THE UNITED REPUBLIC OF TANZANIA

FINANCIAL INTELLIGENCE UNIT

THE TERRORIST FINANCING RISK ASSESSMENT GUIDELINES FOR NON-PROFIT ORGANIZATIONS (NPOs)

JULY, 2023

ACRONYMS

1	AML	-	Anti - Money Laundering
2	AMLA	-	Anti - Money Laundering Act
3	AMLPOCA	-	Anti - Money Laundering and Proceeds Act
4	CDD	-	Customer Due Diligence
5	CFT	-	Counter Financing of Terrorism
6	CFP	-	Counter Financing of Proliferation
7	FATF	-	Financial Action Task Force
8	NPOs	-	Non-Profit Organizations
9	PEPs	-	Politically Exposed Persons
10	RBA	-	Risk-Based Approach
11	TF	-	Terrorist Financing
12	UN	-	United Nations

1. INTRODUCTION

1.1 Background

The global threats of money laundering, terrorist financing and proliferation financing have led counties to strengthen their vigilance to counter these threats and to minimize the possibility of their jurisdictions or institutions becoming involved. Effective enforcement of policies to deter money laundering, terrorist financing and proliferation financing, should, inter alia, enhance the integrity of the financial system and reduce incentives for the commission of crime within jurisdiction.

NPOs have remained potentially vulnerable to the inherent risk of money laundering and terrorist financing, many instances locally and worldwide have revealed terrorist abuse of charitable organizations for raising and moving funds, providing logistic support, encouraging terrorist recruitment or otherwise cultivating the support for terrorist organizations and operations. Terrorist elements also try to exploit every system from where they can collect money and fund their terrorist activities, including corporate sector.

The 2023 Terrorist Financing Risk Assessment Report indicates that the threats of money laundering and terrorist financing extend beyond the traditional financial entities which have been receiving attention for control of these activities. It is therefore necessary for non-financial entities including non-profit organizations to be adequately regulated so as to keep them safe from these nefarious activities, and to protect the legitimate financial system from illicit funds that could find their way into the financial system through non-financial entities.

The Anti-Money Laundering Act (AMLA) and AMLPOCA empowers the Financial Intelligence Unit (FIU) to issue guidelines with respect to money laundering, terrorist financing and proliferation financing. These Guidelines are so issued for the guidance of persons and entities operating as registered NPOs in the United Republic of Tanzania.

1.2 Purpose of Guidance

The purpose of this Guidance is to assist registered NPOs in complying with their legal duties and responsibilities as they relate to money laundering and counter terrorism financing as set out in the AMLA, AMLPOCA, Non- Governmental Organizations Act, 2002 (CAP.56), the Societies Act, Cap 337 and the Societies Act No 6 of 1995 of Zanzibar and other relevant legislation. These Guidelines will not only assist in improving Tanzania's outlook by encouraging increased adherence to the AML and CFT standards set internationally but will also complement enhancing the level of understanding about the due diligence with respect to AML/CFT/CFP in the NPO sector. These guidelines also suggest policies, procedures and internal controls for NPOs to comply with the AML/CFT framework and international best practices.

This Guideline should also be read in conjunction with the Anti-Money Laundering legislation both principal and subsidiary legislation.

1.3 The Financial Action Task Force (FATF) and its Recommendation for NPOs:

FATF has issued a set of recommendations, which are widely endorsed as the international standards for AML and CFT. FATF defines an NPO as "a legal person or arrangement or organization 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".

FATF recommends increased transparency within the non-profit sector and the implementation of a regulatory scheme that includes NPO sector outreach, sector monitoring, effective intelligence and information gathering, and the establishment or strengthening of cooperative relationships between relevant supervisory authorities and law enforcement agencies. In addition, FATF advises countries to encourage the non-profit sector to:

a) adopt methods of best practice with respect to financial accounting, verification of program specifics, and development and documentation of administrative, and other forms of control.
b) use formal financial systems to transfer funds; and
c) perform due diligence and auditing functions of partners and field and overseas operations respectively.

FATF has also issued various reports and detailed guidance to help prevent the NPO sector from the abuse of terrorist financing.

1.4 Legal Framework for NPO Sector in Tanzania

Currently, different laws are applicable for the regulation of the NPOs sector in Tanzania. The NPOs are mainly registered and regulated under different authorities to carter for different intentions that the relevant legislation was enacted to achieve. The following laws are relevant:

- The Societies Act, Cap. 337
- Trustees Incorporation Act.
- The Non-Government Organization Act, 2002 (Cap. 56)
- The NGOs regulations 2019
- The Societies Act No 6 of 1995 of Zanzibar
- The Anti- Money Laundering Act, 2006 The Societies Act, Cap 337.
- The Prevention of Terrorism Act ,2002

1.5 National Initiatives for combating Money Laundering & Terrorist Financing:

The United Republic of Tanzania has taken several initiatives to establish a robust AML/CFT regime by instituting an effective legal and institutional framework including the following;

