# GUIDANCE FOR FOUNDATIONS AND ASSOCATIONS

## Understanding the Risks of Terrorism financing abuse and how to mitigate them

## - November 2023 -

# Table of Contents

[Introduction and Scope 3](#_Toc150897623)

[Introduction 3](#_Toc150897624)

[Scope of Guidance Paper 3](#_Toc150897625)

[Contact details 3](#_Toc150897626)

[Misuse of the Non-Profit Sector 4](#_Toc150897627)

[Categories of NPO Misuse 4](#_Toc150897628)

[Best Practices to Mitigate the Risk of Abuse 6](#_Toc150897629)

[Introduction of Internal Rules 6](#_Toc150897630)

[Understand your Geography 6](#_Toc150897631)

[Screening TF-related Sanctions Lists 7](#_Toc150897632)

[Use of Secure Payment Channels 9](#_Toc150897633)

[Cooperation among NPOs 9](#_Toc150897634)

# Introduction and Scope

### Introduction

1. Non-Profit Organizations (NPOs) are vital stakeholders for domestic and global communities, as their philanthropic nature as well as social and cultural activities improve quality of life for individuals, communities, and nations. Similar to other entities, NPOs vary with regards to their structures, missions, scopes, target audiences, and areas of activity. Especially regarding the latter, this means that some NPOs work in highly vulnerable geographic areas, while others might directly or indirectly aid high-risk communities overseas that are located in conflict zones.
2. Yet, the willingness and efforts exerted by NPOs to help people in need, especially in higher-risk jurisdiction, also raises their risk of being potentially abused for terrorist purposes. The abuse of NPOs for terrorism financing (TF) purposes can be deliberate, inadvertent or coercive, and the forms in which such abuse can take place are manifold (e.g. creation of fictitious NPOs, obtaining financial benefits from a NPO’s activities, concealing the illegal diversion of funds donated to a NPO).
3. Despite being at risk of TF abuse, NPOs can take concrete measures to mitigate the risks. Not only would a lower TF risk contribute to greater confidence by the local and international donor community, but it would also aid financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) to appropriately assess risks that NPOs carry from a customer perspective. With FIs and DNFBPs being subject to AML/CFT regulations, increased NPO transparency would allow them to enhance their understanding of what risks NPOs carry, thus helping to ensure that only the necessary safeguards are taken when it comes to onboarding and maintaining NPOs as customers. Ultimately, this would result in NPOs obtaining easier access to the services of FIs and DNFBPs.

### Scope of Guidance Paper

1. This guidance paper has been issued by the Department of the Interior to assist Monegasque associations and foundations (collectively referred to as NPOs) in understanding the TF risks they could be exposed to, how these can be identified, and ultimately what means exist to mitigate the potential risks of TF abuse.
2. The information contained in this paper does not in any way whatsoever constitute legal advice, and should be read in conjunction with relevant national legislation, international standards, and other guidelines issued by the Department of the Interior or other competent agencies (e.g. Department of Budget and Treasury, SICCFIN, DSP).

### Contact details

1. For any enquiries, comments or feedback regarding this guidance document please contact the Department of Interior.

Email: [**click here**](https://contacts.gouv.mc/en/contact-department?localisation=6714&contact=8038&source=http://en.gouv.mc/content/view/full/6714)

Phone Number 1: (+377) 98 98 84 56

Phone Number 2: (+377) 98 98 82 52

# Misuse of the Non-Profit Sector

1. International case studies have highlighted that NPOs are vulnerable entities for TF abuse. Generally speaking, NPOs can become involved in TF in two main scenarios: either by being used to raise funds and/or serve as channels to transfer funds within and between jurisdictions, or by providing cover, or direct logistical support for the movement of other resources (such as arms) or terrorists themselves. To a lesser extent typologies have also indicated that NPOs can play a part in the diversion and control of funds to recruit members and foster support for terrorist organizations.
2. The list of factors that make NPOs susceptible to abuse can be linked to their inherent characteristics such as their modus operandi, structures, and general public perception. Some of the main reasons that increase NPOs’ risks are the following:
	* Easy process for registering and being established
	* Decision makers are usually few people
	* Reliance on goodwill and voluntary support
	* Large number of people can directly come into close contact
	* Direct or indirect global presence and ability to move funds, supplies and people into or through regions
	* Multiple donors, investments, assets, and currencies for projects
3. It should be underlined that the above list is not exhaustive and that not all NPOs can be linked to these factors. Nonetheless, a mix of the listed factors may increase the vulnerability of a particular NPO to abuse, such as the region in which it operates and the key activities it pursues. Again, each NPO should be analyzed on a case-by-case basis.

