MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

THE RISK OF AN NPO ABUSE FOR THE PURPOSES OF TERRORISM FINANCING

Public version

Updated 2025

Introduction

This material was developed in 2020 as part of the work of the Working Group on the Risk of Abuse of Non-State Non-Profit Organizations (hereinafter "NPOs"), coordinated by the Ministry of the Interior as part of the National Risk Assessment process on money laundering and terrorist financing. The document was prepared with the participation of representatives from the Ministry of Justice, the Ministry of Finance, the Ministry of Culture, the Ministry of Foreign Affairs, the Office of the Government, the Financial Analytical Office, the Police of the Czech Republic, the General Financial Directorate, the National Sports Agency, and the intelligence services. It was also consulted with representatives of the Czech National Bank and the non-profit sector.

The text also reflects the evaluation of the Czech Republic under the 5th round of mutual evaluations in the field of anti-money laundering and counter-terrorist financing, and the resulting report, which identified the absence of a risk assessment in this area as one of the detected deficiencies. It is therefore part of the implementation of the related Action Plan, approved by the Government of the Czech Republic on 8 July 2019 by Resolution No. 488, and contributes to the proper implementation of FATF Recommendation No. 8[1] in the Czech context.

The current version of the text was updated in 2025. Its revision is based on feedback from involved partners, changes in the global security situation, and the development of new methods of terrorist financing driven by advances in new technologies.

Together with the *Analysis of the Non-Profit Sector in the Czech Republic from the Perspective of Terrorist Financing Risks* and the *Awareness-Raising Guide for the Non-Profit Sector in the Area of Combating Terrorist Financing*, this document forms the conceptual and analytical framework of the Czech Republic's efforts to prevent the misuse of non-profit organizations for terrorist financing.[2]

Non-state non-profit organizations (NPOs) play an important role in the Czech Republic in many areas, such as building civil society, providing humanitarian and development aid, delivering social services, promoting advocacy and interest-based activities, and other activities of general benefit.

However, some NPOs — or entities pretending to be NPOs — may be misused in terrorist financing schemes. Such cases are not common in the Czech Republic at present, but their occurrence could represent a significant threat to the country's internal security. Therefore, this area requires adequate attention — especially since the misuse of an NPO can occur even without the deliberate involvement of its representatives.

In this document, the term *terrorist financing* is understood in a broad sense, encompassing both material and non-material support to terrorist entities. Where the text refers simply to "persons," this may mean either natural or legal persons.

The aim of this material is to identify the threats that Czech or Czech-based NPOs may face, to detect potential vulnerabilities, and thereby enable control mechanisms to focus on the potentially highest-risk NPOs. More broadly, it aims to support the effective application of a risk-based approach to the supervision of NPOs. Another goal of this document is to serve as a basis for introducing and sharing good practices among NPOs, helping to reduce their risk exposure in areas where possible. This material will also serve as a basis for training NPOs in the field of terrorist financing prevention. It will

[1] The **Financial Action Task Force (FATF)** is an international intergovernmental organization that sets standards and issues recommendations in the field of combating money laundering and terrorist financing.
[2] https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

be distributed to all public authorities that provide grants or other support to NPOs and need to assess the risk level of potential recipients.

This material may also serve as one of the reference documents for assessing the risk profile of other legal entities — for example, those receiving funds from grant programs or acting as suppliers of goods and services to public authorities. However, when used in this context, the specific differences between such entities and NPOs must be considered. NPOs themselves may also use it when selecting suppliers, foreign partners, or screening donors, as most of the risk factors listed below are of general relevance.

The purpose of this material is *not* to introduce new control mechanisms for NPOs or to impose new obligations on them. In line with FATF recommendations, all measures are applied in a risk-based and proportionate manner, so as not to impose unnecessary burdens or restrictions on legitimate NPO activities — particularly those of humanitarian actors.

This document is available in two versions: a **non-public version**, which contains the full text and is intended only for public authorities, and a **public version**, which omits some of the risk factors.

Definition of Selected Terms

For the purposes of this material, the following definitions are used:

Non-State Non-Profit Organization (NPO)

In accordance with the interpretive note to FATF Recommendation No. 8, non-state non-profit organizations are understood in functional terms — that is, as entities (which in the Czech context are typically legal persons) that collect or distribute funds for charitable, religious, cultural, educational, social, or other purposes, or for any other activity serving the public interest.

