



REPUBLIC OF ESTONIA
MINISTRY OF FINANCE

Estonian National Risk Assessment Report on Countering Terrorist Financing 2020–2024

2025

Table of Contents

1. GENERAL PART	3
1.1. Introduction	3
1.2. FATF Definitions and Concepts	4
1.3. Methodology used	5
1.4. The criteria used in the analysis for assessing threats and vulnerabilities	5
1.4.1. The criteria for assessing national threats	6
1.4.2. The criteria for assessing national vulnerabilities:	7
1.5. Data Collection	8
2. SUMMARY	9
3. TERRORISM THREAT IN ESTONIA	12
3.1. Threat from Islamist Extremism	12
3.2. Threat from Violent Right-Wing Extremism	12
3.3. Threat from Russian Federation	13
3.4. Threat from Left-Wing Extremism	13
4. OVERVIEW OF TERRORIST FINANCING	14
5. NATIONAL TERRORIST FINANCING THREATS	17
5.1. Internal Threat	18
5.2. Outgoing Threat	19
5.3. Incoming Threat	21
5.4. Transit Threat	22
6. VULNERABILITIES	23
6.1. National Terrorist Financing Vulnerabilities	23
6.2. Sectoral Vulnerabilities	26
6.2.1. Virtual asset service providers	26
6.2.2. Credit Institutions	29
6.2.3. Payment institutions, including cross-border payment services (money transfer service providers, currency exchangers)	31
6.2.4. Crowdfunding Service Providers	32
6.2.5. Other Sectors	33
ANNEXES	
Annex 1. Main typologies of terrorist financing	35
Annex 2. Case Studies	36
Annex 3. Guidance for Sectors	38

1. General Part

1.1. Introduction

The terrorist financing risk assessment is part of a broader national risk assessment conducted under the authority of the Ministry of Finance, which includes an analysis of risks related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. The national risk assessment is regularly conducted in Estonia every four to five years and serves as the basis for the action plan to mitigate threats and vulnerabilities. This risk assessment was carried out from September 2024 to June 2025 and includes an analysis of data from 2020 to 2024. The national risk assessment report was approved by the Government Commission for the Prevention of Money Laundering and Terrorist Financing, chaired by the Minister of Finance.

A separate working group was established to assess the risks of terrorist financing. The working group was led by the Ministry of the Interior and included representatives from the **Ministry of the Interior, the Prosecutor's Office, the Financial Intelligence Unit, the Tax and Customs Board, and the Internal Security Service**. The working group also collaborated with parallel working groups that were preparing the money laundering risk assessment, involving more than 100 experts from ministries, government agencies, and the private sector.

The NRA steering committee was formed by the representatives from the Ministry of Finance, the Ministry of Justice and Digital Affairs, the Ministry of the Interior, the Ministry of Foreign Affairs, the Financial Supervision Authority, the Financial Intelligence Unit, the Internal Security Service, the Police and Border Guard Board, the Tax and Customs Board, and the Prosecutor's Office to validate the results of the national risk assessment and evaluate the completion of the report.

The assessment of terrorist financing risks utilized the methodology recognized by the World Bank¹ (see 1.1.2), which was adapted in cooperation with the risk assessment working groups to suit Estonia's specific characteristics. The assessment is primarily based on information collected during the period under review by the state institutions included in the working group (statistics, operational information, international cooperation with partner services, legislative changes, etc.) and on relevant international and national studies and analyses.

In the first phase of the assessment process, initial consultations were held between institutions, necessary statistics were collected, typologies were mapped, and additional training and consultations with methodology experts were conducted. In the second phase, assessment modules were completed, and analysis was carried out using both qualitative and quantitative information. Written surveys and focus group interviews were conducted. In the third phase, the report was compiled. The private sector was involved through written surveys and interviews conducted in focus groups.

¹ World Bank, Washington, USA, www.worldbank.org

During the preparation of the terrorist financing risk assessment, the threats related to the financing of the following terrorist organizations were analyzed, considering, among other things, their funding needs, sources of funding, and channels for moving funds: **ISIS, ISIS-K, Taliban, HAMAS, Kurdistan Workers' Party (PKK), Palestinian Islamic Jihad, Hezbollah**; right-wing extremist accelerationist groups such as **Atomwaffen Division, Feuerkrieg Division, Base, Nordic Resistance Movement**, etc.; **Russian Imperial Movement, Russian Federation special services**. In addition to terrorist organizations, the threats related to the financing of individuals (both Islamist extremism and right-wing extremism) were also assessed.

Since terrorist financing is linked to the overall threat of terrorism, this risk assessment also provides a brief overview of the terrorism threat in Estonia and developments in the field of terrorist financing. The assessment delves deeper into national terrorist financing threats, national vulnerabilities, and sector-specific vulnerabilities. All obligated entities were examined, but sectors with a greater impact were analyzed more thoroughly. The selection was based on the volume and turnover of the sector's services, previous cases, and risk typologies. No significant terrorist financing risks were identified in other sectors.² More detailed data on sectors are published in the national money laundering risk assessment report.

This risk assessment does not cover non-profit organizations (NPOs and foundations). The Financial Intelligence Unit will prepare a separate analysis on non-profit organizations.

1.2. FATF Definitions and Concepts³

The FATF defines the risk of terrorist financing as a combination of three factors:

1. **Threat:** A threat is a person, object, or activity that has the potential to cause harm, for example, to the state, society, economy, or financial system. Examples include terrorist organizations and channels for terrorist financing.
2. **Vulnerability:** Vulnerability is a weakness or situation that a threat can exploit or that facilitates the threat's activities. Examples include inadequate supervision, weak internal control measures, lack of awareness of risks, and insufficient legislation.
3. **Consequence:** Although not always a separately assessable component, consequence refers to the impact that the threat and vulnerability together may have, for example, on the reliability of the financial system or the economy at large.

According to FATF recommendations, countries and institutions should assess these factors to develop a risk-based approach that allows resources to be directed where the risk is greatest.

² A separate analysis will be prepared for non-profit organizations (NPOs and foundations). A separate comment has been added regarding corporate service providers (6.2.5.)