(a) Money Laundering offence was introduced in Tanzania laws for the first time in 1991 through the enactment of the proceeds of crime Act, 1991 which came in force in 1994.
(b) Tanzania enacted the Anti-Money Laundering Act, Cap. 423 which is applicable in Tanzania Mainland and the Anti-Money Laundering and Proceeds of Crime Act, 2009 which is applicable in Tanzania Zanzibar.
(c) The Establishment of an operational Financial Intelligence Unit.
(d) Tanzania has ratified most of the relevant UN Conventions e.g., Vienna Convention and Palermo Convention.
(e) Tanzania is one of the founder members of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and hosts the ESAAMLG Secretariat.
(f) FIU- Tanzania is a member of Egmont Group.
(g) Increase in Prosecution and conviction of Money laundering cases.
(h) Carried out National ML/TF Risk Assessment.
(i) Has the National AML Multi-Disciplinary Committee which is a coordinating authority for AML/CFT/CFP issues and advise the Government on those matters.

2. TERRORIST FINANCING AND PROLIFERATION FINANCING

2.1 Terrorist Financing

2.1.1 Terrorist Financing (TF) is the act of soliciting, collecting or providing funds, from both legal and illegal sources, with the intention of financing terrorist acts, and of terrorists and terrorist groups, entities organizations.

2.1.2 TF abuse to NPOs refers to the exploitation of NPOs, by terrorists and terrorist group, entity or organization to raise or move funds, provide logistical support, encourage or facilitate terrorist recruitment, or otherwise support a terrorist, terrorist group, entity, organization or operation.

2.1.3 Money laundering is concerned with funds generated from unlawful sources which funds for terrorist activities are often legitimate in nature. The source of funds is therefore, not the sole consideration. The conversion of assets into money and the subsequent direction of that money must be observed.

2.1.4 The United Nations publishes list of individuals and entities that are targeted financial sanctions on account of being terrorist or organizations. NPOs are required to remain abreast of this list and check their databases facilitating terrorism. Should any person or entity on the list be a client, any transaction in respect of which there is a reasonable ground to suspect that it is related or linked to the listed individual or entity or intended to finance terrorist acts or a terrorist organization should be immediately communicated to the FIU. In addition, as far as the Prevention of Terrorism (General) Regulations, 2022 (G.N No. 379 of 2022) is concerned, the designated party is subjected, without delay, to targeted

financial until such time when the designation is revoked by the Minister of Home Affairs, or by the UN Security Council.

2.1.5 The 2023 Terrorism Financing Risk Assessment, identified NPOs sector threat to be at **Medium,** and NPO sector vulnerabilities as **Medium**. The overall TF risk for NPOs sector was rated **Medium**. The report also highlighted varied levels of awareness of TF risks amongst NPOs and understanding of implementation of necessary safeguards such as due diligence checks and guidelines relating to disbursement of funds overseas as key vulnerabilities that could make NPOs more susceptible to TF abuse.

2.2 Financing of Proliferation

Proliferation Financing (PF) is an act by any person who by any means directly or indirectly, renders help or provides in whole or in part any assets, funds, economic resources, technology or services to any proliferation of weapons of mass destruction course or to any person or jurisdiction or for the benefit of any person designated by the UNSC to acquire, possess, broker, manufacture, develop, store, transport, convey, transfer, import or export nuclear, chemical or biological weapons and their means of delivery or related materials including technologies and dual use goods used for non-legitimate purpose.

3.0 METHODS OF MISUSE OF NPOS FOR TERRORIST PURPOSES

3.1 Diversion of funds

Funds raised for NPO purposes are re-directed to a terrorist entity or the facilities of charities are misused for terrorist activities. This can occur during the collection of donations and at any point where the funds of the NPO are transferred between different actors. Actors can be internal (e.g., employees of the NPO) or external (e.g. third party fund-raisers, organizations that partner with the NPO).

Example

The Donor informs the NPO that there was a mistake made in a donation made to the NPO and asks for a refund. The donor requests that the refund be directed to a different bank account. Unknown to the NPO, this bank account is controlled by a terrorist group.

3.2 Support for recruitment

Terrorists, terrorist groups and entities use NPO's facilities and funded activities to promote recruitment of terrorists.

Example

An NPO organizes end-of-year event for beneficiaries from low-income families and terrorist groups participate as sponsors or partners to recruit members during the event.

3.3 Abuse of programming

NPOs-funded programmes meant to support legitimate humanitarian, social, educational or religious purposes are manipulated at the point of delivery to support terrorism by internal or external actors.

Example

An NPO uses donations to purchase or rent properties that are used as shelters for terrorists. The shelters are used for the beneficiaries of the NPOs and also act as transit points for terrorists.

3.4 False representation and fake NPOs

False representation occurs when organizations and/or individuals raise funds, promote causes, and carry out other activities in support of terrorism under the guise of NPOs activities.