High-Risk Country

A country in which an armed conflict or terrorist group activities are taking place; a country in their immediate vicinity; a country that is culturally, historically, or otherwise linked to them; or a country that can be considered high-risk for other reasons. This category also includes countries appearing on sanctions or related lists, as well as high-risk third countries within the meaning of the Anti-Money Laundering (AML) Act — that is, countries whose regimes for combating money laundering and terrorist financing have significant deficiencies.[3]

High-Risk Person

A person who has previously been convicted of a criminal offense or is currently under investigation for one; a person involved in the activities of terrorist or extremist entities; or a person originating from, or otherwise linked to, high-risk countries. This definition also includes individuals listed on sanctions lists,[4] fictitious persons, and persons related to or otherwise connected with high-risk persons.

[3] https://www.fau.gov.cz/cs/rozcestnik/legislativa-a-metodika/stanoviska-fau/vysoce-rizikove-treti-zeme-826

[4] Whether a person is subject to **European Union sanctions** can be verified via the EU Sanctions Map: https://www.sanctionsmap.eu/#/main.
Whether a person is subject to **national sanctions** can be verified via the **Czech national sanctions list**: https://mzv.gov.cz/jnp/cz/zahranicni_vztahy/sankcni_politika/sankcni_seznam_cr/vnitrostatni_sankcni_seznam.html.

How to use this document in practice?

The way this material is used in practice will vary significantly depending on the specific entity working with it — its needs, available information, and human and other resources. Therefore, it is not possible to propose a single uniform procedure for applying or using the risk factors listed below. Similarly, the material will need to be applied differently when assessing the risk profile of a small local NPO compared to that of an international NPO with hundreds of employees.

This material does not prescribe a uniform course of action following the assessment of a specific NPO's risk level. In addition to the standard procedures applied by individual entities, it may be appropriate to inform the NPO itself if it is considered risky from a certain perspective, thereby giving it an opportunity to take corrective measures — or, in cases of suspected criminal activity, to inform the Police of the Czech Republic.

General Notes on the Availability of Information for Assessing Individual Factors and Their Selection

The list of risk factors provided below is comprehensive. Each assessing entity should select from it only those criteria that are relevant and assessable given its specific focus. Individual risk factors will generally be evaluated by entities on an *ad hoc* basis — when a specific need arises (for example, during an inspection or before deciding on the granting of public support). However, for some entities, it may be more appropriate to conduct ongoing assessments of certain factors.

Suitable sources of information for such evaluations may include data available from public registers, databases (including non-public ones), and records; information published by the NPO itself on its website (including annual and other reports) or social media profiles; and information from the media and other open sources — searchable, for example, by the name of the NPO or its representatives. Additional insights may come from data accessible to specific entities by virtue of their legal authority (e.g. information on financial transactions) or obtained through direct communication with the entity concerned.

Another category of readily available information includes data already held by the assessing entity as a result of prior communication with the NPO, data obtained continuously through its regular functions, or information that can be easily acquired by contacting the NPO directly. In justified cases, it is of course also possible to request information from other public authorities, including through consultation and the exchange of relevant information within the appropriate working group.

Below, several possible practical applications of this material are presented, corresponding to the anticipated roles of different entities that may use it.

A) Providers of Public Support or Contracting Authorities

For these entities, it is important to ensure that financial resources are not provided to high-risk entities or directly misused for illegitimate purposes. When granting financial support, such entities usually have the opportunity to request a range of information about an NPO in advance. In this context, it is advisable to consider certain risk factors listed below when preparing, for example, grant procedures or other processes requiring NPOs to provide specific information. Public support providers are also authorized to monitor the use of granted funds, giving them access to additional information

that can help better assess the risk profile of a particular NPO in the future. These entities will generally assess the risk level of NPOs on an *ad hoc* basis, as needed.

B) Supervisory or Control Authorities

For these entities, it will generally be important to target their oversight activities toward higher-risk NPOs. A control authority will likely apply easily assessable criteria to a larger group of NPOs in order to focus its efforts on those assessed as higher risk. At the same time, such authorities — given their powers — will have access to more detailed information about NPOs that is not publicly available. Continuous risk assessment of relevant NPOs is also possible for entities with supervisory authority.