³ This report is based on the definition of terrorism and terrorist financing as stipulated in § 237 of the Penal Code, which defines a terrorist offense as the commission of an offense against international security, against a person, against the environment that endangers life or health, against a foreign state or international organization, or the commission of a generally dangerous offense, the production, distribution, or use of a prohibited weapon, the unlawful seizure of property, or the significant damage or destruction of property, interference with computer data, or obstruction of the functioning of a computer system. It also includes threats to commit such acts **if they are carried out with the aim of compelling a state or international organization to do or refrain from doing something, seriously disrupting the political, constitutional, economic, or social order of the state, or destroying it, seriously disrupting the activities of an international organization, or destroying it, or seriously intimidating the population.**

1.3. Methodology used

The risks of terrorist financing were independently assessed by representatives of Estonian authorities using the World Bank's methodology and tools (assessment modules)⁴ for assessing terrorist financing risks.

The role of the World Bank team was limited to the following: 1) providing the tool, i.e., the assessment modules; 2) giving technical guidance on using the tool; 3) reviewing and providing feedback on the draft national risk assessment report.

The data, statistics, and other information entered into the assessment modules, as well as the conclusions, interpretations, and assessments made during the national risk assessment process, belong to the participants of the Estonian national risk assessment project and do not reflect the views of the World Bank.

The World Bank's methodology guidelines and assessment modules are publicly available on the organization's website⁵. As part of the cooperation between the Ministry of Finance and the World Bank, the entire team involved in the national risk assessment project received training and advisory services for the application and adaptation of the World Bank's methodology to Estonia's specific characteristics.

The terrorist financing risk assessment tool addresses risk as the interaction of two main components: threat and vulnerability. The consequences of risks were not assessed separately but are integrated into the analysis of threats and vulnerabilities using weighting factors, preconditions, and a network-based structure. This methodology was applied at both the national and sectoral levels.

The assessment process began with the identification of threats, during which the sources that could influence terrorist financing were analyzed, such as international networks and channels of money flows. Next, the capacity and vulnerabilities of the national prevention system were assessed, such as deficiencies in legislation or supervision. Thirdly, a sectoral analysis was conducted. For each sector, the existence, effectiveness, and level of supervision of control measures, as well as the risk awareness of market participants, were evaluated.

The World Bank's terrorist financing risk assessment methodology uses a point scale to assess the levels of threat and vulnerability, which helps determine how susceptible a sector or system is to the risks of terrorist financing.

1.4. The criteria used in the analysis for assessing threats and vulnerabilities

A **threat** refers to the likelihood that terrorist financing may occur within the country's territory or through the Estonian financial system. Broadly speaking, the assessment is based on the potential presence of terrorist organizations in the country as well as known or potential cases of terrorist financing.

Vulnerability refers to how susceptible a sector or system is to terrorist financing, regardless of whether the threat actually materializes. Broadly speaking, this primarily reflects the strength or weakness of preventive and control measures, including legislation, supervision, internal controls, and risk management. The weaker or less effective these mechanisms are, the greater the system's vulnerability.

Risk is the interaction of threat and vulnerability.

⁴ Terrorist Financing Risk Assessment Tool (2022).

⁵ World Bank, Disclaimer and Terms of Use: National Money Laundering and Terrorist Financing Risk Assessment Toolkit, <https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use>

Experts from the terrorist financing working group populated the assessment modules with numerous sub-criteria for the assessment criteria, where the scale ranged from zero to one hundred points in the range of 0–1. The assessment scale was distributed as follows: 0 – does not exist, 0.1 – almost none, **0.2 – very low, 0.3 – low, 0.4 – low-medium, 0.5 – medium, 0.6 – medium-high, 0.7 – high, 0.8 – very high, 0.9 – almost excellent, 1.0 – excellent.**

Using the World Bank’s terrorist financing risk assessment methodology, the final assessment of threats, vulnerabilities, and risk levels was automatically formed based on internal logic after completing the assessment modules, where experts provided evaluations based on specific assessment criteria.

1.4.1. The criteria for assessing national threats

The assessment criteria for national threat analysis:

Terrorist activity – domestic and cross-border threat:

- The rate of deaths caused by terrorism during the assessment period,
- The frequency of terrorist acts during the assessment period,
- The extent of activities supporting terrorist acts during the assessment period,
- The impact of terrorism on the jurisdiction during the assessment period.

Terrorist entities – domestic and cross-border threat:

- Terrorist organizations, groups, and/or individuals (categorized) active in the jurisdiction,
- The level of funding needs,
- The estimated activity of fundraising,
- Sources of funding,
- Types of assets,
- Channels for moving funds,
- The extent of individuals moving funds through informal or shadow services (e.g., hawala), trade (including goods under export control), and smuggling (including cash couriers).

Supporters – domestic and cross-border threat:

- The number of investigations, prosecutions, convictions, and mutual legal assistance requests related to support for terrorism ideology (even if there is no direct link to terrorist attacks, organizations, or individuals),
- Information on individuals likely supportive of terrorism ideologies, collected through financial intelligence, including suspicious transaction reports (STRs),
- Cases where individuals have traveled from Estonia to areas with active terrorism threats,
- Transfers (both incoming and outgoing) to areas with active terrorism threats,
- Communities within the jurisdiction with close ties to areas with active terrorism threats and the associated potential risk of terrorist financing,
- Information on individuals supportive of terrorism ideologies based on public statements, research, media reports, and expert opinions.

Neighboring countries – domestic and cross-border threat:

- The level of active terrorism threat in neighboring countries,
- The estimated number of terrorism victims in neighboring countries during the assessment period, using evaluation scale if necessary,
- The number of terrorist attacks in neighboring countries over the past five years,

- The level of funding related to terrorism threats in neighboring countries and its connection to the level of terrorism threat,
- The impact of neighboring countries' terrorism-related funding needs on Estonia,
- Information on individuals supportive of terrorism ideologies based on public statements, research, media reports, and expert opinions.

Financial and transport hubs – domestic and cross-border threat:

- The jurisdiction's significance as an international or regional financial center,
- The jurisdiction's significance as a transshipment and logistics hub,
- The jurisdiction's significance as a trade area.

Strategic goods and services – domestic and cross-border threat:

- The involvement of legal entities within the jurisdiction in enabling strategic goods and services to areas with terrorism threats, including areas controlled by terrorist organizations,
- The involvement of government agencies within the jurisdiction, including state-owned enterprises, in enabling strategic goods, services, and financial aid to areas with active terrorism threats,
- The delivery of strategic goods, services, and financial aid to areas with active terrorism threats through non-profit organizations within the jurisdiction.

