



Guidance Note for Non-Profit Organizations and Donors to Combat Financing of Terrorism

INDIA

Table of Contents

1.	BACKGROUND	4
1.1	Introduction	4
1.2	Defining Terrorist Financing	4
1.3	Why Combat Financing of Terrorism?.....	5
2.	INTERNATIONAL AND NATIONAL INITIATIVES	5
2.1	International Convention for the Suppression of the Financing of Terrorism.....	5
2.2	Security Council Resolution 1267 & 1373 and Successors	6
2.3	The Financial Action Task Force (FATF)	6
2.4	FATF Recommendations for NPOs.....	6
2.5	FATF Recommendation 8: Non-Profit Organizations.....	7
3.	RISK AND VULNERABILITY OF NGO/NPO SECTOR	7
3.1	Risk-Based Approach.....	7
3.2	Reasons for Vulnerability of NPO Sector.....	8
3.3	Guidance for Donors	9
4.	COMPLIANCE REQUIREMENTS	10
4.1	Definition of NPO/NGO under the Indian Law.....	10
4.2	Compliance Requirements.....	10
4.3	Management Commitment	11
4.4	Risk Based Approach	11
4.5	Customer Due Diligence	12
4.6	Know Your Donor.....	13
4.7	Laws and Regulations for Donors.....	14
4.7.1	Income Tax Act, 1961	14
4.7.2	Foreign Contribution (Regulation) Act, 2010 (FCRA)	14
4.7.3	Know Your Customer (KYC) and Anti-Money Laundering (AML) Regulations.....	14
4.7.4	Goods and Services Tax (GST)	14
4.7.5	Corporate Social Responsibility (CSR).....	14
4.7.6	Disclosure Requirements.....	14
4.7.7	Public Charitable Trusts and Societies	14
4.7.8	Donation Limits and Modes	14
4.7.9	Donor Privacy	15
4.8	Red Flags/High Risk Indicators for NPOs.....	15
4.8.1	Donations.....	15
4.8.2	Beneficiaries	16
4.8.3	Partners	16
4.8.4	Employees	16

4.8.5	Monitoring of Projects.....	16
4.9	Record Maintenance	17
4.10	Transactions through Banking Channels.....	18
4.11	Foreign Operations	18
4.12	Fund Utilization	19
4.13	Trainings on Countering Financing of Terrorism.....	19
4.14	Restriction on Receiving Fund from Certain Persons / Organizations / Country....	19
4.15	Clearance for Foreign Donation.....	19
4.16	Reporting.....	19
4.17	Providing Information to Law Enforcement Agency (LEAs) and Regulatory Bodies	20
4.18	Penalties for Non-compliance under Unlawful Activities (Prevention) Act, 1967 (UAPA)	20

1. BACKGROUND

1.1 Introduction

Terrorist organizations use advanced techniques to finance their activities, including the use of multiple financial transactions, a variety of financial instruments and other types of value-storing assets, different financial institutions, accountants, financial advisers, shell corporations, and other service providers, as well as a complex web of transfers to and from different countries.

Terrorist financing often display similar transactional features as money laundering, like concealment and disguise. Combating terrorist financing is, therefore, a key element in promoting a strong, sound and stable development sector.

Terrorist financiers are inventing more complicated and sophisticated procedures and using new technologies for financing the terrorism. To address these emerging challenges, the global community has taken various initiatives against the TF. In accordance with international initiatives, India has also taken so many initiatives in this regard.

NPOs pose a risk of being abused for terrorism financing or other forms of terrorist support by virtue of its characteristics or activities. These guidelines will provide more information about these risks, and provides examples of good practices that NPOs can adopt to help them to identify and manage their exposure to such risks.

Overall, combating terrorist financing requires a multi-faceted approach that involves a range of stakeholders, including governments, financial institutions, and law enforcement agencies. By implementing advanced techniques and establishing effective regulatory frameworks, we can work together to prevent, detect, and prosecute terrorist financing and promote a strong, stable, and secure development sector.

1.2 Defining Terrorist Financing

Terrorist financing (TF) can be defined as financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. The International Convention for the Suppression of the Financing of Terrorism (1999) under the United Nations defines TF in the following manner:

- i. If any person commits an offense by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
 - o An act which constitutes an offence within the scope of and as defined in one of the treaties that is annexed to this convention; or
 - o Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any 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 organization to do or to abstain from doing an act.

- ii. For an act to constitute an offense set forth in the preceding paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in said paragraph 1, subparagraph (a) or (b)

1.3 Why Combat Financing of Terrorism?

Terrorist groups need money to sustain themselves and carry out terrorist acts. Terrorist financing encompasses the means and methods used by terrorist organizations to finance their activities. These funds may come from legal sources, such as legitimate businesses, government funding, and religious or cultural organizations, or from illegal sources, such as drug trafficking, kidnapping, and government corruption. The funds may also come from an illegal source but appear to come from a legal source, through money laundering.

The financing of terrorism weakens the economy of a country. India is a member of Financial Action Task Force and other FATF Styled Regional Bodies like the Asia Pacific Group on Money Laundering, and the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG). India's Financial Intelligence Unit is a member of the Egmont Group also.

Sources may include donations or gifts of cash or other assets to organizations, such as foundations or charities that, in turn, are utilized to support terrorist activities or terrorist organizations.

2. INTERNATIONAL AND NATIONAL INITIATIVES

In response to the growing concern about terrorist activities, the international community has taken actions on many fronts.

Many international organizations which set the international standards, have described the documents and instrumentalities for combating the financing of terrorism (CFT) purposes.

The Global Programme on Detecting, Preventing and Countering the Financing of Terrorism (CFT Programme) was launched in 2020 to step up UNOCT/UNCCT¹ efforts in this area as mandated by the General Assembly's Global Counter-Terrorism Strategy and its review resolutions, and the Security Council, including through resolutions 1373 (2001) and 2462 (2019).

This capacity-building programme on Terrorist Designations and Asset Freezing that, since March 2015 provided technical assistance and training to Member States (national regulatory agencies, financial intelligence units, relevant ministries and private sector institutions) and regional bodies on the effective implementation of targeted financial sanctions against terrorism and terrorism financing.

2.1 International Convention for the Suppression of the Financing of Terrorism

Financing of terrorism is an international concern for the global economies. To respond to this concern, the UN adopted the International Convention for the Suppression of the Financing of Terrorism (1999). The convention came into force on April 10, 2002, with 132 countries signing the

¹ United Nations - Office of Counter Terrorism / UN Counter-Terrorism Centre

convention and 112 countries ratifying it including India. The convention requires ratifying states to criminalize terrorism, terrorist organizations and terrorist acts. Under the convention, it is unlawful for any person to provide or collect funds with the

(1) intent that the funds be used for, or

(2) knowledge that the funds be used to, carry out any of the acts of terrorism defined in the other specified conventions that are annexed to this convention.

2.2 Security Council Resolution 1267 & 1373 and Successors

The 1267 Committee issues the list of individuals and entities whose assets are to be frozen and has procedures in place to make additions or deletions to the list on the basis of representations by member States. The most recent list is available on the website of the 1267 Committee. On September 28, 2001, the UN Security Council adopted Resolution 1373, which obligates countries to criminalize actions to finance terrorism. It further obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorists, including freezing funds or assets of persons, organizations or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorists; and
- co-operate with other countries in criminal investigations and sharing information about planned terrorist acts. The resolution also established the Counter Terrorism Committee (CTC) to monitor the performance of the member countries in building a global capacity against terrorism

2.3 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) formed by G-7 countries in 1989, is an intergovernmental body whose purpose is to develop and promote an international response to combat money laundering. In October, 2001, FATF expanded its mission to include combating the financing of terrorism. FATF is a policy-making body, which brings together legal, financial and law enforcement experts to achieve national legislation and regulatory AML and CFT reforms. FATF adopted a set of 40 recommendations which are widely endorsed as the international standard for AML and CFT.

2.4 FATF Recommendations for NPOs

The Financial Action Task Force (FATF) has studied the problem of terrorist financing and abuse across the charitable sector globally and has published typologies of such abuse. The FATF has also published Best Practices for Non-Profit Organizations and issued Interpretive Guidance strengthening the international standard for combating terrorist abuse of non-profit organizations. FATF Recommendation 8 focused on the terrorist financing risk in non-profit organizations (NPO) sector and suggest adequacy of respective country laws and regulations in supervision of NPOs.

2.5 FATF Recommendation 8: Non-Profit Organizations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. The objective of Recommendation 8 is to ensure that NPOs are not misused by terrorist organisations:

- (i) to pose as legitimate entities;
- (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or
- (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes, but diverted for terrorist purposes.