C) Law Enforcement Authorities and Intelligence Services

For these bodies, the list of risk factors may serve as a guide when investigating specific NPOs suspected of engaging in criminal activities or actions threatening the interests of the Czech Republic. These entities, by virtue of their powers, will have access to the most extensive range of information about NPOs and will generally investigate only a small number of entities based on concrete suspicions.

D) Non-Profit Organizations (NPOs)

For NPOs themselves, the list of risk factors can serve as a tool for increasing their resilience and reducing the risk of being misused for illegitimate purposes. Some risk factors can be relatively easily mitigated by improving transparency, implementing internal control mechanisms, and raising staff awareness of potential risks. NPOs may also conduct regular self-assessments of their risk exposure, taking into account the nature of their activities and available capacities.

This material may also be useful when an NPO establishes contact with a new or previously unknown partner or supplier (for example, in a foreign country) and needs to assess the risk level of potential cooperation. Similarly, NPOs can apply these factors when approached by an unfamiliar entity. Many of the risk factors listed below can also be used for donor screening, as most of them are broadly applicable to all legal entities.

A separate educational document has been developed to raise NPOs' awareness of risks and help them reduce their own risk exposure. This material is available on the website of the Ministry of the Interior, including an English-language version.[5]

E) Private Entities Providing Services to NPOs

This material can also be useful for private entities that provide services to NPOs — especially services that, by their nature, could be misused for terrorist financing (e.g., financial institutions offering transaction intermediation, account management, crypto-asset-related services, or other financial services).

[5] https://mv.gov.cz/chh/clanek/terorismus-web-dokumenty-dokumenty.aspx

Possible NPO abuses

In general, it can be stated that the misuse of an NPO or its status may occur in several ways, as identified both in FATF typologies and in the inputs provided by members of the working group:

1. **Deliberate misuse of NPO funds or the NPO itself** – The NPO, or one of its staff members, intentionally uses the NPO's financial or other resources to directly support a terrorist entity or its infrastructure. Proceeds from criminal activity may also be laundered through the NPO with its knowledge. The NPO's training or educational programs, or even its identity, may also be misused.

2. **Unintentional misuse of NPO funds, activities, or the NPO itself** – Humanitarian or other aid provided by the NPO in a conflict area may also be exploited by a terrorist entity. Infrastructure built by the NPO (e.g. hospitals, schools, energy, or water sources) may be used by a terrorist group without the NPO's knowledge. The NPO's training or educational programs may also be misused — either through the influence of terrorist entities (for example, acting as instructors) or by being used in support of these entities (such as survival or first aid courses). Misuse may also take the form of theft or embezzlement of NPO funds without the NPO's knowledge.

3. **Connection between an NPO and a terrorist entity** – The NPO supports a terrorist entity, passes on information, is linked to it through personnel ties, legitimizes its activities, or provides cover for it. Such links can also be unintentional — for example, when a terrorist entity pretends to be a legitimate partner for humanitarian assistance in a conflict zone.

4. **Misuse of the NPO's reputation or achievements** – A terrorist entity claims the NPO's successes as its own and exploits them for recruitment or to gain local support or directly pretends to represent the NPO in the area and "collects" funds on its behalf.

5. **Fake NPO** – A terrorist or state entity establishes an NPO for the purpose of obtaining or transferring funds while concealing its actual activities, including those related to terrorist financing. This may also include exploiting an established NPO's brand — such as its name or logo — by the above-mentioned actors.

6. **Takeover of an NPO and its subsequent misuse to support a terrorist entity** – Exploiting the good reputation and history of an NPO, for instance by personnel infiltration in membership-based organizations: a large number of new members join, vote to change the leadership and direction of the NPO, or take over the NPO's social media accounts and misuse them.

7. **Financial benefit of a terrorist entity from an NPO's activities** – Either through direct payments collected from the NPO as a "fee" for allowing it to operate in an area controlled by a terrorist entity, or through local suppliers linked to such an entity who are obliged to pay it taxes, fees, or other payments (e.g. extortion or protection money).