### Categories of NPO Misuse

1. When trying to identify the various forms of abuse a NPO can become a victim of, international case studies provide generalizations of how misuse can occur (the different examples are described below). It is important to keep in mind that these categories, or their possible combinations, do indicate a severe type of abuse and NPOs should be aware of the specific situations and contexts that may lead to these scenarios occurring in real life. Generally speaking, NPOs more at risk of becoming victims of any of these categories are those that:
* operate in conflict zones
* operate in areas that are also targeted by terrorist organizations
* do not conduct their activities in a transparent manner (incl. management and personnel structure or financials)
* do not fulfil their statutory obligations
* do not exchange information on activities with their supervisory authority;
* lack cooperation and communication with other public authorities (especially law enforcement authorities)
* handle large amounts of funds, mostly in cash

#### Misuse of Funding

1. Funds may be raised under the name of a reputable and well-established NPO, but be used for terrorist rather than the indicated charitable purposes. If money gathered by a respectable NPO is disbursed cross-border — which is likely given the severity and scope of current humanitarian crises —it may be diverted by terrorist groups or their agents while in transit or at the destination country. In addition, a NPO may be used — wittingly or unwittingly — to transfer cash between jurisdictions or as a vehicle for money laundering. The risk of such abuse is heightened in situations where NPOs lack adequate financial controls.

#### Misuse of Assets

1. The physical assets of NPOs, such as offices and vehicles, may be used to store or transport weapons, cash, or people. Under the guise of working for a NPO that is well-known in the country or region, members of terrorist organizations may be granted unrestricted entry. In the worst case scenario, it could be possible to purport to be operating on behalf of a NPO in a jurisdiction within which terrorist training is being orchestrated. In addition, terrorist organizations may use the pre-established and essential communication channels of NPOs to create and maintain their own points of contact.

#### Misuse of the NPO’s name and status

1. A NPO may give money to a humanitarian aid organization, but that organization may simultaneously support terrorist activities. Alternatively, a NPO might collect donations for a specific cause and have a terrorist organization handle the distribution of those donations or provide support. An example of the latter are charities that work in Palestine and have alleged ties to Hamas.

#### Misuse of a NPO after a takeover

1. A NPO could be abused for its reputation, name and history. This could manifest itself in the form of a personnel take-over based on a membership principle – a larger number of new members sign up and they, in the voting procedures, succeed in diverting the course of the NPO’s activities. This can also manifest as taking over social media profiles that are managed by a particular NPO and their subsequent abuse.

#### Misuse of a NPO internally

1. A NPO may be abused from within by individuals who, for example, take money from donations and use it for terrorist purposes. Likewise, those members consent to meetings being held or the propaganda materials being created at the NPO’s offices. The NPO’s trustees may participate in pro-terrorist events and/or speeches, as well as invite speakers and volunteer workers whose opinions are likely to encourage the spread of extremist viewpoints.

#### Misuse of the notion of NPO status

1. A terrorist organization might decide to create a fictitious NPO that is registered and complies with all legal requirements. As such, donations could be lawfully requested, handled, and distributed, and if managed effectively, the NPO could also employ a number of employees who are oblivious to the real source of donations or the final destination of the funds. The following are possible means of achieving this kind of misuse:
* NPOs may be used to raise funds for terrorist organisations and transfer funds and other resources across borders using NPOs with a known international remit for this purpose.
* NPOs could be defrauded at branch level or via aid workers with budgetary responsibility and/or control.
* funds can be leveraged so as to facilitate the recruitment of members from whom support for terrorist organisations and their ideologies can be garnered.

# Best Practices to Mitigate the Risk of Abuse

1. The cornerstones to reduce the possibility of TF misuse are the development of and adherence to preventive measures. Some of these measures are to be implemented once, while other mechanisms need to be continuously assessed and adjusted to reflect changes in the global environment, the NPO’s activities, and applicable legislations.
2. It is the goal of this section to inform NPOs of key best practices that have proven to mitigate risks of TF abuse.

### Introduction of Internal Rules

1. The probably most important building block that mitigates a NPO’s TF risks is the establishment of internal rules and regulations. Such processes aim at regulating the NPO and its functioning, thus guaranteeing better transparency, integrity, control over management, and decision-making. In addition, properly drafted internal rules also promote compliance with relevant legislation and any NPO-related obligations.
2. With lack of transparency often being associated with greater TF abuse, NPOs should seek to develop means that promote their own transparency as well as that of the entities or persons that they are associated with. Examples of transparency-promoting activities could be the conduct of internal risk assessment or undergoing regular financial and administrative audits. As such, NPOs should develop clear rules for their modus operandi.

