FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

14 July 2026
BOF/FIN-FSA-UNRESTRICTED
Public

Update for supervised entities – Consider terrorist financing risks

Obliged entities under the Act on Preventing Money Laundering and Terrorist Financing (444/2017) have an obligation to identify and prevent terrorist financing risks and to report any suspicious transactions that may be linked to terrorist financing. Combating terrorist financing is a parallel but independent framework alongside the anti-money laundering.

Anti-money laundering indicators are usually insufficient on their own to identify the risk of terrorist financing

Alongside anti-money laundering, combating terrorist financing is an **independent framework**, and its risk elements and indicators must be determined separately. When designing risk management methods, the specific characteristics of terrorist financing must also be taken into account. The management methods must be implemented based on risks so that they are proportionate and effective. In practice, this requires that risk management methods support the effective detection and prevention of terrorist financing. Well-functioning prevention requires that the specific characteristics of the phenomenon are taken into consideration and practical measures are targeted appropriately.

In comparison with money laundering, key differences related to terrorist financing and its prevention may arise in relation to the following areas, for example:

- The origin of funds is not as central an indicator as in anti-money laundering, because in combating terrorist financing the main suspicion relates to the use of the funds, not their origin. Therefore the best possible information on the recipients of funds is essential in combating terrorist financing. In particular, if funds are known to be transferred onwards from the first recipient, it is important to obtain a comprehensive picture of the entire recipient chain.
- Funds used for terrorist financing may originate from legal or illegal sources.
- The size of an individual transaction is often of lesser significance in terrorist financing, and transactions linked to terrorist financing may be small and appear ordinary.
- Terrorist financing may be connected to otherwise legitimate activities in which funds, or part of the funds, are misused.
- The risk profiles of parties sending and receiving funds may vary significantly depending on ideology, operating methods, and, for example, the platforms used to raise funds.

Risk-based approach and risk assessment for terrorist financing

The supervised entity's risk assessment of its business activities forms the basis for effective measures to prevent and detect terrorist financing. A good understanding and concrete assessment of terrorist financing risk is a prerequisite for identifying and taking risk factors into account in risk classification and in the rules of monitoring systems.

As part of its own risk assessment, the supervised entity must:

- identify terrorist financing risks in its products, services, clients, distribution channels and geographical connections,
- document the nature and likelihood of terrorist financing risks,
- scale its risk mitigation measures and preventive actions according to the risks,
- assess the residual risk in relation to the effectiveness and quality of its own controls, and evaluate whether the residual risk is consistent with the supervised entity's established risk appetite,
- update its risk assessment regularly and in connection with material changes.

The terrorist financing risk assessment must be sufficiently concrete and also describe the risk mitigation measures in place and assess their effectiveness. Risk assessment may reveal deficiencies or poor practices, after which it is possible to address the identified problems through corrective action.

Dynamic nature of terrorist financing and risk profiles

Many factors underlying terrorist financing are subject to rapid change, which means that terrorist financing risk is also significantly dynamic in nature. Therefore, monitoring changes in risk should generally cover, for example, geopolitical conflicts, radicalisation, societal changes, and even changes related to charitable activities. New payment methods, crypto-assets and social media have also been found to be exploited for raising terrorist financing. As a result, factors that may affect the determination of indicators are variable and may require broader awareness than before.

Different ideologies that potentially engage in terrorist activity may require different terrorist financing indicators and risk profiles. This may be reflected, for example, as differences in

- the methods and platforms used to raise funds,
- donation and crowdfunding models,
- the geographical direction of fund transfers.

A risk assessment that takes different extremist movements (and similar groups) and their operating models into account separately will generally provide better preconditions for combating terrorist financing than one based on a uniform risk model. For example, there may be significant differences between far-right and extremist Islamist actors in the methods used to raise funds, as well as in the relevant indicators. Mapping potential differences in terrorist financing linked to different extremist movements may be facilitated by dividing terrorist financing into its different stages: fundraising, transfer and use of funds, and then assessing possible differences from these perspectives for each extremist movement.

Customer due diligence and management of terrorist financing risks

The supervised entity must identify and verify the customer's identity and:

- determine the purpose of the transaction and the business relationship,
- identify the beneficial owner,

- monitor the business relationship on an ongoing basis from a terrorist financing risk perspective.