Example

Terrorists or their sympathizers may claim to work for an NPO and rely on the NPO's good name and legitimacy in order to gain access to a region or community.

3.5 Affiliation with Terrorist Activity

Affiliations range from informal personal connections involving management and employees of the NPO, to more formalized relationships between an NPO and terrorist entities. This affiliation translates into activity that is meant to financially or otherwise support activities carried out by one or both parties.

Example

Donations received in Tanzania are used to fund an NPO's overseas humanitarian work. Unknown to the NPO, the overseas project manager employs individuals linked to terrorist organizations and some of the funds are misused for terrorism.

3.6 Use of NPO assets

NPO vehicles may be used to transport people, cash, weapons or terrorist propaganda, or NPO premises used to store them or arrange distribution. The communications network of an NPO may be exploited to allow terrorists to contact or meet each other.

3.7 Use of an NPO's name and status

Individuals supporting terrorist activity may claim to work for an NPO and trade on its good name and legitimacy in order to gain access to a region or community. They may use the NPO and/or its name as a seemingly legitimate cover to travel to difficult to reach places to

take part in apparently appropriate but actually inappropriate activities such as attending terrorist training camps. An NPO may give financial or other support to an organization or partner that provides legitimate aid and relief. However, that organization or partner may also support or carry out terrorist activities.

3.8 Abuse from within an NPO

Although it is less likely than abuse by third parties, those within an NPO may also abuse their position within the NPO and the name of NPO itself for terrorism purposes. This might include 'skimming' off money in charitable collections and sending or using the funds to support terrorist activities. People within an NPO may arrange for or allow NPO premises to be used to promote terrorist activity. Sponsors themselves may also be held accountable for engaging in inappropriate behavior or making inappropriate comments for a similar purpose. NPOs may use volunteers they know to be likely to promote terrorism to influence the NPO's work. They may abuse the NPO by allowing those involved in terrorist activity to visit or work with them.

4.0 RISK ASSESSMENT METHODOLOGY

NPOs should regularly review and assess their exposure to abuse for TF and mitigate the identified risks in a systematic manner. The following methodology guides NPOs using a step-by-step approach in assessing TF risks.

4.1 Identify

- Identify TF risk indicators that are applicable to the NPO.
- Identify risk owners - the individuals who are best placed to assess, oversee and implement action plans to manage the identified risks.

4.2 Assess

- Assess and score the TF risks.

4.3 Communicate and Manage

- Communicate the risk scores to governing board members and other stakeholders of the organization.

- Establish action plans to mitigate the risks according to risk appetite, with recommendations from risk owners.

4.4 Monitor

- Monitor the effectiveness of action plans periodically, adjust the action plans where required and review TF risk profile of the NPO regularly.

4.5 Report

- Update or exchange information with governing board members and stakeholders of outcomes derived from managing identified risks by risk owners.

5.0 IDENTIFY: RISK OF TF AND RISK OWNERS

5.1 First, NPOs should identify the TF risks the organization may face and the risk owners.

5.2 When identifying TF risks, NPOs should begin with TF risks central to their NPOs activities, before any mitigating controls are applied. These risks are associated with the characteristics of NPO's activities with respect to their donors, beneficiaries, partners, employees and volunteers, programmes and services provided, geographic regions where they operate and delivery channels. These identified TF risks are also known as inherent risks.

5.3 TF risks can be broadly categorized into the following three categories:

5.3.1 **Donors, Beneficiaries, Partners, Employees and Volunteers**

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

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

(2) 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 domestically for Targeted Financial Sanctions?

(3) 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?

5.3.2 **Delivery and Operational channels**

The NPO must review and be able to obtain information on whether there exist potential illicit activities that arises from day- to-day operations and business/operational activities of the NPO.

The NPO should obtain answers to the following questions:

1. Does the NPO have high volume of donations and disbursements, that use non-regulated financial channels, or have multiple overseas operations and hence find it difficult to identify suspicious activities?

2. Does the NPO have written policies and procedures for

disbursements and utilization of donations within and beyond United Republic of Tanzania?

3. Does the NPO have written procedures to monitor delivery of programmes within and beyond United Republic of Tanzania

4. Does the NPO have high volume of donations and disbursements, that use non-regulated financial channels, or have multiple overseas operations and hence find it difficult to identify suspicious activities?
5. Does the NPO have written policies and procedures for disbursements and utilization of donations within and beyond United Republic of Tanzania?

6. Does the NPO have written procedures to monitor delivery of programmes within and beyond United Republic of Tanzania?

7. Has the NPO established any formal procedures for reporting of suspicious activities or transactions noted in the course of its operations?

5.3.3 **High-Risk Jurisdictions**

This Risk is related to whether there is a higher risk of abuse for the NPO operating or providing services in close proximity to an active terrorist threat.

The relevant questions to be answered when assessing this risk are:

1. Does the NPO have overseas missions or operations in high-risk jurisdictions subject to call for action and/or jurisdictions under increased monitoring identified by the FATF?