**Elements to consider when developing internal rules:**

- a clearly defined **mandate and mission** (incl. individual programmes)

- the **statutes, mission**, etc. that stipulate the **distancing from any support of terrorism** or other criminal activity

- transparent **management of finances**;

- outlined **reporting/record keeping processes**

- clear authorities for **overseeing the distribution and withdrawal of funds**

- requirement to apply a **"four eyes" principle**

- conduct of regular **risk assessments**;

- regular **audits** (incl. assessments of how donations were used)

- **working processes** (incl. guidelines for public procurements, application of KYC[[1]](#footnote-1), etc.)

- regular **publication of complete information** about activities.

### Understand your Geography

1. NPOs need to understand that some geographical zones, which may range from a region within a jurisdiction to multiple countries, may pose higher risks of abuse than others. To date, no universally recognized criteria for assessing and determining risks in particular countries or geographic regions exist. However, it is important to highlight that exposure to any of the following does pose a greater risk of being abused for TF:
* regions where terrorists or terrorist organizations are known to operate
* countries subject to sanctions by the United Nations or other international organizations (see more below);
* countries or regions vulnerable due to internal conflict or criminal activity
* countries identified by the FATF as having weak AML/CFT Laws or those that lack proper enforcement of said laws. The list of countries classified by the FATF as such can be accessed [**here**](https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html).
1. In addition to the above, NPOs should conduct research and critically assess the following geography-related factors before deciding on whether or not to become operational in specific regions:
* strength of local laws and law enforcement
* the political environment and the ability of the receiving jurisdiction’s State to govern the region
* the extent and types of criminal activity in the region
* the size and reliability of Fis
* the main channels available for financial transactions

### Screening TF-related Sanctions Lists

1. The United Nations (UN), through its Security Council Resolutions (UNSCRs) and Sanctions Committees, aims to maintain peace and security, by mandating the implementation of freezing measures related to, among other things, terrorism and terrorist financing. By adopting resolutions aimed at blocking terrorists’ and terrorist organizations’ disposal of their financial assets and sanctioning persons, the objective of these resolutions is to curtail the movement of payments and capital related to terrorism.
2. The Principality of Monaco, as a member of the United Nations, is committed to implementing UNSCRs. Consequently, through Sovereign Ordinance No. 8.664 of May 26th, 2021 relating to procedures for freezing funds and economic resources in application of international economic sanctions (SO 8664) Monaco is also implementing relevant UNSCRs on the suppression and combating of terrorism and terrorist financing.

**Important Note**

Exemptions for humanitarian purposes may be granted so that civilians do not unduly suffer from sanctions. You can contact the Budget and Treasury Department (DBT) (click [**here**](https://contacts.gouv.mc/en/contactez-un-service-de-l-administration?localisation=6494&contact=49510) for the contact site), which is Monaco’s national coordinator for the implementation of international sanctions, regarding the scope of such exemptions and for exemption requests.

1. The UN maintains a Consolidated List (available [**here**](https://scsanctions.un.org/phkbnen-all.html)) which includes all individuals, entities, or groups that are subject to measures imposed by the UN Security Council (i.e. persons and entities that have been designated due to TF links). In addition to the UN’s list, Monaco also has its own National List, where it designates persons and entities on its own notion, which are not necessarily included in the UN Consolidated List. Considering the risks posed by TF, it is appropriate to restate that it is prohibited to make available, directly or indirectly, any assets to persons subject to sanctions, who are listed on either the UN Consolidated List or Monaco’s National List, which is an obligation stemming from SO 8664.
2. To help NPOs remain up to date with the designation and de-listing of individuals, entities, or groups following decisions taken by the Minister of State, the DBT has provided the public with a free service to subscribe to its email notification system. Once subscribed, the system automatically sends notifications to those registered for every new listing or update to the list of designated persons or entities.

**Subscribe to the DBT’s Newsletter**

NPOs are requested to subscribe to the newsletter service (click [**here**](https://geldefonds.gouv.mc/en/newsletter/register)) as it allows the receipt of updated and timely information about the designation and de-listing of individuals, entities, or groups subject to sanctions regimes.

1. Once a notification of a change to the list of designated entities or persons is received via email, it is the NPO’s obligation to screen its databases to ensure that any potential designees are identified and successively have their funds and/or economic resources become immediately subject to freezing measures.
2. As a general principle, screening should be done when establishing a new relationship, to ensure the relationship is permissible, and then at regular intervals, either upon a trigger event or when underlying information changes, to validate that the relationship(s) remain permissible. Where either internal or external data sets change frequently, periodic screening may be as often as daily, but longer intervals between periodic re-screening may be acceptable in situations where change is less frequent or the risk of a potential sanctions exposure is lower.

**Important Note**

Finding a match to a donor, beneficiary, intermediary, collaborator, or beneficial owner with the data on these sanctions lists may indicate a suspicion of TF.