1.4.2. The criteria for assessing national vulnerabilities:

The **national vulnerability assessment** is based on the analysis of the following factors: 1) the country's capability to mitigate the threats of terrorist financing, 2) sectoral vulnerabilities in conjunction with the presence, effectiveness, and awareness of control measures among market participants.

Assessment criteria⁶ for a country's capability to mitigate the threats of terrorist financing:

- The quality of terrorist financing prevention policies and strategies,
- The effectiveness of the definition of the terrorist financing crime,
- The effectiveness of customs and border controls in preventing terrorist financing,
- The quality of information collection and processing related to terrorist financing,
- The quality of investigations into terrorist financing,
- The quality of prosecutions for terrorist financing,
- The quality of adjudications for terrorist financing,
- The quality of mechanisms for the confiscation and seizure of assets related to terrorist financing,
- The quality of targeted financial sanctions related to terrorist and terrorist financing,
- The control of strategic equipment, goods, and services related to conflict areas.

Assessment criteria for sectoral vulnerability analysis:

Inherent vulnerability of the sector:

- The suitability/usefulness of the sector for terrorist financing,
- The volume and turnover of the sector,
- The profile of the customer base,
- Outgoing international transactions,
- Outgoing international transactions to higher-risk jurisdictions,
- Incoming international transactions,

⁶ These are overarching criteria, which in turn had sub-criteria.

- Incoming international transactions from higher-risk jurisdictions,
- The use of cash,
- The use of agents, service providers, and intermediaries,
- Other vulnerability factors.

The quality of terrorist financing prevention controls:

- The scope of the legal framework for preventing terrorist financing,
- The effectiveness of supervisory and control activities,
- The availability and application of administrative penalties,
- The availability and application of criminal penalties,
- The availability and effectiveness of market entry control mechanisms,
- The integrity and reliability of sector employees,
- The knowledge and awareness of sector employees in the field of terrorist financing prevention,
- The effectiveness of compliance controls,
- The effectiveness of the implementation of international financial sanctions (TFS),
- The effectiveness of monitoring and reporting suspicious transactions,
- The availability and access to beneficial ownership data,
- The existence of a reliable identity verification infrastructure,
- Access to reliable information sources.

1.5. Data Collection

In the risk assessment, information was gathered from both official and public sources. Key official sources included data from the Estonian Internal Security Service, statistical data from the Financial Intelligence Unit, and criminal statistics from the Prosecutor's Office, among others. Additionally, data from written surveys and focus group interviews conducted in the private sector were utilized. All data used in the assessment were collected annually for the period under review, specifically for the years 2020–2024.

2. Summary

Table 1. National Terrorist Financing Risk

Category	Threat	Vulnerability	Risk
Internal	low	below average	below average
Outgoing	medium	below average	medium
Incoming	medium	below average	medium
Transit	above average	medium	above average

The level of terrorist financing risk is determined by the interaction of two main components – threat and vulnerability.

National terrorist financing threats

The national terrorist financing threat is divided into four categories: 1) **internal threat**, 2) **outgoing threat** (threat arising from Estonia to other countries), 3) **incoming threat** (external threat), and 4) **transit threat** (threat arising from transit).

The term “**internal threat**” refers to threats arising from the conditions in Estonia, where all phases of terrorist financing occur within the country. The term “**outgoing threat**” refers to the threat posed by the Estonian jurisdiction to other countries. The term “**incoming threat**” refers to the threat posed to Estonia by other jurisdictions. The term “**transit threat**” refers to situations where foreigners outside Estonia use products and services offered within the Estonian jurisdiction for the purpose of terrorist financing. This may also mean the physical movement of funds through Estonia. The funds do not remain in Estonia but pass through it.

The level of internal TF threat is low. There are no terrorist organizations or their cells operating in Estonia, nor do their fighters reside here. The number of individuals with extreme views who might be involved in terrorist financing is low. The risk level of using funds collected for terrorist purposes in Estonia is low. The greatest threat comes from radicalized individuals and those influenced by the Russian Federation. The case related to violent right-wing extremism also involved radicalized individuals (see case study 1). During the observed period, there were no cases of terrorist financing within Estonia.

The level of outgoing TF threat is medium. A significant threat is posed by fundraising campaigns conducted under the guise of charity for foreign countries, in which Estonian residents may also participate (see case study 2). This particularly concerns the support of terrorist organizations related to Gaza and Russia. The context in Estonia is also influenced by the activation of ISIS-K in Central Asia, through workers of Central Asian origin who send funds back home via cross-border payment services and financial institutions. It is also important to note the risk of misuse of the e-residency program for terrorist financing purposes under the cover of business activities (see case study 3 and section 6.2.5).

The level of incoming TF threat of terrorist financing is medium. The greatest and most persistent threat source is Russia, which, as an aggressor state, seeks individuals in Estonia willing to carry out terrorist acts in its interests and is willing to finance them. In the neighboring regions, there are large Muslim communities in Scandinavia and Russia, among whom there are individuals spreading radical Islam and returning foreign fighters. Scandinavia also has a considerable number of right-wing extremists. The level of terrorism threat, which is also related to financing, is low in the Baltic States.

The level of transit TF threat is higher than average. The main threat is related to correspondent relationships, where a foreign resident with a residence permit in another country, who is associated with terrorism or is radicalized, may wish to conduct transactions for the purpose of terrorist financing through the client of an Estonian service provider (see case studies 5 and 6). This concerns both the provision of VIBAN services by credit institutions and the still relatively large sector of virtual asset service providers (VASPs). Although Estonia is not a significant travel, goods, or transport hub, one of the threat sources is the travel of individuals associated with terrorism or radical Islam and foreign fighters through Estonia. The primary threat here lies in the transportation of cash, debit cards, and communication devices to conflict zones.

Vulnerabilities

National Vulnerabilities

The assessment of national vulnerabilities is based on the analysis of the following factors: 1) the state's ability to prevent terrorist financing threats, 2) sector vulnerabilities and the existence, effectiveness, and awareness of control measures among market participants. National vulnerabilities are examined by categories: internal, outgoing, incoming, and transit. The assessment of national vulnerability is influenced by the state's ability to prevent specific threats and the overall vulnerability of the sectors⁷.