2. Does the NPO have overseas missions or operations in an area of conflict where there is active terrorist threat or within a community that is actively targeted by a terrorist movement for support and cover?

List of jurisdictions that are subject to call for action and increased monitoring can be accessed at the FATF website: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html. The list of jurisdictions is reviewed throughout the year and NPOs should keep themselves informed of periodic updates by checking the FATF website. NPOs should also be vigilant and be informed of ongoing news about areas with active or potential terrorist threat especially if the NPO conduct activities in or near these areas.

5.4 It is very important for NPOs to monitor these inherent risks as they may change with

a shift in the NPO's focus or activities. The following examples illustrate how inherent risks may change:

Example 1:

An NPO runs a donor management programme and a significant portion of donations come from reputable international cooperating partners or donors. In recent years the NPO has also encountered donors that are trusts, foundations and philanthropists with origins from overseas locations.

Example 2

An NPO used to conduct overseas missions to directly provide charitable services to low-income groups. In recent years, the NPO opted to continue to provide services through a local partner in Tanzania instead.

Example 3

An NPO used to provide only non-monetary goods to benefit low-income groups as part of its mission. In recent years, there is an increase of cash pay-outs provided directly to these low-income groups.

5.5 Risk Owners

Risk owners are staff/personnel of the NPO in charge of assessing and monitoring the potential risks in their respective areas of responsibilities and are accountable for the management of those risks.

Having identified the TF risks, NPOs should assign appropriate risk owners to the identified TF risks. The risk owner assigned should be the staff/personnel with the most relevant knowledge, resources and authority to assess and manage the risk.

Example of the report of the Assessment on Risk Owners is as shown below:

Source of risk	Risk owner
Disbursement of funds	Treasurer, Finance and Admin Manager
Overseas activities	Chief Executive Officer/Executive Director, Programme coordinator
Volunteers	Volunteer Coordinator, Human Resource Director
Overseas partners, vendors and suppliers	Overseas partners, vendors and suppliers
Employees	Chief Executive Officer/Executive Director, Human Resource Director
Donations	Fund-raising Coordinator, Finance and Admin Manager

6.0 ASSESS: TF RISK SCORING

After identifying the TF risks and the corresponding risk owners, NPOs should derive the risk ratings for each of the risks using a two-dimension rating model –

(a) its likelihood of occurrence and
(b) the impact of which the occurrence would have on the organization.

A. Likelihood

When assessing the likelihood of occurrence, NPOs should consider whether the risk in question has occurred since its establishment, or whether such a risk has occurred within the sector and if so, the frequency of occurrence.

B. Impact

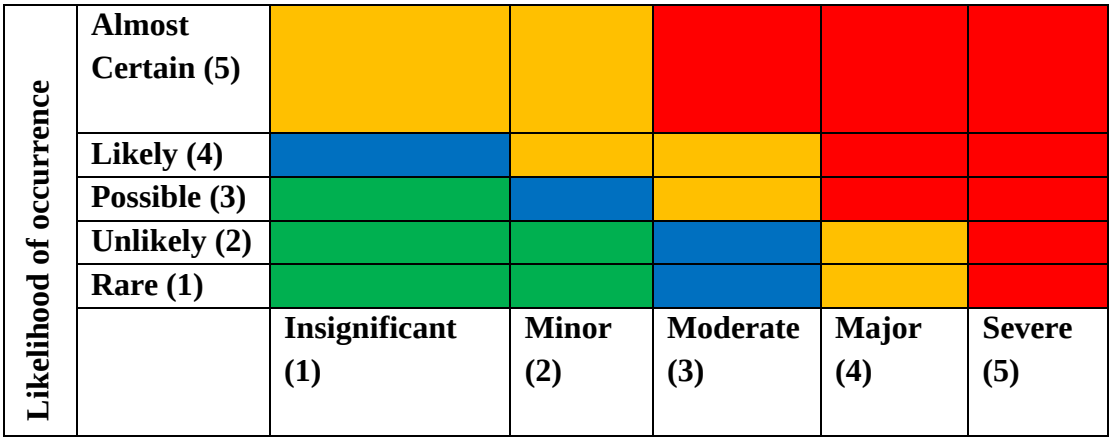
When assessing the impact upon occurrence, NPOs should assess which aspects of the organization may be impacted and the magnitude of the impact, if any. Examples of impact may include:

OperationalDisruptions • Disruption to service • Delay in programme delivery • Revision of scope of programme	**Reputational Losses** • Adverse media associated with charities; • Loss of stakeholders' confidence and trust (e.g. volunteers)
Financial Losses • Loss of donations originally meant to benefit the intended beneficiaries • Potential decline in future donations; • Loss of sponsorships; • Loss of funding	**Legal Implications** • Penalty imposed on charities as a result of non-compliance to law and regulations

6.3 NPOs should rate/score the likelihood of occurrence and impact upon occurrence on an inherent basis, i.e. risk score before the consideration of existing mitigating measures in place.