Risk factors increasing the possibility of the abuse of an NPO

The risk of misuse of an NPO for the purpose of terrorist financing is assessed through the lens of specific **risk factors**, which—when considered collectively—may serve as grounds for conducting an inspection of a particular entity or taking other measures against it. However, these factors, or even their combination, do not in themselves necessarily constitute a clear indication of NPO misuse.

It should also be noted that for some NPOs, certain factors are **inherent characteristics** (for example, activities in a specific geographic area) that the NPO cannot avoid without abandoning its core mission. Such factors should be recognized by the NPO and **actively mitigated** through appropriate preventive measures. Some of these factors may arise not only from deliberate actions by individuals within the NPO but also from ignorance of legal norms and statutory obligations, or from unintentional behaviour or omission.

Similarly, in certain situations—particularly when an NPO operates in countries with **repressive regimes**—it may have to use alternative channels for the provision and receipt of funds (e.g. transporting cash across borders, non-cash transfers made in the name of an individual employee of the organization, use of traditional informal systems, etc.), since in some countries, the financing of local citizens by a foreign NGO may cause serious problems for the beneficiaries. Many developing countries also restrict the transfer of funds abroad.

The following text describes and comments on each factor, including its **importance within the set of risk factors**, rated on a **low–medium–high scale**. This parameter reflects both practical experience and findings from international standards and FATF methodologies as of the end of June 2025. The assessment represents **expert judgment** by members of the working group.

A **high level of importance** indicates a greater risk of NPO misuse due to the presence of a particular feature—it serves primarily as a warning indicator but may also correspond to a greater potential impact that misuse of the NPO could have on society. **Low-importance factors** are those that do not, by themselves, necessarily indicate a risk of misuse (and may stem from mere negligence, lack of knowledge, or inconsistency by NPO representatives). Conversely, **high-importance factors** are typically those that, on their own, may represent a risk of NPO misuse.

Each **risk factor must be assessed in the context of the specific NPO**. For example, failure to publish financial statements has a very different level of significance for a small local association with no assets or funds compared to a large NPO with a multimillion-crown budget. Therefore, this document does not propose any scoring or ranking system for NPOs based on risk factors, as no universal system could be applied across the diverse range of NPO forms.

For each factor, the **possibility of detection** is also indicated—particularly where it may be inferred from public sources prior to contacting the NPO directly. Given the diversity of factors, it is clear that some can be easily detected from public information, while others cannot be identified without close interaction with the specific NPO or access to non-public information sources.

In general, and in line with FATF methodology, the highest-risk NPOs in terms of potential misuse for terrorist financing are those operating in high-risk or unstable areas, whose activities, governance, staffing structure, or financing lack transparency, and which have no functional control mechanisms, fail to meet legal obligations, do not communicate with the public or supervisory authorities, and handle large amounts of funds, mainly in cash.

Conversely, lower-risk NPOs are typically those with a local focus, operating only within the Czech Republic, handling little or no cash, and possessing minimal or no assets. However, even organizations operating solely within the Czech Republic can still face some risk of their facilities being misused to support terrorism.

It should be added that, based on available evidence from practice, the **majority of Czech NPOs**—especially those operating in conflict areas—demonstrate **sufficient awareness of terrorist financing (TF) risks** and possess **fairly robust risk management systems**. The risk level of large NPOs operating across multiple countries is further reduced by the **strict oversight** of institutional and governmental donors (e.g. registration, framework agreements, and EU or UN grant schemes), as well as by the **NPOs' own risk management efforts**, particularly their **transparent operations**, including clear governance and staffing structures.

Risk factors categories

1) Public registers and registration

Code	Risk factor	Significance	Possible detection	Description and commentary
1A	A fictitious NPO	high	Checking public registries or open sources	The NPO is not listed in public registries, and therefore it is not a legal person according to the Czech law. There is a risk that the persons in charge might be only pretending to be an NPO.
1B	The NPO does not comply with legal obligations in relation to public registers	medium	Checking public registers in the context of legal obligations	The NPO does not submit financial statements, does not update its statutory bodies and other information, does not enter required documents – or only fulfils these obligations formally or belatedly – these documents do not contain complete information, or this information does not correspond to known facts.
1C	Lack of publicly available data on founding legal acts	high	Checking public registries, NPO website	No founding-related information is available, which would make it possible to identify the purpose and declared main activity of the NPO.
1D	Lack of information on the beneficial	low	Checking the records of beneficial owners	As a rule, these will be persons who are already listed in the public register (i.e. persons who are members of the statutory body).