1. For further supporting information regarding the sanctions regimes applicable in Monaco, visit the DBT’s website (<https://geldefonds.gouv.mc/en>). The website also contains general as well as specific information on the implementation of international sanctions, guidance documents, TF-related typology reports and other relevant information to help NPOs understand their sanctions-related obligations.
2. When it comes to the actual screening process, NPOs should be screening the following:
* **Donors**

Receiving funding and subsidies is essential for NPOs because it allows them to carry out their missions and activities. It is possible to use private or smaller foundations and individual donations in addition to large institutional donors (e.g. states or international organizations). For NPOs that rely on individual, private donors it becomes especially important to thoroughly investigate the source of the donor’s funds, as these stem from terrorist organizations or come from illicit activities. In cases where the donors themselves do not have any control systems, the NPO should identify this as a potential risk in itself.

Opting for long-term framework agreements and financial support from major donors who have a solid track record, positive reputation, and an established system of operation, in general, significantly lowers the risk of engaging with donors that have TF links.

* **Collaborators, Contractors, and Suppliers**

Using the assistance of local organizations or individuals is often a necessity for a NPO’s security and effectiveness when providing material and financial support, particularly in conflict zones, remote areas, or politically isolated areas. The use of cash in such instances is also frequently required, which can make it difficult to maintain an overview of the actual cash flow. Therefore, it is essential for NPOs that operate in such areas to have access to complete and up to date identification data so that collaborators (internal and external) can be continuously screened.

Additionally, there is a risk that someone, even within a legitimate local organization, misuses the intended funds for terrorist activities without anyone else's knowledge. Given the high-level of staff turnover in the NPO sector, extra diligence should be exerted on checking the staff of local organizations that serve as intermediaries for the distribution of donations.

While using the UN Consolidated List or other applicable sanctions lists for basic and formal screening of collaborators and suppliers is an option, NPOs should also opt for on-site inspections and ad hoc visits to verify the persons that are acting as intermediaries (where possible).

**Important Note**

Screening of the core NPO employees, including those at the organization’s headquarters, should not be neglected.

* **Beneficiaries**

In general, screening beneficiaries of aid and assistance is required when delivering such. This is particularly true in situations where aid provided to beneficiaries located in conflict or crisis areas, since terrorist groups may be controlling entire communities. The risk is that a beneficiary’s legal representative is the direct recipient of a donation, and instead of forwarding said donation to the intended person, the funds or assets are given to terrorists, terrorism financers or terrorist organizations. An additional scenario could be the coercion of intended beneficiaries to force them to provide the entirety or parts of the funds or assets received to entities or persons linked to terrorism.

When selecting beneficiaries, NPOs should develop clear and transparent criteria. Said criteria should be documented in a formal governance document (e.g. the NPO’s internal procedures) and be made available to all employees and decision-makers. Such procedures, which ensure a certain form of control, are considered to be good practice.

**Procedures for deciding on beneficiaries**

- setting **clear and transparent criteria** for the selection of beneficiaries

- **vetting** the beneficiaries (incl. assessing whether all selection criteria are met **before** the actual distribution of donations)

- periodic review of **screening processes** (incl. screening of collaborators)

- **exchange of information** with other NPOs on potentially overlapping beneficiaries

- type of **funds and delivery channels needed** for reaching beneficiary

- **ad-hoc inspections** of beneficiaries, intermediaries, other parties involved

### Use of Secure Payment Channels

1. Using secure payment channels to transfer funds is one of the fundamental tools for risk mitigation. It is best to use non-cash payments and transparent bank accounts whenever feasible. However, using secure payment channels isn't always an option due to the nature of aid in various conflict or isolated areas. A few of the options include remittances (through a payment service provider) or non-cash transfers of funds (i.e. from one bank account to another bank account) to the closest jurisdiction, followed by cash withdrawals and transfers.
2. Tracking the flow of cash to the recipient and its subsequent use is necessary, even in situations where it is not possible to directly arrange a physical transfer of funds. Special care and thorough verification of all the individuals or entities involved needs to be maintained. It is important to always ensure that records of transactions within specific transaction channels are kept, including the identification of the final recipient.

### Cooperation among NPOs

1. A further approach to mitigating risks is the exchange of information with other NPOs. Currently, examples have shown that national and international collaborations occur within the NPO sector, with such collaborations proving beneficial to individual NPOs.
2. By cooperating with other local or regional NPOs, the exchange of information and experiences can be bolstered. The sharing of experiences and know-how helps NPOs strengthen their own measures by becoming informed of similar NPO’s stories, risks and implemented measures.
1. It is important to ensure that any KYC-related processes clearly stipulate that these have to be applied to **donors, contractors, collaborators, intermediaries, and final beneficiaries**. [↑](#footnote-ref-1)