6.4 NPOs should select the highest rating if there are differing ratings for operational disruptions, reputational losses, financial losses and legal implications. A sample of the risk assessment matrix can be illustrated as follows:

Risk Assessment Matrix

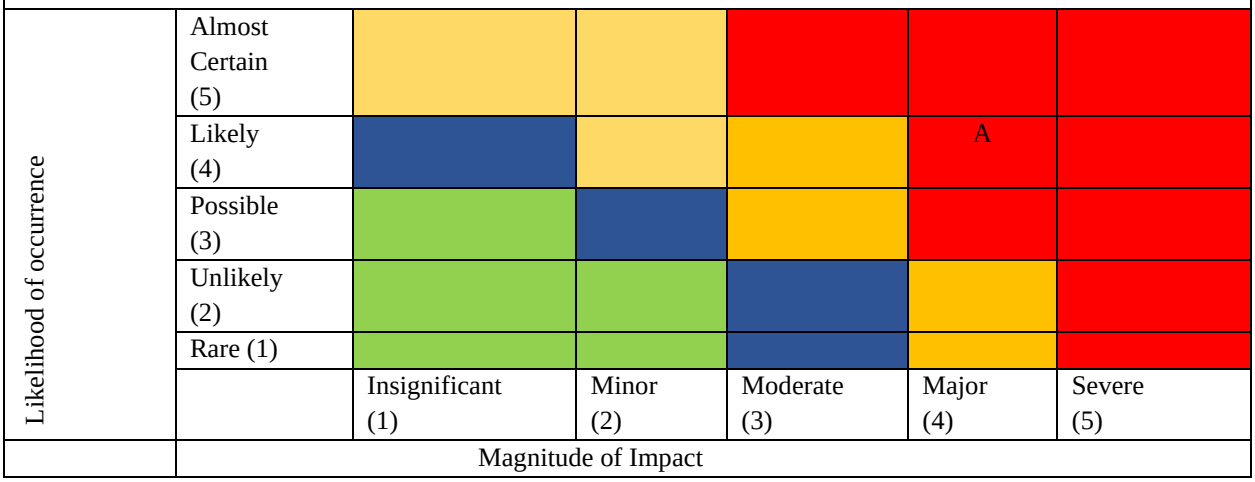


Example:

RISK 1 An NPO engages in missions or programmes in Northern Mozambique where there are active terrorist threats					
Likelihood	Rare;	Unlikely	Possible,	Likely;	Almost Certain
	The NPO Assessment: The NPO has regular missions to provide aid to Northern Mozambique a high-risk jurisdiction for both terrorism and Terrorist financing. This has been identified by the organization as a potential risk indicator				
Impact	Insignificant	Minor	Moderate	Major	Severe
	Operational disruptions		Management considers that in the event that the aid provided is suspected of being diverted for terrorism or for financing terrorists, this would have short term disruption to the overseas operations as aid beneficiaries will be delayed and the organization may need to re-channel resources to address the need. The management has rated the Impact as **Moderate**		
	Reputational Losses		Management has assessed the reputational losses to be Major in the event that the aid provided is suspected of being diverted to support terrorist and/or terrorism activities. Concerns may be raised regarding the credibility of the organization.		
	Financial Losses		Management has assessed that the immediate financial losses is likely to be Minor as such missions are only a small part of the organization's overall activities.		

	Legal Implications	Management has assessed the legal implications to be Moderate on the ground that the overseas missions do not form the bulk of the organization's activities and any diversion of aid in support of terrorism or terrorists may have possible legal/criminal consequences under the law and/or legal suits from victims of terrorist activities.

The management has determined that the appropriate likelihood rating would be Likely (4) and the Impact rating would be Major as shown in the XY plain below



7.0 COMMUNICATE AND MANAGE

This involves communicating and establish Action Plans to manage risks.

7.1 The results of the risk scoring should be communicated to the governing board members and other stakeholders as risk management often requires buy-in from governing board members and the commitment from other stakeholders who may not be the primary risk owners.

7.2 It is part of the fiduciary/trust duties of governing board members to ensure that appropriate measures are implemented to mitigate the identified risks so as to ensure proper control and management in the administration of the NPO.

7.3 NPOs should adopt a risk-based approach towards managing the identified TF risks. This is achieved by prioritizing the management of critical risks. That is, TF risks that fall within the red zone of the matrix.

7.4 Action plans established should ideally include recommendations from risk owners and circulated to all stakeholders upon approval.

7.5 Four measures of risk management are:

7.5.1 **Risk Acceptance**

This involves acceptance of the consequences that arise when a risk occurs. It is Viable for minor risk where the cost of mitigation would be greater over time than the potential loss or damage sustained by the NPO, and if the risk is not contrary to public interest. NPOs may decide to carry on with certain activities on a case-by-case basis, subject to the relevant approvals by the authorized personnel, with appropriate safeguards in place.