	owner of an NPO[6]			
1E	NPO has a fictitious seat that does not correspond to the actual seat	medium	Attempt to serve a document, on-the-spot inspection	It is not possible to contact the NPO at its official headquarters, nor does it receive documents. This is linked to 5A.
1F	The name of the NPO is easily mistakable / interchangeable	medium	Checking public registries, NPO website	If an NPO uses a name similar to that of another, usually large and well-established, or international NPO, it may be easily confused with it, with the "unknown" NPO effectively parasitizing the reputation of the better-known organization.
1G	An NPO carries out activities that are not subject to (sectoral) inspection	low	The NPO carries out activities which only the Financial Administration is authorized to check	NPO is only subject to supervision for tax purposes, and there is only limited information available to the authorities on its activities.
1H	This risk factor is not part of the public version.			
1I	Unknown foreign NPO	medium	Checking public registries and their foreign counterparts	An unknown NPO can be a foreign NPO; considering different registration standards (e.g. foreign associations operating in the Czech Republic should also be registered in the appropriate register, but it is not fully possible to rely on it).

2) Focus of the NPO activities

Code	Risk factor	Significance	Possible detection	Description and commentary
2A	A local partner of an NPO is linked to activities associated with terrorism	high	Media, grant projects	If the information comes from reliable sources.
2B	The NPO's activities have the potential to assist undesirable	high	NPO website, public registers, annual	Activities that support, for example, survival in the wilderness, handling of weapons, martial arts training,

[6] In the context of an NPO, this primarily refers to those individuals who ultimately exercise **decisive influence** within the legal entity.

	actors, including unintentionally		reports, grant projects, media	explosives training, communication and digital technology training, provision of healthcare, food, and emergency shelter, or facilitating the education of citizens from high-risk areas in potentially sensitive fields, etc.
2C	The NPO handles dual-use technologies and goods, or substances and equipment that can be easily misused	medium	NPO website, public registers, annual reports, media, information from permitting and licensing authorities	This does not necessarily refer only to hazardous chemical, biological, or radioactive substances, but also to IT and communication equipment, drones, survival gear, precursors, etc.
2D	It is difficult to prove or verify the actual implementation of an NPOs' activities	medium	NPO website, annual reports, media	This factor is risky especially in connection with afore-mentioned factors. Working in very remote areas, conducting activities without clear and tangible results, missing outputs – documentation, lists of beneficiaries, no media presence, information on social networks, etc., the NPO does not work with public funds and is not subject to subsidy control.
2E	NPO programs and activities are only vaguely explained to supervisory authorities	medium	NPO website, public register, annual reports, media, program, and grant reports	This factor is risky especially in connection with afore-mentioned factors. E.g. it may not always be clear who is the final recipient, if the help or assistance in the field is outsourced, the goals of individual programs and recipient selection are not clear, etc.

3) Financial resources

Possible detection of these risk factors is not included in the public version.

Code	Risk factor	Significance	Description and commentary
3A	This risk factor is not part of the public version.		
3B	Concealed income	high	Especially relevant for larger amounts, even if split into many smaller items.

3C	NPO has no bank account	medium	Does not apply if the NPO has no income or only minor income (e.g., a few thousand CZK). Using a transparent account reduces risk.
3D	Unusually high deposits, income, or assets not corresponding to the NPO's activities	high	
3E	Deposits and donations from high-risk persons	high	
3F	NPO funds are mixed with personal or commercial financial resources	medium	The owner or source of the funds cannot be clearly identified; may also lead to unintentional misuse for TF due to negligence.
3G	NPO shares assets with another organization suspected of supporting terrorism or terrorist-related activities	high	The NPO's assets and resources may be exploited to support terrorism, even if the NPO does not intend to misuse them—e.g., real estate, technical equipment, or other assets could be used for recruitment, printing leaflets, storing supplies, etc.
3H	This risk factor is not part of the public version.		
3I	NPO accepts or otherwise operates with virtual assets	high	Particularly if transactions are not transparently reported and involve unusually large volumes. Risk also arises from using service providers linked to virtual assets.
3J	NPO conducts an unusual number of public collections, or the collections are not consistent with its activities	medium	Especially if their purpose or documented use of proceeds is unclear.
3K	NPO extensively uses crowdfunding campaigns where donors are not identifiable, or their identification is unreliable	medium	Donor information may be missing, unverifiable, or inauthentic (e.g., AI-generated).
3L	NPO primarily accepts cash donations	high	Particularly for large amounts beyond ordinary sources, e.g., membership fees or other regular income.