3. RISK AND VULNERABILITY OF NGO/NPO SECTOR

3.1 Risk-Based Approach

The due diligence approach of a non-profit organization (NPO) should align with the level of risk it encounters. These risks can stem from various factors, including donors, beneficiaries, the nature of charitable services offered, or the geographic areas where the NPO extends its charitable support. Once these risks are recognized, it's important to take measures to reduce them by putting in place policies and procedures that are appropriate in relation to the specific risks at hand.

The first step is to identify the potential risks when establishing a relationship with your donors or beneficiaries. The following factors can be considered:

- **Donors and Beneficiaries**
 - Type of donor/beneficiary (individual, legal entity, Government department etc.);
 - Nature of relationship with donor/beneficiary (e.g. long-standing, new, one-off);
 - Location of the donor/beneficiary.
- **Type of Charitable Support**
 - The type of charitable support offered by the NPO (funds, goods, services etc.);
 - The type of charitable support offered by the Donor or requested by the beneficiary.
- **Delivery Method for Charitable Support**
 - Whether the charitable support is delivered by cash, cheque, electronic means etc.;
 - Location where the charitable support is delivered.

Once the potential risks to the NPO have been established it is likely that not all donors, beneficiaries and charitable support will pose the same level of risk. The NPO is therefore unlikely to need to know all donors and beneficiaries equally. There are three levels of due diligence which can be considered: simplified due diligence, standard due diligence and enhanced due diligence. The level of identified risk will determine the level of due diligence that is required. Any due diligence that is completed should be documented for future reference and recorded in line with the NPO's documentation policies and procedures.

3.2 Reasons for Vulnerability of NPO Sector

The vulnerability of NPOs to TF abuse stems from the ease with which funds can be transferred across borders, the limited regulatory oversight in certain areas, and the diversity of actors involved in the sector.

One of the key risks is the potential for terrorist organizations to use the NGO/NPO sector to conceal the source and destination of funds. Terrorist groups may establish their own NGOs/NPOs or exploit existing organizations, posing as legitimate entities, to move funds for their activities. This highlights the importance of strong due diligence measures to verify the legitimacy of organizations and their funding sources.

Another risk is the potential for the misuse of funds intended for legitimate purposes to support terrorist activities. This can occur through the diversion of funds or the use of front companies to disguise the true nature of transactions. The use of cash-based transactions, particularly in rural areas, further increases the risk of illicit financing activities.

The use of third-party intermediaries, such as money transfer agents, also creates a risk of terrorist financing in the NGO/NPO sector. These intermediaries may be used to move funds across borders or to convert funds into different currencies, making it difficult to trace the flow of funds and identify the ultimate beneficiary.

Overall, the terrorist financing risks and vulnerabilities in the NGO/NPO sector in India highlight the importance of strong regulatory oversight and due diligence measures to prevent the sector from being exploited for illicit financing activities.

There are five categories of abuse or risk facing NPOs:

- i. The diversion of funds is a significant method of abuse, with actors inside the NPO or external actors (such as foreign partners or third-party fundraisers) being responsible for the diversion to support terrorist entities at some point through the NPO's operational or financial processes;
- ii. NPOs or their directing officials knowingly or unknowingly maintaining an affiliation with a terrorist entity which may result in the NPO being abused for multiple purposes, including general logistical support to the terrorist entity;
- iii. Abuse to support recruitment efforts by terrorist entities;
- iv. The abuse of programming in which the flow of resources is legitimate, but NPO programmes are abused at the point of delivery; and v. Abuse through false representation in which terrorist entities start "sham" NPOs or falsely represent themselves as the agents of "good works" in order to deceive donors into providing support. Well-planned deceptions are difficult to penetrate with the resources available to non-governmental actors, making state-based oversight and its capabilities a necessary element to detecting the most sophisticated threats to the sector's activities.

3.3 Guidance for Donors

For donors it is good practice to undertake reasonable steps to research publicly available materials in order to ascertain how an NPO operates, how it is managed, the nature of its programmes and where they operate. This is especially true for NPOs that operate in areas where there is known risk of terrorist activity. Donors may access the following websites for checking information on the NPOs:

1. DARPAN PORTAL- <https://ngodarpan.gov.in/>
2. INCOME TAX PORTAL- <https://incometaxindia.gov.in/Pages/utilities/exempted-institutions.aspx>
3. FCRA PORTAL- https://fcraonline.nic.in/fc8_statewise.aspx

4. COMPLIANCE REQUIREMENTS

4.1 Definition of NPO/NGO under the Indian Law

In India, Non-Profit Organizations (NPOs) are commonly referred to as Non-Governmental Organizations (NGOs), and are defined as entities that are organized and operated for a charitable, social, cultural, educational, religious, or similar purpose.