7.5.2 **Risk Reduction**

This involves cutting the severity of the loss when a risk occurs and can be achieved through implementing appropriate and viable mitigating measures. NPOs can implement controls and measures to reduce the likelihood or impact of risks.

7.5.3 **Risk Avoidance**

This involves pulling back the activity that would carry the risk and may be useful in circumstances when the loss or damage sustained would be greater than the benefits of conducting an activity. NPOs that lack experience or resources in conducting certain activities in a particular environment may opt to avoid carrying out the activity altogether.

7.5.4 **Risk Sharing**

This involves sharing the burden with a third party to implement measures in mitigating the risk. The chosen third party should be able to demonstrate a higher capability in managing the risk. A smaller NPO may consider collaborating with more established NPO to carry out certain activities as such NPOs generally have more resources to ensure risks can be managed appropriately.

8.0 MONITOR

This entails ensuring Effectiveness of Action Plans and Review Risk Profile and refers to the process of evaluating the effectiveness and relevance of action plans periodically.

8.1 NPOs should periodically review the risk assessment or when there are material trigger events, whichever is earlier, as action plans may become irrelevant or outdated over time.

8.2 When determining the frequency of review, NPOs should primarily consider their risk profiles, changes in the landscape where the NPO operate in and secondarily, the availability of resources.

8.3 A review should be conducted at least once a year to ensure that the NPO's risk profiles remain up-to-date.

8.4 As part of the monitoring, NPOs should also assess whether they are able to meet the internal timelines for actions set previously to manage the risks.

9.0 REPORT

This entails the outcome of monitoring of the risks through Communicating risks. It involves informing the respective risk owners in the organization of the outcome derived from monitoring of risks.

9.1 Risk owners should exchange critical information about the findings with each other so that they can collectively develop and implement follow-up actions to be taken.

9.2 NPOs should keep a copy of the risk assessment and related documentation for a period of at least five years.

10.0 TF RISK INDICATOR

10.1 In identifying the Risks, NPOs can use the checklist below to ascertain if they have potential exposure to TF risk(s).

INDICATOR	YES	NO
1. **Donors, Beneficiaries, Partners, Employees and Volunteers**		
(a) Does the NPO accept donations from unusual donors or donors who are new or unknown to the NPO without first performing due diligence on such donors?		
(b) Does the NPO provide financial assistance or services to beneficiaries without first performing due diligence on the beneficiaries to ensure they are qualified and bona fide individuals?		
(c) Does the NPO establish working relationships with partners (including vendors) without first performing due diligence on these partners?		
(d) Does the NPO hire employees or engage volunteers without first performing due diligence on the individuals?		
(e) Does the NPO accept donations that come with conditions attached (e.g. donor requests for donation to be utilized for a specific group of individuals or organizations)?		
2. **Delivery and Operational**		

(a) Does the NPO have high volume of donations and disbursements, which make identifying suspicious activities difficult?		
(b) Does the NPO disburse funds through high-risk financial channels or non-regulated financial channels? For example, using cash, cash couriers or virtual assets?		
(c) Does the NPO disburse funds through an intermediary such as another NPO or partner which may be used to hold or transfer funds to a particular region outside of United Republic and make payments on the NPO's behalf?		
(d) Does the NPO operate without providing training or disseminating information to increase awareness among employees and volunteers about the risks and corresponding safeguards in relation to AML/CFT?		
(e) Does the NPO carry out its activities without written policies and procedures for disbursements and utilization of donations?		
(f) Does the NPO lack a formal channel to report suspicious activities or transactions noted in its operations?		
3. **Geographical Areas**		
(a) Does the NPO have operations, missions or programmes in an environment where there is an urgency to provide aid? For example, providing emergency aid in natural disaster zones where there may be weak banking infrastructure		
(b) Does the NPO engage in missions or programmes located in:		
(i) an area of conflict where there is an active terrorist threat; or		
(ii) domestically in a country where there is no conflict, but within a population that is actively targeted by a terrorist movement for support and cover?		

10.2 If your responses to any of the questions above is "Yes", it is recommended that you perform a TF risk assessment using the risk assessment methodology described in this guide.

11.0 FUNDAMENTAL PRINCIPLES OF GOOD PRACTICES:

11.1 Adoption of Best Practices:

11.1.1 NPOs must take appropriate steps to identify and assess the ML/ TF risks for donors, customers/ beneficiaries (including persons, group of persons and organizations, etc.), country specific or geographic areas, products, services, transactions and delivery channels. Based on risk assessment, the NPO shall take measures to mitigate the risks.

11.1.2 Training of employees and staff on AML/CFT strategy and issues may be conducted on an annual basis. Record of such trainings may be maintained.

11.1.3 NPOs shall not indulge in activities that amounts to breach of security or in any activity inconsistent with national interests, or contrary to Government policy.

11.1.4 NPOs shall also not take part or assist in any kind of political activities, conduct research or surveys unrelated to their activities. Violation may lead to cancellation of their license and/or registration.

11.1.5 NPOs shall not engage in money laundering, terrorist financing, weapon smuggling, anti-state activities or maintain links with the proscribed individuals or organizations.

11.2 Good Governance:

11.2.1 The management must have in place adequate measures to clearly identify every board member, both executive and non-executive.

11.2.2 The most important element of a successful AML/CFT program is the commitment of senior management, including the chief executive officer and the board of directors, to the development and enforcement of the AML/CFT objective.

11.2.3 The management must frame its AML/CFT Risk and Compliance Policy, which shall be approved by the Board of Directors and be publicly made available. The NPO shall review the said policy on an annual basis. Management must communicate updated version of the policy clearly to all employees on an annual basis along-with statement from the chief executive officer.

11.2.4 The management must also consider to establish an independent and well-resourced compliance function within the NPO to achieve the objective of AML/CFT Risk and Compliance Policy.

11.2.5 Based on a risk-based approach, the NPOs may consider forming an independent oversight committee of its operations, and each NPO must select the oversight structure, which best suits its needs.

11.3 **Know Your Beneficiaries and Partners:**

11.3.1 NPO must ascertain correct and complete identification particulars of each of its beneficiary (person, group of persons or organization etc.) who receives cash or services or in-kind contributions.

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

11.3.3 In case where the projects are implemented through partnership agreements with other partners, the NPO shall make it a part of its project agreements that partners shall maintain and share beneficiaries' information. NPOs must ensure that the partner organizations shall not be from any such organization whose license has been revoked or registration cancelled by other authorities.

11.4 **Know Your Donors:**

11.4.1 Before receiving funds from a donor, NPOs must establish that the donor is not placed on the United Nations' list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.

11.4.2 Before receiving funds from a donor, NPOs must establish that the donor is not placed on the United Nations' list of persons who are linked to terrorist financing or against whom a ban, sanction or embargo subsists.

11.4.3 NPOs shall undertake best efforts to document the identity of their significant donors. NPO must collect and maintain record or correct and complete identification particulars of major donors.

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

11.5 **Know your Employees:**

11.5.1 NPO must maintain records of particulars of its employees (both Tanzanians or foreign nationals), including but not limited to permanent address, present address, copy of National Identity, passport number, nationality, personal email ID, Tax Identification Number, phone or mobile number, past experience, etc.

11.5.2 These guidelines put in place the procedure that citizens can use to obtain information on the income and expenditure of an NPO that implements a project that has been funded in their area. (Public engagement).

11.6 **Ensuring Transparency and Financial Accountability:**

11.6.1 **Soliciting Donations:**

Any solicitation of donations must clearly state the goals and purposes for seeking funds (how and where these donations are to be expended) so that the donors as well as persons examining the NPOs disbursement of funds can check as to whether the funds are used against the determined goals.

11.6.2 **Receipt and disbursement of Donations and Funds:**

(a) NPO must receive all donations and funds through banking channel and which must be in conformity with the books of accounts of NPO.

(b) The identity of depositors and withdrawers must be ascertained by the NPO.

(c) The NPO should account for all disbursements including the name and particulars of grantee, the amount disbursed, date and form of payment. Disbursements may be made through proper banking channel except in extreme circumstances, which may require cash or currency transactions. Detailed internal records of cash transactions, if any, may be kept and oversight needs to exercise while handling such disbursements.

(d) In case transactions with the parties including donors appear unusual or suspicious, regardless of the amount involved and whether or not made in cash, Registrars of NPOs shall consider to issue suspicious transaction report (STR). In addition, transactions which give rise to a reasonable ground of suspicion that may involve financing of activities relating to terrorism, shall also be reported to FIU.

11.7 **Utilization of Funds:**

11.7.1 NPOs receiving legitimate foreign contributions or foreign economic assistance shall appropriately utilize these financial resources on the agreed areas of public welfare, simultaneously ensuring due monitoring, accountability and transparency of their governance, management and funding streams.

11.7.2 Some NPOs are running projects that generate profit. In addition, these guidelines provide that the profits generated be invested to foster the objectives of the NPO instead of being distributed to members or leaders. Also, the funds remaining

(surplus) after the project's slippages are meant to be counted as part of the NPO's income and used in the NPO's activities.

11.8 **Internal Audit**

11.8.1 NPOs may consider to set up an internal audit function to help identify risks, provide an assurance to the board of directors on NPO's risk management effectiveness, internal control and governance processes.

12.0 RED FLAGS/HIGH RISK INDICATORS FOR NPOs

12.1 **Donations:**

(a) If unusual or substantial one-time donations are received from unidentifiable or suspicious sources.
(b) if a series of small donations are received from sources that cannot be identified or checked.
(c) 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.
(d) where donations are made in a foreign currency or foreign sources where financial regulation or the legal framework is not as rigorous.
(e) where donations are conditional to be used in partnership with particular individuals or organizations where the NPO has concerns about those individuals or organizations.
(f) where an NPO is asked to provide services or benefits on favorable terms to the donor or a person nominated by the donor.
(g) where payments received from a known donor but through an unknown party.
(h) where donations are received from unknown or anonymous bodies.
(i) where payments received from an unusual payment mechanism where this would not be a typical method of payment.