3M	NPO uses services of non-bank payment institutions that allow accumulation and transfer of funds	high	Includes income collected via various web and mobile applications.
3N	NPO uses foreign financial institutions without apparent justification	medium	

4) The use of funds

Possible detection of these risk factors is not included in the public version.

Code	Risk factor	Significance	Description and commentary
4A	Unusually high cash withdrawals/deposits	high	If not justified by the focus of the NPO's activities.
4B	Non-transparent handling of financial resources	high	Transfer of funds or other assets to other persons without an apparent purpose (especially to individuals in offshore jurisdictions, non-contact persons, high-risk individuals, etc.).
4C	Transactions involving fictitious or unknown NPOs, or benefiting such NPOs	high	
4D	Transactions involving high-risk persons	high	
4E	Use of funds for purposes other than those for which the NPO was established, or inconsistent with usual NPO procedures	medium	If not justified by a change in the NPO's focus.
4F	Fictitious or inflated expenses or costs, including suspected cases	high	Especially relevant in areas where services are difficult to value (e.g., job placement services, marketing, or promotional services).
4G	Discrepancies between reported statements (accounting, tax) and actual financial flows	high	Particularly for large amounts.
4H	Illogical, unexplained, and/or unannounced	high	

	transfer paths of payment funds		
4I	Lack of internal control over the use of funds at the point of disbursement	low	
4J	Lack of approval mechanism for higher financial amounts	low	
4K	Third parties are used to open accounts or carry out transactions on behalf of the NPO	high	May lead to diversion of funds, misuse of accounts for laundering criminal proceeds, or concealment of the source of funds, etc.

5) Other activities and attributes of an NPO

Code	Risk factor	Significance	Possible detection	Description and commentary
5A	The NPO does not communicate with state authorities	medium	Attempt to communicate with the NPO	Notices regarding obligations to the public register, tax obligations, obligations related to the management of public funds, etc.
5B	Concealment of the NPO's actual operations	high	Searching in open sources	The NPO's publicly declared activities or representatives do not correspond with reality.
5C	Engaging in business activities unrelated to the NPO's main purpose	low	NPO website, media	
5D	NPO does not inform the public about its activities	low	Searching in open sources	The NPO lacks a website, social media profiles, notice boards, or other information channels.
5E	Purchased or leased property is used in a manner inconsistent with the NPO's mission	low	Searching in open sources	E.g. the NPO rents a real estate property for the purpose of carrying out first aid training, but, in fact, carries out activities aimed at radicalizing individuals.
5F	Lack of awareness of sanctions lists and other legal obligations in AML/CFT	low	Communication with NPO	May lead to unintentional or negligent misuse. Such NPOs may also be targeted by terrorist entities due to their

				lack of knowledge or negligence.
5G	Absence of internal policies mitigating the risk of NPO misuse	low	Internal NPO documentation, NPO website, communication with NPO	Hinders internal and external control of programs, employees, etc.
5H	Absence of designated individuals responsible for mitigating NPO misuse	low	Internal NPO documentation, NPO website, communication with NPO	Hinders internal and external control of programs, employees, etc.
5I	Absence of a mechanism to screen foreign partners and suppliers	low	Internal NPO documentation, NPO website, communication with NPO	E.g. against sanction lists.
5J	Large operational capacities	low	Internal NPO documentation, NPO website, communication with NPO, media	Access to resources, often in cash; global presence, especially in high-risk areas – NPO can be targeted for misuse of resources, networks, and programs (e.g. for recruiting).
5K	NPO merges with another organization suspected of supporting terrorism or terrorist-related activities	high	Internal NPO documentation, NPO website, communication with NPO, media	The NPO's assets and resources may be used to support terrorism without the NPO intending to do so.
5L	NPO premises cover criminal or other illegitimate activities	high	Internal documentation, media	The NPO's assets and resources may be used to support terrorism without the NPO intending to do so.
5M	Sudden change in the nature of activities, personnel, financing, or other essential aspects of the NPO, leading to higher overall risk	medium	NPO website, communication with NPO, media	May indicate takeover, control, or misuse of a legitimate NPO for illegal or security-risk activities.
5N	NPO has not activated a data mailbox, or does not respond to messages sent there	low	NPO website, communication with NPO	