Under the Indian law, the primary legislation governing the registration and functioning of NPOs/NGOs is the Indian Societies Registration Act, 1860, Public Trust Acts of States and the Companies Act. Additionally, the Income Tax Act, 1961, provides tax exemptions to registered NPOs/NGOs that meet certain conditions and Foreign Contribution Regulation Act govern the foreign funding of NPOs.

To be considered a registered NPO/NGO in India, the organization must meet the following criteria:

- i. The organization must be a trust, society, or a non-profit company registered under Section 8 of the Companies Act, 2013.
- ii. The organization must have a clear purpose and objective that falls under one of the categories recognized under Indian law, such as charitable, social, cultural, educational, religious, or similar purposes.
- iii. The organization must have a governing board or managing committee, which is responsible for the management and administration of the organization.
- iv. The organization must comply with all applicable laws and regulations, including filing annual tax returns and maintaining proper books of accounts.
- v. Once registered, NPOs/NGOs in India are required to file annual reports with the relevant authorities, which outline their activities and financial performance. They are also subject to regular audits and inspections by government authorities to ensure compliance with applicable laws and regulations.

4.2 Compliance Requirements

The laws require NPOs/NGOs to take measures to ensure that their funds and resources are not used for terrorism-related activities. CFT laws for NPOs/NGOs in India:

- i. FCRA (Foreign Contribution Regulation Act) 2010: The FCRA regulates the acceptance and utilization of foreign contributions by NPOs/NGOs in India. It requires all NPOs/NGOs receiving foreign contributions to register under the act and comply with the rules and regulations specified in the act. NPOs/NGOs must use the foreign contribution for the specific purpose for which it was received and maintain proper records of such utilization.
- ii. PMLA (Prevention of Money Laundering Act) 2002: The PMLA aims to prevent money laundering and terrorist financing. It requires all NPOs/NGOs to maintain proper records of all donations received, including the identity of the donor, the amount donated, and the

purpose of the donation. NPOs/NGOs must report any suspicious transactions to the Financial Intelligence Unit (FIU) of India.

- iii. UAPA (Unlawful Activities Prevention Act) 1967: The UAPA prohibits the use of funds for terrorist activities and organizations. NPOs/NGOs must ensure that their funds and resources are not used for any such activities. They are also required to report any suspicious activities or transactions to the authorities.
- iv. KYC (Know Your Customer) norms: NPOs/NGOs must comply with the KYC norms while accepting donations. They must verify the identity of the donor and maintain proper records of the same.
- v. Due Diligence: NPOs/NGOs must conduct due diligence while accepting donations, especially if they are from foreign sources. They must ensure that the funds are not coming from sources linked to terrorist activities or organizations.

Failure to comply with these laws can result in severe consequences, including cancellation of registration, fines, and even criminal prosecution. Therefore, it is essential for NPOs/NGOs in India to comply with all applicable CFT laws and regulations to prevent the misuse of their funds for terrorist activities.

4.3 Management Commitment

To have a successful Countering the Financing of Terrorism (CFT) program, the commitment of senior management is crucial. Senior management must actively support the development and enforcement of CFT objectives. By doing so, they can deter criminals from using their facilities for money laundering and terrorist financing, while also ensuring compliance with legal obligations.

NGOs/NPOs must also have a clear CFT policy that is communicated to all employees on an annual basis. This policy should be endorsed by the CEO and should explicitly state the organization's stance against money laundering, terrorist financing, and any activities that facilitate these crimes. The statement should reflect the strong commitment of the organization and its senior management to comply with all relevant laws and regulations related to CFT.

4.4 Risk Based Approach

NGOs/NPOs should conduct a thorough assessment of their terrorist financing (TF) risks with respect to their customers or direct beneficiaries (such as individuals, groups, or organizations), countries or geographic regions, transactions, etc. Based on the outcome of the risk assessment, NGOs and NPOs shall implement appropriate measures to mitigate the identified risks.

These are the risks arising from interaction, or lack thereof, with donors, beneficiaries, partners, employees and volunteers. The NPO should be able to obtain answers to the following questions to identify this risk:

- Does the NPO perform independent due diligence on donors, beneficiaries, partners, employees and volunteers, before establishing working relationships?

- Does the NPO screen donors, beneficiaries, partners, employees and volunteers against UN-designated individuals and entities and the list of persons and entities designated by the Minister of Home Affairs or any other agency/authority domestically for Targeted Financial Sanctions?
- Does the NPO conduct enhanced due diligence by doing additional checks on donors, beneficiaries or partners that are located in high-risk jurisdictions and/or near conflict zones?

4.5 Customer Due Diligence

If an NGO or NPO is giving money to another NGO or NPO to carry out a project, they need to make sure that the partner organization is not indulging in illegal activities like money laundering or terrorist financing.

The NGO or NPO that gives the money (the "donor") is responsible for making sure that their partner organization is following these rules. The partner organization is responsible for collecting the personal information of the people who benefit from the project.

The donor organization should also ask their fund recipient organizations (NGOs/NPOs) for information about their projects, how they are working, where they are located, and where their money comes from.

Simplified due diligence is the lowest level of due diligence that can be completed on a donor or beneficiary. This is appropriate where there is little opportunity or risk of the NPO, donor or beneficiary becoming involved in terrorist financing. Where the NPO, donor or beneficiary fall into simplified due diligence criteria then the only requirement is to identify the donor or beneficiary.

The NPO's relationship with the donor or beneficiary should be continually monitored for events which may require further due diligence in future.

There are a number of factors that can help determine if a situation is low risk, such as the type of charitable support being solicited or offered or the type of donor or beneficiary the NPO is engaging with. Consideration can also be given to whether the donor or beneficiary is required by law to disclose information regarding their ownership structure and business activities or is otherwise subject to Anti-Money Laundering and Terrorist Financing laws.

If at any point during the relationship with the donor or beneficiary additional intelligence becomes available which suggests that the donor, beneficiary or the type of charitable support involved may pose a higher risk than originally thought, one of the more rigorous levels of due diligence discussed below should be conducted.

Standard due diligence requires the NPO to identify the donor or beneficiary as well as verify their identity. The NPO would also need to gather information to allow it to understand the nature of the relationship with the donor or beneficiary. This level of due diligence should provide the NPO with confidence that it knows who the donor or beneficiary is and that the charitable support of the

NPO is not being used to commit or facilitate terrorist activity (or money laundering or other criminal activity).

As with simplified due diligence, there is a requirement to monitor the donor or beneficiary and the relationship, which will highlight any circumstances requiring enhanced due diligence.

Enhanced Due Diligence is necessitated in cases where the amalgamation of the donor or beneficiary and charitable support presents a heightened risk. High-risk scenarios typically emerge when there is an elevated potential for facilitating activities like terrorist financing, money laundering, or other illicit endeavors through the specific charitable support mechanism employed in a given transaction.

The specific measures for additional due diligence may vary, contingent upon the nature and gravity of the perceived risk. These assessments should be commensurate with the level of risk identified, ensuring that they instill confidence that any potential risk has been effectively minimized and that the likelihood of that risk materializing is low.

4.6 Know Your Donor

The NPO should conduct a reasonable search of publicly available information to determine whether the donor is suspected of activity relating to terrorism, including terrorist financing or other support. The NPO should assure itself that the donor is not a designated individual/entity. The following, amongst other factors, should be considered by the NPO in assessing the risks related to donors:

- Does the NPO have a well-established relationship with donor?
- How is the money being received? (Cash, cheque, bank transfer or some other means?)
- How large is the donation?
- Is the donation in the form of a loan? If so, can the source of the funds be identified or checked by the NPO? Is there a condition that funds are only to be retained by the NPO for a period and then returned to the donor, with the NPO retaining the interest?
- Are there unusual or substantial one-off donations?
- Does the donation come with any conditions attached? What are they? Are they reasonable?
- Is the donation conditional on particular organizations or individuals being used to apply the funds?
- Is the donation conditional on being applied to benefit particular individuals either directly or indirectly?
- Is there a suspicion that the NPO is being used as a conduit for funds to a third party?
- Is the donation in Indian Rupees or another currency, perhaps with a requirement that the donation be returned in a different currency?
- Is the donation received from a known donor but through an unknown party or an unusual payment mechanism where this would not be a typical method of payment?

- Are any of the donors based, or does the money originate, outside India? If so, from which country? Does this country/area pose any specific risks?
- Are donations received from unknown bodies or international sources in countries where financial regulation or the legal framework is not rigorous?
- Is anything else unusual or strange about the donation?

4.7 Laws and Regulations for Donors

Donors to NPOs have certain rules and regulations they should be aware of. Here is an overview of some key laws and regulations related to NPO donors in India:

4.7.1 Income Tax Act, 1961

Donations to eligible NPOs can qualify for tax deductions under Section 80G of the Income Tax Act. Donors can claim deductions of up to 50% or 100% of the donated amount, depending on the nature of the NPO and specific provisions.

4.7.2 Foreign Contribution (Regulation) Act, 2010 (FCRA)

If an NPO receives foreign contributions, it must be registered under FCRA. Donors should ensure that the NPO they are donating to has a valid FCRA registration to accept foreign contributions.

4.7.3 Know Your Customer (KYC) and Anti-Money Laundering (AML) Regulations

Donors, particularly those making large donations, may be subject to KYC and AML regulations. Banks and financial institutions may require donors to provide specific information about the source of funds.

4.7.4 Goods and Services Tax (GST)

Donations to NPOs are generally exempt from GST. However, it's essential to ensure that the NPO provides the necessary documentation to establish the tax-exempt status of the donation.

4.7.5 Corporate Social Responsibility (CSR)

Companies meeting specific financial criteria are required to spend a portion of their profits on CSR activities. Donations made for CSR purposes are regulated under Section 135 of the Companies Act, 2013.

4.7.6 Disclosure Requirements

NPOs are typically required to disclose information about their finances, activities, and governance. Donors may want to review an NPO's financial statements, annual reports, and other disclosure documents to ensure transparency and accountability.

4.7.7 Public Charitable Trusts and Societies

Depending on the legal structure of the NPO (e.g., trust or society), there may be specific regulations governing their operations. Donors should be aware of the specific legal framework under which the NPO operates.

4.7.8 Donation Limits and Modes

Some modes of donations, such as cash donations, have limits beyond which they may not be eligible for tax benefits. Electronic and bank transfers are generally preferred for larger donations.

Section 80G deductions can be claimed by taxpayers when they make donations through the following modes:

- Cheque
- Demand draft

- Cash (for donations below Rs 2,000)

Note: Contributions in the form of goods, such as food, materials, clothing, medicines, etc., and donations exceeding Rs 2,000 that don't meet the eligibility criteria for deduction under Section 80G should be made using non-cash methods to be eligible under Section 80G.

4.7.9 Donor Privacy

Donors should be aware of the NPO's policies regarding the privacy of their personal information and whether their details will be kept confidential.

It's important for donors to exercise due diligence when contributing to NPOs, ensuring the organizations are compliant with relevant laws and using the funds for the intended charitable purposes. Additionally, donors should retain records of their donations and any acknowledgment receipts to claim tax benefits.

Robust internal governance practices for NPOs can be grouped into the following four categories:

- 1) Organisational integrity;
- 2) Partner relationships;
- 3) Financial transparency and accountability; and
- 4) Programme planning and monitoring.

4.8 Red Flags/High Risk Indicators for NPOs

4.8.1 Donations

- If unusual or substantial one-time donations are received from unidentifiable or suspicious sources.
- If a series of small donations are received from sources that cannot be identified or checked.
- If 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.
- Where donations are made in a foreign currency or foreign sources where financial regulation or the legal framework is not as rigorous.
- 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 favourable 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.

4.8.2 Beneficiaries

- 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 or similar names and signatures.

4.8.3 Partners

- 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.

4.8.4 Employees

- 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 behaviour or conduct.
- Sudden or increased staffing costs.

4.8.5 Monitoring of Projects

- 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 services 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.
- Infrequent and/or poor reconciliation of local banking and accounting records / bank reconciliations not done in a timely manner.
- Payments to suppliers via cash payments to employees.
- Offers for monitoring to be carried out by friends or known associates of the local partner without the need for the NPO to carry out an inspection or checks on the partner themselves.
- Requests to use particular officials in the locality for monitoring purposes.
- Emails from new or unusual email addresses not in the partner's domain name or from someone who is not a previously agreed contact point.
- Inconsistencies between narrative reports and financial claims and reports.

4.9 Record Maintenance

NPOs/NGOs must take the following steps to maintain, preserve, and report customer account information:

- i. Keep all records of transactions between the donor and the beneficiary (both domestic and international) for at least five years from the date of transaction.
- ii. Preserve the records related to donor/intermediary/beneficiary identification and their addresses for at least five years after the association ends.
- iii. Provide identification records and transaction data to authorities if requested.
- iv. Keep all necessary information about transactions to allow reconstruction of individual transactions, including details like the nature of the transaction, the amount, the currency, the date, and parties involved.
- v. Develop a system to maintain and preserve account information that enables easy and quick retrieval when required by authorities.
- vi. Maintain records of customer identity and address, and transaction records in either hard or soft format.

4.10 Transactions through Banking Channels

- i. NGOs/NPOs are advised to maintain a bank account in the name of their organization. For transactions involving INR 50,000 or more, they must use the banking channel.
- ii. NGOs/NPOs can maintain only one bank account for receiving donations and grants. If they receive donations for specific projects, they can open separate bank accounts after receiving the funds in their main account.
- iii. NGO/NPO bank accounts should be operated with joint signatures of at least two officials approved by the appropriate authority.
- iv. NGOs/NPOs must ascertain the identity of depositors/withdrawers when issuing or depositing cheques from/to their bank accounts for future reference.

These guidelines aim to ensure transparency and accountability in financial transactions of NGOs/NPOs.

4.11 Foreign Operations

Rules that NPOs/NGOs should follow for their foreign operations to avoid vulnerability:

- i. The bank account operations policy/rules of foreign branches/subsidiaries, even if registered as separate entities, must be approved by the competent supervisory body of the parent organization in the home country. Failure to comply with this requirement may result in penalties or other legal consequences.
- ii. Aid/Grant sent abroad should be restricted to NPOs/NGOs officially registered and licensed for the intended purpose in their respective countries. Direct aid to individuals, institutions, or small foreign NPOs/NGOs that are not subject to regulations and supervision by their own countries must be avoided due to inherent risks and difficulties in supervising them. Violation of this requirement may lead to legal liability, including civil and criminal penalties.
- iii. The provision of aid should focus on the implementation of specific projects, programs, and activities under the effective supervision of competent authorities in the beneficiary countries or an international organization. Non-compliance with this requirement may result in the suspension or termination of aid, as well as other legal consequences.
- iv. All cross-border remittances should be made through formal banking channels after complying with all regulatory requirements. Remittances should be made exclusively to the order of the first beneficiary and deposited into their bank account in the host country through correspondent banks. Failure to comply with this requirement may result in penalties, fines, or other legal consequences.
- v. NPOs/NGOs should maintain detailed information in their home country about the functions of their foreign operations and updated information on the key officers/staff working there. Failure to comply with this requirement may result in penalties or other legal consequences, including the suspension or termination of the NGO's registration or licensing.

4.12 Fund Utilization

NPOs/NGOs have a responsibility to ensure transparency and accountability in their financial operations and to maintain the trust of their donors and stakeholders. To achieve this, the Board of Trustees/Executive Committee and senior management must ensure that all funds are utilized in a manner consistent with the organization's stated goals, objectives, and activities approved by the regulatory authority. Failure to comply with this requirement may result in legal consequences, including penalties, suspension, or revocation of the NGO/NPO's registration or licensing.

Furthermore, all NPOs/NGOs must follow appropriate accounting practices, including maintaining accurate and complete financial records, preparing financial statements that fairly represent the organization's financial position and performance, and implementing effective internal controls to prevent financial improprieties. Adhering to these rules can help NPOs/NGOs avoid legal and reputational risks and maintain their credibility and accountability to their stakeholders.

4.13 Trainings on Countering Financing of Terrorism

The senior management of the NPO/NGO shall organize training programs or send its officers, including senior management, finance, compliance, and program staff, for training on CFT issues. Also, maintain records of all meetings and training conducted.

4.14 Restriction on Receiving Fund from Certain Persons / Organizations / Country

NPOs/NGOs are prohibited from receiving any funds directly or indirectly from any individuals, organizations or their associated organizations listed under United Nations Security Council Resolutions 1267, 1373, 1540 and their successor resolutions. Any such transaction must be reported immediately to the Financial Intelligence Unit - India, and the funds frozen.

In addition, NPOs and NGOs must conduct Enhanced Due Diligence (EDD) when receiving funds from individuals or organizations in countries that are listed as High Risk or Non-Cooperative Jurisdictions by the Financial Action Task Force.

4.15 Clearance for Foreign Donation

Each NGO/NPO is required to obtain clearance from the appropriate authority before receiving any foreign aid, grant, donation, or loan. The organization must maintain and preserve all relevant documents related to the transaction. The NGOs/NPOs must not return any portion of the donation to the donor without obtaining prior approval from the appropriate authority.

4.16 Reporting

- i. It is advised that NPOs/NGOs report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND).
- ii. NPOs/NGOs should carefully go through all the reporting formats. There are altogether five reporting formats viz. i) Manual reporting of cash transactions ii) Manual reporting of suspicious transactions iii) Consolidated reporting of cash transactions by Principal Officer

- of the NPO/NGO iv) Electronic data structure for cash transaction reporting and v) Electronic data structure for suspicious transaction reporting.
- iii. The reporting formats contain detailed guidelines on the compilation and manner/procedure of submission of the reports to FIU-IND
 - iv. The Cash Transaction Report (**CTR**) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR All cash transactions of the value of more than Rupees Ten lakhs or its equivalent in Foreign Currency to be reported.
 - v. The Suspicious Transaction Report (**STR**) should be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request;
 - vi. The Cross-border Wire Transaction Report (**CBWTR**) all cross border wire transfers of more than Rs. 5 lakh or its equivalent in foreign currency, where either the origin or destination of the fund is in India should be submitted to FIU-IND by 15th of the succeeding month
 - vii. The Principal Officer will be responsible for timely submission of CTR, STR and CBWTR to FIU-IND;
 - viii. Utmost confidentiality should be maintained in filing of CTR, STR and CBWTR to FIU-IND. NPOs/ NGOs may not put any restrictions on operations in the accounts where an STR has been made. However, it should be ensured that there is no tipping off to the donor/intermediary/beneficiary at any level.

4.17 Providing Information to Law Enforcement Agency (LEAs) and Regulatory Bodies

The NPOs/NGOs should maintain the accurate records related to the donations received and the beneficiaries served up to last 5 years.

When a request for information is received from the law enforcement agency or regulatory body NPOs/NGOs should respond promptly and provide accurate information with them.

4.18 Penalties for Non-compliance under Unlawful Activities (Prevention) Act, 1967 (UAPA)

Under the Unlawful Activities (Prevention) Act, 1967, non-compliance by the NPO/NGO with the provisions of the Act can result in penalties and legal consequences under the following sections:

- i. Section 13 (Punishment for unlawful activities) This section provides for the punishment for the persons involved in unlawful activities, which includes imprisonment for a term ranging from 5 to 10 years, fine or in some cases to life imprisonment.

- ii. Section 16 (Punishment for Terrorist Act) This section provides that any person who commits the terrorist act or has resulted to death of any person will be punishable with imprisonment ranging from 5 years to life imprisonment, death and also be liable for fine.
- iii. Section 17 (Punishment for raising funds for terrorist act) This section provides punishment for the persons involved in raising and collecting funds in India or in foreign country, either directly or indirectly knowing that such funds are likely to be used, in full or in part by such person or by a terrorist organization or by a terrorist gang or by an individual terrorist to commit a terrorist act will be punishable with imprisonment ranging from 5 years to life imprisonment, death and also be liable for fine.
- iv. Section 38 (Offence relating to membership of a terrorist organization) This section provides that any person who is associated with the terrorist organization with an intention to commit further offence will be punishable with the imprisonment for a term not exceeding 10 years or with fine or both.
- v. Section 39 (Offence relating to support given to a terrorist organization) Whoever supports a terrorist organization with intention to further its activities shall be punishable with the imprisonment for a term not exceeding 10 years or with fine or both. This section defines term 'support' as providing, collecting or receiving property or any other kind of assistance including financial assistance and training for the purpose of committing or facilitating the commission of a terrorist act.
- vi. Section 40 (Offence of raising fund for a terrorist organization) Any person commits the offence of raising or collecting fund or property for a terrorist organization with an intention to use them or knowing it will be used for the furtherance of the activities of a terrorist organization, shall be punishable with imprisonment for a term not exceeding fourteen years or with fine or with both.