The main vulnerability remains the potential misuse of Estonian financial system participants and their service environments for the transfer of funds. A considerable risk is associated with transactions made with foreign partners, such as the correspondent relationships of service providers with an Estonian operating license, where due diligence measures are not sufficiently applied.

The vulnerability level of the **national system for preventing terrorist financing is below average**. The biggest issue is the exchange of information with third countries outside the EU and countries with which there is no legal cooperation (including Russia).

Sector Vulnerabilities

The risk level of sectors is influenced by both threat and vulnerability. The threat level is affected by the national threat of terrorist financing, threats related to typologies, and threats related to sector-specific circumstances. The level of sector vulnerability is influenced by 1) the inherent vulnerability of the sector and 2) the quality of controls to prevent terrorist financing, which are further divided into sub-criteria.

⁷ The overall sectoral vulnerability assessment (below average) takes into account sector vulnerabilities in conjunction with the existence, effectiveness, and awareness of control measures among market participants (see section 6.2).

All sectors considered obligated entities⁸ were examined, with a more detailed analysis conducted on selected sectors. The selection was based on the volume and turnover of the sector's services, past cases, and risk typologies. The following sectors were chosen for more detailed assessment: virtual asset service providers (VASPs), credit institutions, payment institutions, including cross-border payment services (money transfer service providers and currency exchangers), and e-money institutions⁹ (both domestic and foreign), as well as crowdfunding service providers. No significant terrorist financing risks¹⁰ were identified in other sectors. A separate comment is added regarding corporate service providers and the e-residency program (see section 6.2.5).

The main vulnerability of both credit institutions and virtual asset service providers stems from correspondent relationships. For credit institutions, a mitigating factor is the sector's high awareness and the level of application of due diligence measures. The awareness of VASPs regarding terrorist financing risks is uneven but is steadily improving. The main vulnerability of payment institutions is related to the complexity of identifying the sender and receiver of funds through payment agents operating in third countries. For e-money institutions, the biggest challenge is the limited possibilities for information exchange with cross-border e-money institutions and often more lenient know-your-customer requirements.

The vulnerability level of virtual asset service providers, credit institutions, and crowdfunding service providers is below average, while for payment institutions it is average. The threat level for virtual asset service providers and payment institutions is medium, for credit institutions it is below average, and for crowdfunding service providers it is low. The residual risk level is highest in the sectors of virtual asset service providers and payment institutions – medium – while for credit and crowdfunding service providers it is below average.

Table 2. Results of the Terrorist Financing Risk Assessment by Sector

Sector	Threat	Vulnerability	Residual Risk
virtual asset service providers	medium	below average	medium
credit institutions	below average	below average	below average
payment institutions, including cross-border payment services (money transfer service providers, currency exchangers, and e-money institutions) ¹¹	medium	medium	medium
crowdfunding service providers	low	below average	below average

⁸ MLTFPA § 2. <https://www.riigiteataja.ee/akt/113032019126?leiaKehtiv>

⁹ E-money institutions include services such as Paysera, Revolut, Koronapay, OpenPayd, Papaya, Paysafe, Payward, etc.

¹⁰ A separate analysis will be prepared regarding non-profit organizations (associations and foundations).

¹¹ E-money institutions include services such as Paysera, Revolut, Koronapay, OpenPayd, Papaya, Paysafe, Payward, etc. E-money institutions refer to both domestic and foreign entities.

3. Terrorism Threat in Estonia

This chapter presents detailed conclusions about the **overall level of terrorism threat**. The following chapters 4 and 5 provide an overview of specific **threats related to terrorist financing**.

3.1. Threat from Islamist Extremism

The threat level of an Islamist extremism terrorist attack in Estonia is **low**.

No Islamist terrorist organizations or their cells have been identified in Estonia, nor do any fighters permanently reside here. Estonia has a relatively small Muslim community, among whom there are very few individuals with extreme views; the vast majority of the community adheres to moderate Islam. No terrorist acts motivated by Islamist extremism were committed in Estonia between 2020 and 2024.

The greatest threat is the terrorist activity of an individual influenced by radical Islamist ideology. During the observed period, no such individuals were identified in Estonia. However, several individuals with mental health issues, who do not hold religious or ideological beliefs, have been identified as potential sources of threat. The radicalization of individuals is difficult to detect, so the threat they pose cannot be completely ruled out. Additionally, during the observed period, there have been isolated cases where former Islamist foreign fighters and individuals with terrorism connections living in neighboring countries have visited or traveled through Estonia.

3.2. Threat from Violent Right-Wing Extremism

The threat level of a right-wing extremist terrorist attack in Estonia is **low**.

In connection with violent right-wing extremism, an individual was convicted in 2021 for posting threats towards young politicians in a Facebook group following the Siege¹² culture in 2019. During the observed period, three minors who were members of the terrorist organization Feuerkrieg Division¹³ were identified in Estonia and were convicted in January 2025 for belonging to a terrorist group. The convicted individuals were limited to making calls to action and did not commit any actual acts of violence.

The number of right-wing extremists in Estonia is relatively small, and no individuals willing to commit actual terrorist acts have been identified among them. As of 2024, no right-wing extremist terrorist organizations are operating in Estonia. The greatest threat from violent right-wing extremism is the potential emergence of a lone actor.

¹² Siege Culture – an umbrella term for movements based on the ideology of John Mason, which advocates for carrying out terrorist acts by small and independent units. The goal is to bring about the collapse of the global political system and a race war. See also: <https://www.counterextremism.com/james-masons-siege-ties-to-extremists>.

¹³ Feuerkrieg Division – a terrorist organization that follows the ideology of accelerationism, which aims to hasten the collapse of society.

3.3. Threat from Russian Federation

The threat level originating from the Russian Federation (RF) is **medium**.

From a terrorism perspective, the greatest threat to Estonia comes from the RF, which intensified its activities against NATO and EU countries after starting the war against Ukraine in 2022.

In this context, it is important to note the ultranationalist organization **Russian Imperial Movement**¹⁴ (RIM) and its military wing, the **Russian Imperial Legion**. RIM is connected to Russian intelligence services and actively recruits supporters from the diaspora outside the RF.

The source of the terrorist threat also includes the activities of RF intelligence services. In 2023–2024, various attacks organized by the Main Intelligence Directorate (GRU) of the RF Ministry of Defense took place in Estonia and other Baltic countries. The targets of these attacks were monuments related to World War II and current public figures – politicians and journalists, as well as their property (cars). The aim was to incite fear and create conflict in society. RF intelligence services attempt to recruit local Russian nationalist extremists and ordinary criminals to carry out these attacks.

3.4. Threat from Left-Wing Extremism

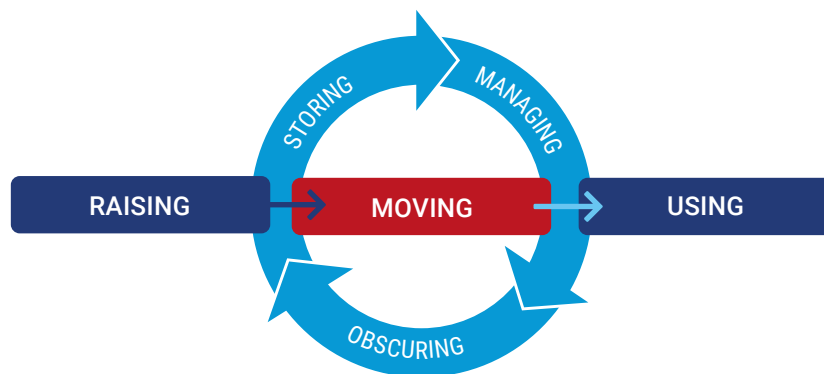
No left-wing extremist terrorist organizations or individuals have been identified in Estonia. The threat level from them is **low**.

¹⁴ Due to its involvement in aggression against Ukraine, the USA considers the organization to be terrorist; at the European Union level, the organization's key figures have been added to the sanctions list.

4. Overview of Terrorist Financing

According to the legislation¹⁵ in force in Estonia, terrorist financing is the financing of a terrorist crime or knowingly supporting it in any other way, making funds available or collecting them. Terrorist financing also includes financing or otherwise supporting a terrorist organization or person whose activities are aimed at committing a terrorist crime, making funds available or collecting them, or knowingly supporting them in any other way.

Figure 1. Phases of Terrorist Financing



In the context of terrorist financing, three phases are typically distinguished: raising, moving, and using funds. For analytical purposes, the concept of terrorist financing has also begun to include the storing, managing, and obscuring of funds.¹⁶ In this risk assessment, the three phases are considered for simplicity.

During the preparation of the terrorist financing risk assessment, the threats related to the financing of the following terrorist organizations were analyzed, taking into account their funding needs, sources of funding, and channels for moving funds: **ISIS, ISIS-K, Taliban, HAMAS, Kurdistan Workers' Party (PKK), Palestinian Islamic Jihad, Hezbollah**; right-wing accelerationist groups such as **Atomwaffen Division, Feuerkrieg Division, Base**, etc.; **Russian Imperial Movement, Russian Federation intelligence services**. In addition to terrorist organizations, the threats related to financing **by individuals** (both Islamist extremism and right-wing extremism) were also assessed.

¹⁵ Terrorist financing is defined by the Penal Code, which addresses terrorism and its financing in sections 2371–6. The financing and support of terrorist crimes and activities aimed at committing them are covered in section 2373, while the organization, financing, and support of travel for terrorist purposes are addressed in section 2376. The Money Laundering and Terrorist Financing Prevention Act (MLTFPA) bases its handling of terrorist financing on these sections of the Penal Code.

¹⁶ Davis, Jessica (2021). Prevention of Terrorist Financing. – Alex P. Schmid (Ed.), Handbook of Terrorism Prevention and Preparedness. The Hague: ICCT (International Centre for Counter-Terrorism), 444–473.
<https://www.icct.nl/handbook-terrorism-prevention-and-preparedness>

In general, terrorist organizations need funds depending on their size, scope of operations, and objectives. Organizations require funds for salaries, training, travel, implementing covert measures, logistics, propaganda, recruiting new members and supporters, etc. In the case of Islamist extremism, supporting the families of the deceased may also be included. Violent right-wing extremism often requires funds for legal expenses. If an organization controls territory, additional expenses for managing and maintaining unity are incurred. A lone actor, on the other hand, may use readily available resources to carry out a terrorist attack.

From the perspective of **fund collection**, a lone actor can rely on self-financing: salary, loans, social benefits, support from relatives, including pocket money from parents. This was also the case in a criminal case in Estonia related to the violent right-wing extremist movement (see case study 1) – the minors were supported by their parents. Terrorist organizations can collect financial resources through donations and support (NPOs, crowdfunding campaigns), apparent legal business activities, taxing the local population, or through organized crime (extortion, robbery, drug trafficking, human trafficking, fraud, etc.). The sending of funds in the form of crowdfunding campaigns to conflict zones has been observed in isolated cases in Estonia. In the case of violent right-wing extremism, it is characteristic to collect money and spread ideology through fight clubs and gyms, the sale of merchandise with symbols, income from organizing events (concerts and competitions), music production and sales, self-financing (donations, membership fees, salaries, etc.), and renting out real estate.

For the **transfer of funds**, both traditional transfer methods (payment services with a wide global network of payment agents) and modern information technology channels such as e-money institutions and virtual currencies can be used for the purpose of terrorist financing. All of this has also been observed through Estonia, as outlined below. The hawala system¹⁷ and cash couriers are still in use. It should be noted that no hawaladars, or hawala service providers in the classical sense, have been identified in Estonia, but the use of accounts with possible hawala characteristics can be observed. During the observed period, credit institutions have also reported this to the Financial Intelligence Unit. Terrorist financing can also occur as a symbiosis of the aforementioned different services.

In the sector of virtual asset service providers, connections with online casinos and remote gambling operators operating in third countries can be observed. Since the clients of such casinos and operators have been individuals who have had connections with cryptocurrency addresses categorized¹⁸ as terrorist through blockchain transaction analysis, this poses a certain risk of terrorist financing. However, in known cases, it has not been possible to prove that the casino and gambling sector has been knowingly used for terrorist financing.