6) Personnel

Code	Risk factor	Significance	Possible detection	Description and commentary
6A	High risk persons within an NPO	high	Public registers, media, open sources, criminal record register, register of beneficial owners	Especially in leadership positions, employees (internal and external), implementers, coordinators.
6B	High risk persons conducting public collections	high	Public registers, media, open sources, criminal record register, register of beneficial owners	
6C	Unusual increase in the net worth of individuals associated with the NPO	medium	Tax returns, NPO accounting	Could concern founders, directors, employees, or collaborators, particularly if it does not correspond with declared or verified data.
6D	Excessive radicalism of NPO representatives or inclinations towards extremist groups and ideologies	high	Communication with NPO, NPO website, media	May also indicate internal conflict within the NPO.
6E	Large amounts of associates and temporary workers	low	Grant projects, annual reports	Verifying short-term collaborators can be challenging; NPOs may face frequent personnel changes and lose the know-how needed to reduce the risk of NPO misuse.
6F	Decentralized communication and management	low	Internal NPO documentation, annual reports, NPO website	This can make control and understanding of the organization functioning difficult.

7) Geographical risks

Code	Risk factor	Significance	Possible detection	Description and commentary
7A	NPO headquarters located in a high-risk country	high	Check in public registers, NPO website, annual reports	

7B	Significant part of NPO activity occurs in a high-risk country	high	NPO website, annual reports, grant projects, media	See Definition of specific terms."
7C	NPO activity supports high risk persons, or the NPO has another clear connection to high-risk persons or countries	medium	NPO website, annual reports, grant projects, media	See Definition of specific terms."
7D	Transfer of financial resources or other assets to entities operating near or directly in high-risk countries	medium	NPO accounting, bank account transactions	Especially if the NPO was not established or intended to operate in these areas.
7E	NPO records are stored in a high-risk country	high	NPO internal documentation, NPO website, communication with NPO, media	Sensitive information about staff and aid recipients may be misused, especially if a recipient is also a target of terrorist actors; access to accounts could be exploited.
7F	NPO representatives frequently travel to high-risk countries	medium	Communication with NPO, NPO website, media	Especially if there is no clear link to the declared activities of the NPO in that area.

Conclusion

The risk level of an NPO must be assessed through the prism of all available information, of which the above list of risk factors represents only a partial fragment. The purpose of this material is not to interfere with the legitimate activities of lawful NPOs, but to provide control authorities and bodies providing public support or issuing public contracts with a tool to determine the risk level of individual NPOs based on the available information about their specific risk factors. At the same time, it can enable NPOs themselves to evaluate their own risk exposure and take steps to gradually reduce it, thereby lowering the likelihood of their misuse, whether intentional or unintentional. It can also assist NPOs in identifying partners and suppliers who do not exhibit risk indicators.

This material and the risk factors contained within it will be regularly updated as part of the activities of the relevant working group, as needed, but at least once every four years.

Other relevant sources on the topic in English

FATF Recommendations – FATF Recommendations (as of June 2025)

https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Comprehensive Update on Terrorist Financing Risks – Overview of Terrorist Financing Risks (2025)
https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf

Best Practices Paper on Combating the Terrorist Financing Abuse of NPOs – Specific examples of good and bad practices, experiences from other countries (2023) https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Bpp-combating-abuse-npo.html

FATF Report: Crowdfunding for Terrorism Financing – New typologies of abuse of digital fundraising (2023)

https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

Terrorist Financing Risk Assessment Guidance – Methodology for conducting terrorist financing risk assessments involving NPOs (2019)

https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf