international standards.

46. Such engagement not only enhances the credibility of the NPO sector but also helps build trust with stakeholders and reinforces the collective effort to prevent misuse of charitable platforms for terrorist financing.

[7] If any member of the public would like to provide information about suspicions of money laundering or of the financing of terrorist activities, a voluntary information report (VIR) can be submitted via mail to the FIUTT. If you believe that the information you provide is serious and requires an immediate law enforcement response, then you may also wish to provide this information directly to your local law enforcement agency.
[8] The FIUTT will communicate with the NPO through the official liaison appointed by the NPO, usually this will be the Controller.

GLOSSARY[9]

WORD	DEFINITIONS
Associate NPOs	Includes foreign branches of international NPOs, and NPOs with which partnerships have been arranged.[10]
Beneficiaries	Refers to those natural person, or groups of natural persons who receive charitable humanitarian or other types of assistance through services of the NPO[11]
Financing of Terrorism/Terrorism Financing	A person who by any means, directly or indirectly, wilfully provides or collects funds, or attempts to do so, or coerces, encourages, entices, or incites another person to do so, without lawful excuse, with the intention or in the knowledge that such funds are to be used in whole or in part – (a) in order to carry out a terrorist act (b) by a terrorist (c) by a terrorist organisation (d) in order to facilitate travel by an individual to a foreign State for the purpose of – (i) carrying out a terrorist act; or (ii) participating in, or provide instruction or training to carry out a terrorist act; (e) by a listed entity; or (f) to facilitate the travel or activities of a foreign terrorist fighter, commits the offence of financing of terrorism.[12]
Non-Profit Organisations or NPO	means a body of persons, whether incorporated or unincorporated, which— (a) is established primarily for the promotion of a patriotic, religious, philanthropic, charitable, educational, cultural, scientific, literary, historical, artistic, social, professional, fraternal, sporting or athletic purpose, or some other useful object and raises or disburses funds for that purpose or object; (b) carries on its business without pecuniary gain to its members or officers except as reasonable compensation for services rendered; and (c) restricts the use of any of its profits or other accretions to the promotion of its purpose or object;[13]

[9] The definitions contained in this Glossary were sourced from the Laws of the Republic of Trinidad and Tobago and the FATF Glossary or Interpretive Note to FATF Recommendation 8 ("INR 8"), where a term was not covered by the said laws.
[10] INR 8
[11] *ibid*
[12] Section 22A(1), Anti-Terrorism Act, Chap. 12:07, Laws of the Republic of Trinidad and Tobago
[13] Section 3(1), Non-Profit Organisations Act, 2019, Laws of the Republic of Trinidad and Tobago

Competent Authorities	means public authorities with designated responsibilities for combatting money laundering, terrorist financing and proliferation financing and includes– (a) the FIUTT; (b) public authorities that have- (i) the functions of investigating or prosecuting money laundering, associated predicate offences, terrorist financing and proliferation financing and seizing or freezing and confiscating criminal assets, receiving reports on cross-border transportation of currency and bearer negotiable instruments; (ii) supervisory or monitoring responsibilities for ensuring compliance by financial institutions and listed businesses with anti-money laundering and counter-financing of terrorism and counter-proliferation financing requirements, but does not include self-regulatory bodies.[14]
Terrorist	Includes a person who – (a) commits a terrorist act by any means directly or indirectly, unlawfully and wilfully; (b) participates as an accomplice in terrorist acts or the financing or terrorism; (c) organises or directs others to commit terrorist acts or the financing of terrorism; or (d) contributes to the commission of terrorist acts or the financing of terrorism by an individual or a group of persons acting with a common purpose where the contribution is made intentionally – (i) with the aim of furthering the terrorist acts or the financing of terrorism; or (ii) with the knowledge or the intention of the individual or group of persons to commit the terrorist act or the financing of terrorism.
Terrorist Act	Any person who – (a) with the intent to compel a government or an international organisation to do or refrain from doing any act or intimidates the public or a section of the public, for the purpose of advancing a political, ideological or a religious cause religious, philosophical, racial or ethnic cause or other cause of a similar nature, does any act which he intends to cause, creates the likelihood of causing, or is likely to cause— (i) loss of human life or serious bodily harm; (ii) substantial damage to property; (iii) the endangerment of a person's life, other than the life of the person taking the action; (iv) the creation of a serious risk to the health or safety of the public or a section of the public; or

[14] Section 57A(1B), Proceeds of Crime Act, Chap 11:27 (as amended by the FATF Compliance Act, 2025 which was unproclaimed at the time of this publication) of the Laws of Trinidad and Tobago

	(v) prejudice to national security or disruption of public safety including disruption— (A) in the provision of emergency services; (B) to any computer or electronic system; or (C) to the provision of services directly related to banking, communications, infrastructure, financial services, public utilities, transportation or other essential infrastructure; (b) threatens to commit an act referred to in this Part; (c) takes any preparatory steps for the purpose of committing an act under this Part; or (d) coerces, encourages, entices, or incites another person to commit an offence under this Part[15], commits the offence of committing a terrorist act.[16] Also see the definition of Terrorist act as contained in the FATF Glossary – A *terrorist act* includes: (a) an act which constitutes an offence within the scope of, and as defined in one of the following treaties: (i) Convention for the Suppression of Unlawful Seizure of Aircraft (1970); (ii) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971); (iii) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (1973); (iv) International Convention against the Taking of Hostages (1979); (v) Convention on the Physical Protection of Nuclear Material (1980); (vi) Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988); (vii) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (2005); (viii) Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (2005); (ix) International Convention for the Suppression of Terrorist Bombings (1997); and (x) International Convention for the Suppression of the Financing of Terrorism (1999).

[15] Refers to Part II of the Anti-Terrorism Act, Chap 12:07, Laws of the Republic of Trinidad and Tobago, however, this definition also includes any offence under Parts II, III or IIIA of the said Anti-Terrorism Act

[16] Section 3(1), Anti-Terrorism Act, Chap 12:07, Laws of the Republic of Trinidad and Tobago

	(b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organisation to do or to abstain from doing any act.
Terrorist Financing Abuse	Refers to 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.[17]
Terrorist Organisation	means a legal entity or group of terrorists that— (a) commits a terrorist act by any means, directly or indirectly, unlawfully and wilfully; (b) participates as an accomplice in terrorist acts or the financing of terrorism; (c) organises or directs others to commit terrorist acts or the financing of terrorism; or (d) contributes to the commission of terrorists acts or the financing of terrorism by an individual or a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or the financing of terrorism with the knowledge of the intention of the group to commit the terrorist act or the financing of terrorism;[18]

[17] INR 8

[18] Section 2(1), Anti-Terrorism Act, Chap 12:07, Laws of the Republic of Trinidad and Tobago

APPENDIX I – NPO INTERNAL VULNERABILITY ASSESSMENT CHECKLIST

1. Organisational Structure & Governance

☐ Is there a clearly defined governance structure that has been documented?
☐ Are board members and senior staff vetted for integrity and background?
☐ Are roles and responsibilities documented and regularly reviewed?
☐ Are internal rules and standard operating procedures in place to prevent TF abuse?

2. Financial Management & Transparency

☐ Are financial records maintained accurately and consistently?
☐ Are funds tracked from source to final use?
☐ Are financial audits conducted regularly by independent auditors?
☐ Are financial records kept up-to-date and easily accessible for audits?

3. Programme Implementation & Beneficiary Vetting

☐ Are beneficiaries and partners screened against sanctions lists (e.g., using the FIUTT's TFS Tool)?
☐ Is there a documented process for selecting and vetting beneficiaries?
☐ Are field activities monitored to ensure alignment with stated objectives?
☐ Are there safeguards to prevent diversion of aid or resources?

4. Geographic Risk Assessment

☐ Does the NPO operate in high-risk or conflict zones?
☐ Is your NPO partners with high-risk counterparts or intermediaries?
☐ Are there contingency plans for operations in unstable regions?

5. Funding Sources

☐ Are donors and funding sources vetted for legitimacy?
☐ Is there a policy for accepting anonymous donations?
☐ Are large or unusual donations flagged and reviewed?

6. Staff & Volunteer Screening

☐ Are staff and volunteers subject to background checks?
☐ Is there ongoing training on anti-terrorism and financial compliance?
☐ Are whistle-blower protections in place?

7. Information Sharing & Reporting

- ☐ Is there a mechanism for reporting suspicious activities?
- ☐ Are incidents documented and investigated internally before reporting?
- ☐ Is the NPO compliant with local and international reporting obligations?

8. Use of Cash & Transfers

- ☐ Are cash transactions minimised and documented?
- ☐ Are wire transfers monitored and justified?
- ☐ Are financial institutions used reputable and compliant? or Are financial institutions used for all large transactions?

9. Legal & Regulatory Compliance

- ☐ Is the NPO registered and compliant with the NPO Act and any other relevant laws?
- ☐ Are there policies aligned with the FATF recommendations?

APPENDIX II- SAMPLE RISK MATRIX AND RISK SCORING MODEL

The derivation of a Risk Score can be seen from the risk matrix and risk scoring model shown below. Four levels of risk are shown, but you can have as many as you believe may be necessary.