Both in Estonia and globally, the development of information technology has also expanded the channels for terrorist financing. The transfer fees of various payment intermediaries and virtual asset service providers for global transactions have, in some cases, proven to be cheaper than traditional bank payments. The payment solutions of global companies offer faster transaction speeds and often additional anonymity, which is exploited by criminals. **Most transactions related to terrorist financing range from a few euros to a few dozen euros.** Although there are exceptions, reports indicating terrorist financing in the Estonian context typically involve small amounts. Terrorist organizations generally no longer share payment details publicly in their campaigns; more precise funding instructions are transmitted on private communication platforms and

¹⁷ Hawala – a traditional trust-based method of money transfer prevalent in the Middle East, Africa, and Asia, where money does not need to be physically sent to the destination. The hawala manager (hawaladar) can accept valuable items, real estate, or movable property instead of cash, and their value is converted into the money given to the recipient.

¹⁸ NBCTF – National Bureau for Counter Terror Financing of Israel.

in closed chat rooms. Advanced artificial intelligence, which allows the creation of realistic fake identities through deepfakes and the setup of fundraising campaigns supported by realistic-looking fake videos, is becoming increasingly accessible to a wider user base. Although deepfakes have not been identified in the Estonian context, service providers do notice forged documents.

In the case of terrorist financing, the purpose of the activity is concealed from the service provider, **the amount may be very small, and the origin of the funds may be legal. The person behind the transaction may also be hidden, using**, for example, **family members**, stolen or forged documents (with the growing threat of **deepfakes** in selfies). The use of family members and stolen and forged documents can also be seen in reports submitted to the Financial Intelligence Unit, particularly concerning clients of virtual asset service providers. Reaching a suspicion of supporting terrorist financing may require, in addition to **general monitoring and skillful use of tools, knowledge of other cultural areas and geopolitical conflicts**. Identifying a supporter of violent extremist ideology requires a **broader understanding of different ideologies and their symbols**. Additionally, it is increasingly possible to observe the blurring and merging of extremist ideologies – not only in terms of tactics and strategies but also in how an individual assembles an ideology from components that suit them.

Historically, countering terrorism, and consequently preventing terrorist financing has focused on geographical risk. Unfortunately, this approach is no longer sufficient today, as the number of Islamist radicals has grown and continues to grow in Western countries that fall outside the geographical filter. This makes monitoring cross-border transactions and detecting terrorist financing more complex and requires more attention and knowledge from market participants.

This is a challenge for the entire prevention system. Therefore, cooperation with supervisory and security agencies plays an increasingly important role. In the case of terrorist financing, it is also inevitable that it occurs in **small amounts** and that there are few cases (considering the number of transactions), which means that **anomalies may remain invisible during big data analysis**.

5. National Terrorist Financing Threats

The level of terrorist financing threat in Estonia is medium (see Table 1).

The national terrorist financing threat is divided into four categories: 1) **internal threat**, 2) **outgoing threat** (threat arising from Estonia to other countries), 3) **incoming threat** (external threat), and 4) **transit threat** (threat arising from transit). Additionally, the umbrella terms “domestic threat” and “cross-border threat”¹⁹ are used to encompass the previous categories:

- **Internal threat level – low**
- **Outgoing threat level – medium**
- **Incoming threat level – medium**
- **Transit threat level – above average**

The threat level assessment (see also Table 1) is based on the fact that Estonia has a low level of internal terrorist financing threat, a medium level of outgoing and incoming terrorist financing threat, and above average level of transit terrorist financing threat. Estonia’s strong financial sector faces additional terrorist financing threats stemming from financial services and assistance provided to countries with a higher risk of terrorist financing²⁰. The domestic and cross-border terrorist financing threat in Estonia increased due to Russia’s military aggression towards Ukraine and the associated hostilities directed at NATO and Western countries. As a neighboring country to Russia, Estonia faces cross-border threats related to the trade of strategic goods/weapons. The threat level of using funds collected in Estonia for terrorist purposes within the country is low. However, Estonia’s geographical location, open economic environment, and financial services – especially through correspondent relationships – make the country vulnerable to threats related to the transfer of funds for terrorist purposes and, to a lesser extent, the collection of funds.

The main threats are associated with the **movement of funds**, which may occur through market participants operating within Estonia’s jurisdiction via **correspondent relationships**.

¹⁹ The domestic threat consists of internal, outgoing and incoming threat. The cross-border threat consists of outgoing, incoming and transit threat. Both the domestic and cross-border threat levels are medium. Both contribute to the national threat level.

²⁰ The list of countries with a higher risk of terrorist financing is published as an annex to the guidelines on suspicious transaction indicators by the Financial Intelligence Unit: <https://www.fiu.ee/oigusaktid-ja-juhendid/juhendid#korgema-terrorismi-r>. The determination of countries with a higher risk of terrorist financing takes into account the assessments and reports of international organizations (EU, FATF, etc.) in line with the threat assessments of Estonian authorities, as well as the existing connections of Estonian service providers with various countries. A higher risk of terrorist financing does not mean that a specific country finances terrorism, but it indicates a risk that may materialize under certain circumstances. The list of countries with a higher risk of terrorist financing is reviewed annually and updated as necessary.

Levels of terrorist financing threats by umbrella criteria:

- **Arising from terrorist attacks and activities within the jurisdiction.**
Domestic – low, cross-border – medium.
Trend: increasing.
- **Arising from terrorist organizations and individuals within the jurisdiction.**
Domestic – very low, cross-border – very low.
Trend: stable.
- **Related to individuals who support terrorist organizations, individuals, and ideologies.**
Domestic – very low, cross-border – very low.
Trend: increasing.
- **Arising from active terrorist threats in neighboring jurisdictions.**
Incoming threat – medium, outgoing threat – low.
Trend: increasing.
- **Arising from financial centers. Cross-border threat (transit): very low.**
Trend: stable.
- **Related to strategic goods and services. Cross-border threat (transit): medium.**
Trend: stable.

5.1. Internal Threat

Internal threat refers to domestic threats arising from the conditions in Estonia. In the case of internal threat, all phases of terrorist financing (collection, transfer, use) occur within Estonia.

The level of internal terrorist financing threat in Estonia is **low**.

There are no Islamist, right-wing extremist, or left-wing extremist terrorist organizations or their cells operating in Estonia. Additionally, there are no fighters associated with terrorist organizations living here. The main threat comes from radicalized individuals who generally self-finance. The number of extremely radicalized individuals in Estonia is also small. However, during the observed period, there was one case involving minors who spread the ideology of violent right-wing extremism.