The supervised entity may use information available from various reliable and credible sources about the customer or their beneficial owner, for example to prepare and maintain a risk assessment of the customer and to prevent terrorist financing. Customer information should be sufficient to assess whether funds, payments or services could be linked, directly or indirectly, to terrorist financing.
The supervised entity must pay particular attention to customer transactions that are unusual in terms of structure or amount, or for example, the size or location of the supervised entity. The same also applies where transactions lack an obvious economic purpose or are inconsistent with the supervised entity's experience or knowledge of the customer. Enhanced customer due diligence is regulated in chapter 3, section 10 of the Act on Preventing Money Laundering and Terrorist Financing. The FIN-FSA has also issued guidance on the matter in chapter 6.6 of its regulations and guidelines 2/2023 on the prevention of money laundering and terrorist financing[1].

Combating terrorist financing is also linked to international sanctions. So-called counter-terrorism sanctions have been imposed on individuals, groups and entities involved in terrorist acts, such as ISIL, al-Qaida, Hamas and Palestinian Islamic Jihad. In practice, this means that international sanctions lists, together with related information, must also be used as sources when mapping terrorist financing risks associated with a business relationship. In addition to international sanctions, the public list of asset freezing orders by the National Bureau of Investigation under the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013) must also be taken into account as a source of information.

When applying sanctions, however, the humanitarian exemptions provided for in UN Security Council resolutions must be considered (UNSCR 2664 (2022), 2761 (2024) and 2615 (2021)). It is important that humanitarian aid reaches its intended recipients, because it helps protect human life, health and basic needs such as food, drinking water and medicine in crisis situations, enables access to urgent medical care, and supports, for example, the provision of shelter, heating and other essential assistance to people in vulnerable situations.

Link between risk assessment and risk classification

Terrorist financing risk factors refer to such characteristics and features related to clients, products and services, distribution channels and geographical connections that may increase the likelihood of these being exploited for terrorist financing.

Through the assessment of business areas, it may be possible to identify that a particular business area may involve higher risk, for example due to a high prevalence of cash payments and the use of money transfer services. On the other hand, from a product perspective, different forms of financing or loans may, for example, involve different levels of terrorist financing risk. For example, remotely applied for consumer loans granted quickly based on limited customer due diligence may involve higher risk than long-term secured loans, where the customer's background, source of funds, loan collateral and purpose of the funds are examined more thoroughly. If different risk factors are combined for example, by examining different products in different business areas, it may be possible to produce very specific risk

[1] Regulations and guidelines 2/2023 Preventing Money Laundering and Terrorist Financing https://www.finanssivalvonta.fi/globalassets/en/regulation/fin-fsa-regulations-and-guidelines/2023/02_2023/maaraykset-ja-ohjeet-2_2023_en.m3-clean.pdf

descriptions and highlight factors that may indicate an accumulation of risks. For example, the combination of certain products with a high-risk country may be a factor that increases customer risk.

In some cases, terrorist financing risk descriptions may be very similar to money laundering risk descriptions, but this is not automatically the case. For example, factors that increase the likelihood of countries being destination countries for terrorist financing-related fund transfers are likely to differ from the factors that make countries attractive destination countries for money laundering.

An individual customer's level of terrorist financing risk can be assessed on the basis of the identified risk factors in the supervised entity's general terrorist financing risk assessment and how the customer's characteristics and activities relate to these factors. Customer due diligence measures and the ongoing monitoring of the customer relationship are, when functioning well, closely linked to the understanding of the level of terrorist financing risk that the particular business relationship represents. The importance of ongoing monitoring is emphasised by the fact that in some cases, particularly changes in the customer's behaviour may indicate an increased terrorist financing risk.

Terrorist financing risk assessments can, where necessary, include concrete descriptions of how different factors may increase terrorist financing risk. This may include, for example, how charitable organisations can be exploited for the benefit of terrorist organisations, and how a large number of small transfers to different organisations without a known or clear connection between the donor and the charitable purpose may serve as an indicator that increases the customer's risk level.

In addition to identifying different and varying risk factors, combating terrorist financing also requires an **assessment of the effectiveness and quality of the supervised entity's own risk management measures**: whether matters and events requiring attention are identified correctly and timely, and, on the other hand, whether the preventive measures are effective enough to keep the residual risk at an acceptable level.

It may also be justified to include in the terrorist financing risk assessment descriptions and assessments of potential **emerging** terrorist financing risks. These could include developments or events which, if they materialise, could be considered to change the prevailing terrorist financing risk so significantly that the supervised entity deems it necessary to monitor the possible progression and impacts of such developments. Examples of such developments include the escalation of conflicts in the Middle East or African countries and potential related radicalisation, as well as the increasing collection of funds on social media platforms and related transfers of crypto-assets. It should be noted that **external events can lead to rapid changes** potentially requiring a quick update of the risk assessment and changes in operations, which should also be considered in risk assessment methodologies and risk mitigation.

Good understanding and use of information sources

The supervised entity must ensure that the prevention of terrorist financing is taken into account in its internal guidelines and procedures, and that staff receive the necessary training on identifying terrorist financing.

Good use of information sources is essential for understanding and assessing terrorist financing risk. Below is a selection of current publications related to terrorist threats and terrorist financing which, along with other similar sources, can be used in the management of terrorist financing risks:

- Different countries' national risk assessments on (money laundering and) terrorist financing. Focusing, for example, on countries to which the supervised entity has exposure through its clients (e.g.
    - Finland, *Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio (2026)*
    - United States, *National Terrorist Financing Risk Assessment (2026)*
    - United Kingdom (UK), *National risk assessment of money laundering and terrorist financing (2025)*
    - Europol, updating publication *European Union Terrorism Situation and Trend report (EU TE-SAT)*, and terrorism threat assessments published by the intelligence services of various countries.
    - The Institute for Economics & Peace, annual publication *Global Terrorism Index*, and the institute's other publications related to the threat of terrorism
- FATF (Financial Action Task Force): *Comprehensive Update on Terrorist Financing Risks (2025)*
    - Annex A of the report ("Terrorist Financing Risk Indicators on Evolving Methods and Techniques") presents terrorist financing risk indicators derived from responses to the FATF questionnaire related to this project and from previous FATF findings.
- EBA (European Banking Authority) publications related to money laundering and countering terrorist financing: Anti-Money Laundering and Countering the Financing of Terrorism
- The Royal United Services Institute for Defence and Security Studies (RUSI), Insights Papers: *Reassessing the Financing of Terrorism in 2025* and other RUSI publications related to terrorism
- Reports by the Analytical Support and Sanctions Monitoring Team on ISIL and Al-Qaida for the UN Security Council
- Publications by various countries' Financial Intelligence Units on terrorist financing, for example:
    - Finanstilsynet (Norway): Terrorfinansiering – håndtering av risiko for terrorfinansiering i et utvalg banker, Temarapport 24. juni 2025
    - Financial Intelligence Unit: Terrorismin rahoittamisen ominaispiirteet 2020–2025 (public summary)

Conclusion

When identifying terrorist financing, supervised entities should consider, for example, the following:

- Terrorism can be financed, for example, through business activities, salary income, grants, donations, consumer credits, or funds obtained through criminal activity such as fraud.
- Business activities (or front activities) related to fundraising may also be fictitious, meaning that significant amounts of money may flow through bank accounts even though the registered business activity is non-existent or very limited. In some cases, the value of purchased or sold products does not clearly correspond to the funds transferred.
- The raising of terrorist financing and the transfer of funds may also be disguised as charitable activities, which can be quite conspicuous in order to attract clients and donations.
- Funds may also be transferred abroad for terrorist purposes through value transfer systems operating outside the conventional banking system, such as so-called hawala systems. Particularly concerning from the perspective of combating terrorist financing are money transfer

agents who are not registered as money transmitters in Finland or elsewhere in the EEA, but operate as so-called dark hawalas.

- International conflicts and the situation in countries where terrorist activity is particularly prevalent may affect the need for terrorist financing and, consequently, the amounts collected.
- Terrorist acts can also be committed in Finland, so terrorist financing does not necessarily involve cross-border fund transfers. Terrorism is generally associated with extremist thinking focused on a particular ideology, social networks of like-minded individuals and mutual trust relationships, as well as some form of personally perceived need to influence societal issues without shying away from violence.