12.2 **Beneficiaries:**

(a) 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.
(b) where an NPO provides services to large numbers of beneficiaries, where it may be easier to disguise additional beneficiaries.
(c) where there may appear signs that people may have been placed on distribution and aid lists by providing kickbacks and bribes to officials.
(d) lists of beneficiaries contain multiple manual corrections, multiple names may appear, may contain more family members.
(e) evidence that third parties or intermediaries have demanded payment for recommending or nominating beneficiaries.

(f) fake or suspicious identity documents.
(g) beneficiaries with identical characteristics and addresses or multiple or similar names and signatures.

12.3 **Partners:**

(a) the project proposal is vague or lacks adequate financial or technical details.
(b) the structure or nature of the proposed project makes it difficult to identify the partner and verify their identity and details.
(c) the proposals include delegating work to other unknown partners or newly formed organizations.
(d) it is difficult to contact the partner at their main address, or their telephone numbers are not working.
(e) 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.
(f) partners request unnecessary or unusual levels of privacy and secrecy.
(g) requests by partners to use a particular auditor or accountant.

12.4 **Employees:**

(a) indications that staff may be living beyond their means or appearing at unusual times.
(b) staff carrying out tasks or jobs they should not be, or other unusual staff behavior or conduct.
(c) sudden or increased staffing costs.

12.5 **Monitoring of Projects:**

(a) invoices and paperwork have been tampered with, altered in crucial aspects with handwritten amendments.
(b) inventory shortages.
(c) there is a lack of evidence to show fair and transparent tendering or procurement procedures.
(d) invoices and papers recording a higher cost for goods or services than expected or agreed.
(e) 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.
(f) signatures confirming receipt or payment are missing or the invoice is unsigned or undated.
(g) receipts have been signed and dated a long time after the goods or services should have been delivered.
(h) particularly late or early invoicing.
(i) repeated excuses of system crashing, losing records or paperwork.
(j) relief, goods or items provided by the NPO in connection with the project have been tampered with.
(k) documents accompanying goods and items are missing.

(l) the local community is receiving aid or assistance by other unexplained or unexpected means.
(m) unexpected transactions, where commission charged or no receipts are available.
(n) figures in documents or records that look familiar or may be repeated.
(o) discrepancies between budgeted needs and payments requested.
(p) requests for payment in cash to be made to an unknown third party or other organization.
(q) payment of administration costs not appearing to relate to the project or which appear unusually high taking into account the nature of the project.
(r) cash advances and payments that are unusually frequent and/or have not been recorded or approved.
(s) funds are not being banked or accounted for.
(t) infrequent and/or poor reconciliation of local banking and accounting records / bank reconciliations not done in a timely manner.
(u) payments to suppliers via cash payments to employees.
(v) 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.
(w) requests to use particular officials in the locality for monitoring purposes.
(x) 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.
(y) inconsistencies between narrative reports and financial claims and reports.

13.0 RECORDS KEEPING

13.1 NPOs should establish internal control and monitoring system to ensure that funds and services are being used as intended. For example, NPOs should clearly define and document the purpose and scope of their activities, identify beneficiary groups, and consider the risks of terrorist financing and risk mitigation measures before undertaking projects. They should maintain detailed budgets for each project and generate regular reports on related purchases of expenses. NPOs should establish procedures to trace funds, services, and equipment, and carryout transactions through the financial system, when possible, to maintain transparency of funds and mitigate the risk of terrorist financing. Project performance should be monitored on a regular basis by verifying the existence of beneficiaries and ensuring the receipt of funds, NPOs should take appropriate measures, based on the risks, to account for funds and services delivered.

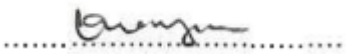
13.2 To demonstrate compliance with the laws and to allow for timely access to records by the registrars, NPOs should establish a document retention policy that provides for the maintenance of a broad spectrum of record, including donor and beneficiary identification data, business transaction record, internal and external reporting and training records, as well as analysis done. Business Transactions should be maintained for a minimum of ten (10) years.

14.0 EFFECTIVE DATE

These Guidelines shall become effective on 20th July, 2023

15.0 APPROVAL

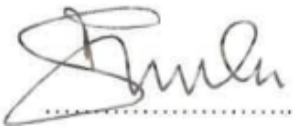
These guidelines were developed by FIU in collaboration with the NPOs Supervisors in Tanzania who append their signatures below:



Vickness Mayao
REGISTRAR OF NGOs
TANZANIA MAINLAND

Ahmed Abdulla
REGISTRAR OF NGOs
ZANZIBAR

Emmanuel Kihampa
REGISTRAR OF SOCIETIES
TANZANIA MAINLAND



Fatma Simba
COMMISSIONER
FINANCIAL INTELLIGENCE UNIT