Due to the support for violent ideology, the level of internal threat in the country is low. The Muslim community is relatively small and peaceful. There is a somewhat larger number of individuals who support right-wing extremism and those who sympathize with the Russian Federation. During the observed period, there were no cases of terrorist financing. Consequently, the risk of using funds collected for Islamist terrorism purposes in Estonia is low. The level of threat of financing violent right-wing extremism is low. The identified and prosecuted cases have been related to lone actors who self-financed.

Looking ahead, the demographic threat cannot be overlooked: **the growth of the Islamic community in Estonia** with connections to high-risk countries²¹. In 2019, there were about 4,300 individuals from high-risk

²¹ The list of countries with a higher risk of terrorist financing is published as an annex to the guidelines on suspicious transaction indicators by the Financial Intelligence Unit: <https://www.fiu.ee/oigusaktid-ja-juhendid/juhendid#korgema-terrorismi-r>. The determination of countries with a higher risk of terrorist financing takes into account the assessments and reports of international organizations (EU, FATF, etc.) in line with the threat assessments of Estonian authorities, as well as the existing connections of Estonian service providers with various countries. A higher risk of terrorist financing does not mean that a specific country finances terrorism, but it indicates a risk that may materialize under certain circumstances. The list of countries with a higher risk of terrorist financing is reviewed annually and updated as necessary.

countries living in Estonia, and by 2024, this number had increased to about 10,000. The emergence of larger communities tends to lead to communal isolation – the larger the community, the more possible it is to live daily life without leaving one’s linguistic and cultural environment. From a security perspective, it is important that parallel societies do not emerge in the country, which may, under the influence of charismatic individuals, including those from foreign countries, wish to establish internal rules that may be considered superior to Estonian laws and societal norms. **The isolation and segregation of communities provide fertile ground for radicalization**, thereby increasing the threat levels of both terrorism and terrorist financing. The pressure of migration from high-risk countries to Estonia persists. Additionally, there is pressure from entrepreneurs to bring in cheap labor and to ease immigration quotas for this purpose. There is no set limit on the immigration of top foreign specialists, but employers are required to pay them 1.5 times the average Estonian salary.

Integrating community members into Estonian cultural and legal frameworks is important from the perspective of both Islamist and Russian-origin terrorist financing threats.

The demographic threat also applies to violent right-wing extremism – increasing immigration generally increases the number of individuals with right-wing extremist views. **Currently, the threat level arising from the demographic situation is low, but it is on an upward trend.**

CASE STUDY 1. Youth Associated with the Violent Right-Wing Extremist Movement Feuerkrieg Division (FKD)

Young people radicalized online were engaged in promoting white supremacy in Estonia and around the world. Through internet communication platforms and posters, they incited hatred against immigrants, Jews, people of color, sexual minorities, journalists, and police officers. Additionally, they spread hostility against the state as a whole, based on the ideology of the accelerationist group. No terrorist financing was identified in the criminal case; the youths were supported by their parents, who were unaware of their children’s activities.

5.2. Outgoing Threat

The outgoing threat refers to the threat posed by Estonia’s jurisdiction to other countries.

The level of outgoing terrorist financing threat is **medium**.

A significant source of threat is **the support for terrorist organizations related to Russia**. Considering the relatively large community living within the influence of the Russian Federation’s information sphere in Estonia, it is likely that the number of supporters of the Russian Imperial Movement (RIM) or the idea of Russian imperialism may be relatively high. However, no individuals have been identified who wish to actually finance RIM. Although RIM has conducted fundraising campaigns on Russian-language social media, no funds have been identified as being sent from Estonia. In the case of Russian intelligence services, more complex financial schemes for obtaining funds cannot be ruled out, but none have been identified so far.

In terms of Islamist terrorism, the threat comes from fundraising campaigns for terrorist organizations under the guise of charity, which can reach Estonian residents via the internet. This means the financing of terrorist organizations by Estonian residents through crowdfunding or other fundraising methods, either intentionally or accidentally, out of ignorance or negligence. The main threat lies in the fact that **money is sent for charitable purposes to (conflict) areas** where there is no clear overview and control of both the

end-user and the actual use of the collected funds, i.e., to areas that are more or less under the control of terrorist organizations.

Based on the experiences of other countries, it is likely that funds collected in Estonia may become accessible to foreign terrorist organizations through crowdfunding²² platforms. At the end of the period under review, the threat level associated with fundraising was mainly raised by the war between HAMAS²³ and Israel that began in October 2023, and the accompanying international charitable fundraising campaigns and the use of crowdfunding platforms. Estonian residents also participated in such campaigns – **funds were collected and transferred from the Estonian jurisdiction for charitable purposes to support civilians in the Gaza**. Since the territory was controlled by a terrorist organization at that time (extortion, kidnapping, bribery), it is not possible to completely rule out the possibility that the funds from well-intentioned supporters ended up in the hands of the terrorist organization.

A significant threat is associated with the activation of ISIS-K²⁴ in Central Asia, particularly in Tajikistan, Kyrgyzstan, and Turkmenistan, which has led to the recruitment of members among the local population. The threat originating from Estonia is related to **workers of Central Asian origin, who are characterized by sending funds to their homeland through cross-border payment services and financial institutions**. Since there is no legal cooperation with **Tajikistan, Kyrgyzstan, and Turkmenistan**, identifying the recipient of funds sent from Estonia is problematic, and it cannot be ruled out that the funds may end up supporting terrorist organizations or individuals associated with them.

At the same time, the migration pressure from the mentioned region to both Estonia and the European Union as a whole increased. Several Estonian companies compensated for the departure of Russian, Ukrainian, and Belarusian citizens from the labor market due to Russia's aggressive war against Ukraine by recruiting citizens of Central Asian countries for short-term work. Their number increased significantly in 2022–2023.²⁵

To mitigate the threat of terrorist financing, all three aforementioned countries were added to the list of countries with a higher risk of terrorist financing. Control over the arrival of workers from Central Asia with short-term work permits and their legal stay in Estonia was increased, resulting in a significant decrease in the number of workers from that region in Estonia in 2024.²⁶

It is also important to note the risks associated with **the exploitation of Estonia's open economic and business environment and the e-residency program by terrorists** to infiltrate both Estonia and the EU under the guise of legitimate business development. It is easy for e-residents to establish a legal entity. The risk level of exploiting the **e-residency program for terrorist financing purposes is moderate, as several individuals with links to terrorism were identified during the period under review, who had been granted e-residency. All such permits were revoked**.