LIKELIHOOD/IMPACT	MINOR	MODERATE	MAJOR
Very likely	Medium 2	High 3	Extreme 4
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2

Risk score/level and Response table

RISK SCORE	RISK LEVEL	DESCRIPTION AND RESPONSE
4	Extreme	Risk almost certain to happen and have very consequences. Response: Do not allow donation or the transfer of funds to occur unless the risk is reduced to an acceptable level.
3	High	Risk likely to happen and/or to have serious consequences. Response: Do not allow donation or the transfer of funds until risk reduced.
2	Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but take steps to reduce risk.
1	Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

Risk Matrix Template

RISK MATRIX		IMPACT		
		LOW	MEDIUM	HIGH
LIKELIHOOD	LOW	Low	Low	Medium
	MEDIUM	Low	Medium	High
	HIGH	Medium	High	Extreme

APPENDIX III – TYPOLOGY OF SUSPECTED NPO ABUSE FOR TF

Typology

15. The Suspected Abuse of Non-Profit Organizations relative to the Financing of Terrorism

Suspected Offence	Financing of Terrorism
Customer Type	Individual; Group
Industry	FI's
Channel	Physical; Electronic
Jurisdiction	Local; Foreign

A faith-based charitable organisation ("the NPO") was established to fund the renovation of local places of worship of the same faith as the NPO. Accounts were opened at Bank A to facilitate collection of donations from local persons of the same faith. The NPO subsequently conducts fund-raising activities in order to assist victims of natural disasters in foreign jurisdictions. Cash deposits to the NPO's account at Bank A increased exponentially. The NPO partnered with foreign agencies to provide relief to persons affected by natural disasters. Funds were subsequently remitted from the NPO's account to foreign agencies.

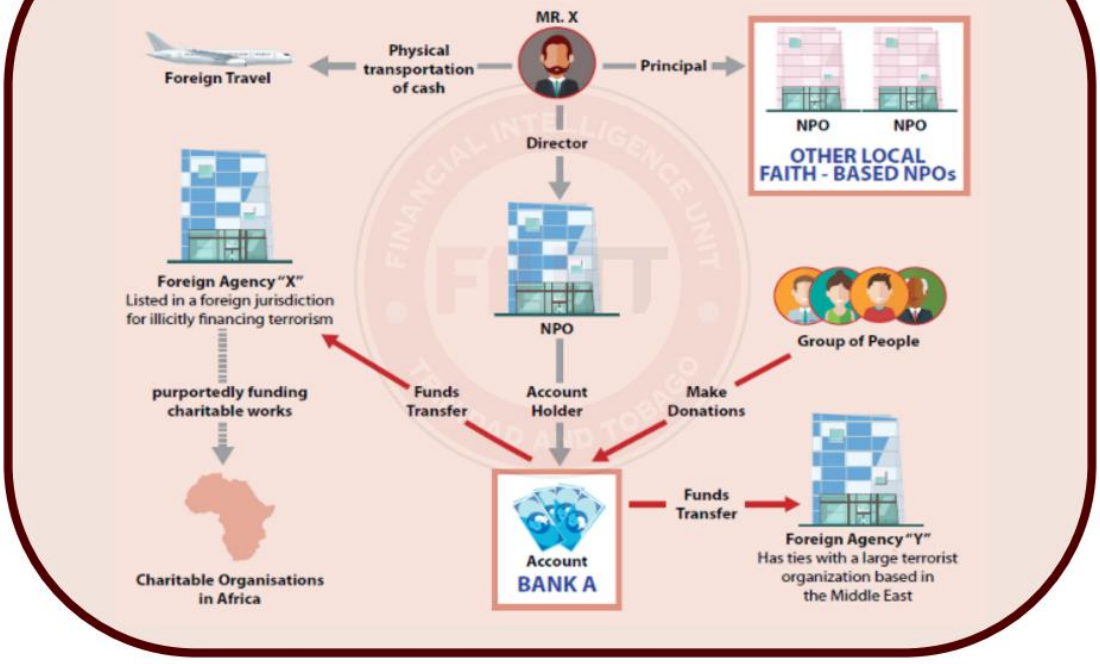
Ensuing fund transfers were declined by Bank A as a result of due diligence conducted which revealed that the foreign agencies were linked to suspected global terrorist organisations. It was later revealed that the director of the NPO was also linked to several other NPOs within Trinidad and Tobago and later identified as travelling internationally from Trinidad and Tobago with large amounts of cash on his person. The ultimate destination and/or beneficiary of these funds could not be verified.

Suspicious Indicators

- Significant cash deposits within a short period of time where the true source and legitimacy of the source(s) cannot be determined;
- The NPO's accounts are used to conduct suspicious or large, complex or unusual transactions;
- One of the foreign agencies being from a country listed as a high risk jurisdiction by the FATF;
- Large wire transfers to foreign agencies whom are suspected of being involved in the financing of terrorism; and
- Official of the NPO travelling to foreign jurisdictions with large amounts of foreign currency on his person circumventing the tracing of funds via the financial system.

DIAGRAM 12

SUSPECTED NPO ABUSE FOR FINANCING OF TERRORISM



End of document