²² For example, GoFundMe, www.gofundme.com

²³ HAMAS – Ḥarakat al-Muqāwamah al-Islāmiyyah (Islamic Resistance Movement) – is a Sunni Islamist political organization with a military wing (Qassam Brigades). The organization has governed the Gaza since 2007. The European Union, the USA, Israel, the UK, Japan, New Zealand, and Canada have recognized HAMAS as a terrorist organization.

²⁴ ISIS-K – The Islamic State – Khorasan Province; also known as ISKP. The Central Asian branch of Daesh/ISIS.

²⁵ As of October 2022, short-term work permits had been granted to 4,147 citizens of Central Asian countries, which constituted about 75% of those registered for short-term work from high-risk countries at that time.

²⁶ As of November 2024, there were 1,051 individuals of Central Asian origin with short-term work permits in Estonia.

CASE STUDY 2: Attempts to Send Funds to Gaza (Various Cases)

In 2023, various individuals, in connection with the HAMAS-Israel war, attempted to send money through the Estonian jurisdiction for humanitarian reasons to both individuals and organizations in the Gaza Strip. Most of the supporters were foreign nationals, but there were also e-residents and Estonian citizens. Among the organizations, Gaza Now propaganda channels with links to HAMAS were identified.

The upcoming transactions noticed by credit institutions were halted. Legal cooperation was carried out within Estonia with the Estonian Internal Security Service and the Financial Intelligence Unit, as well as with foreign cooperation partners, to identify the transactions and participants involved. The e-residency statuses of the associated individuals were revoked.

CASE STUDY 3: Individuals with Extremist Links Identified Among E-Residents

In 2021, a case was identified where two individuals, as e-residents, established a company in Estonia that offered a streaming service. The content of the service was music provided on their self-created streaming platform, which had an ideological message aligned with violent right-wing extremism. The individuals were associated with the organization Nordic Resistance Movement (NRM). While NRM is not listed among terrorist organizations at the European Union level, it has been declared a terrorist organization by the United States (USA) and its activities have been banned in Finland. The organization operates mainly in Sweden, but also in Norway and Denmark. The e-residency status of the individuals was revoked.

CASE STUDY 4: Short-term Workers Suspected of ISIS-K Links

In 2022, individuals from Central Asia arrived in Estonia for short-term work, and it was discovered that they had links to ISIS-K. The employment of these individuals inevitably involved a financial component, i.e., the payment of wages and their subsequent use. Foreign workers from Central Asia typically send part of their salary back home. In this case, no terrorist financing was detected. All foreign workers involved in this case have now left Estonia.

5.3. Incoming Threat

Incoming threats refer to dangers originating from other jurisdictions. This means situations where foreign countries or individuals outside of Estonia attempt to finance terrorist activities within Estonia.

The level of incoming terrorist financing threat is **medium**.

The risk of sending money from abroad to establish Islamist terrorist organizations in Estonia or to carry out Islamist-motivated terrorist acts here is low.

The greatest source of threat is Russia, which, as an aggressive state hostile to Europe and NATO, actively seeks through its special services to find individuals in Western countries, including Estonia, willing to carry out terrorist acts in its interests and is willing to finance them. Russia remains a persistent source of threat as an aggressive state hostile to Europe and NATO.

Regarding the level of terrorist financing threat from neighboring countries, the level of terrorism threat in the Baltic States is low, which in turn affects financing. In the Scandinavian countries and Russia, there are large Muslim communities, among whom there are individuals spreading radical Islam and a considerable number of returning foreign fighters. There are also quite a few right-wing extremists in Scandinavia (see Case Study 3 for the context of Estonia).

As previously mentioned, there are no terrorist organizations in Estonia, and the number of people supporting radical ideologies is small. This means that it is not worthwhile to send funds to Estonia for terrorist financing, and the Estonian population is not directly targeted. However, propaganda and influence activities carried out on the internet have a greater impact, especially on individuals.

5.4. Transit Threat

The transit threat refers to situations where foreigners outside of Estonia use products and services offered within the Estonian jurisdiction to support terrorist organizations or individuals. This can also mean the physical movement of funds through Estonia.

The level of transit terrorist financing threat is **above average**.

The main threat is related to **correspondent relationships** and involves the transfer of funds through Estonian service providers. Transactions are conducted through the legal entity client of the Estonian service provider (credit institution or virtual asset service provider). The respondent institution's individual client, who transfers the funds, also resides elsewhere. For example, in 2022, a VIBAN account was opened for an individual who had been convicted of terrorist financing in another jurisdiction and was in prison (see also Case Study 6). In the case of virtual asset service providers, there is a risk that an individual with terrorism links may conduct transactions using the nested service provided by a VASP client with an Estonian license (see Case Study 5). The respondent institution of the VASP may not apply due diligence measures to the necessary extent (including being located in an offshore area) and may offer payment options in private coins.

The number of individuals with terrorism links traveling through Estonia has increased. In neighboring countries (Russian Federation, Finland, Sweden), there are relatively large Islamic communities from the Balkans, North Caucasus, as well as Somalia, Iraq, and Syria, among whom there are numerous individuals with terrorism links who travel between their new and old homelands via Estonia. The Russian Federation's war against Ukraine and hybrid attacks on the borders of Finland, Latvia, Lithuania, and Poland, followed by border closures, have led to an increase in transit through Estonia. While in the years 2020–2022, about 50 individuals with identified terrorism links passed through Estonia annually, in 2024, this number was about 200 people per year. The increase is primarily related to people traveling through Estonia to and from Russia.

In the case of individuals in transit with terrorism links, the following circumstances have been identified, which may be related to possible terrorist financing: large amounts of cash in various currencies (these are cases that occurred at Schengen internal borders, where there is no declaration requirement), various debit cards, including those of VASPs, and packaged smart devices.

A factor that increases the threat level is the fact that there is generally no cash declaration requirement when moving within the Schengen area. However, some member states have separate control and declaration provisions for intra-Community cash movements, which are applied in addition to EU regulations. The risk level is lower in the direction of export, as there is 100% border and customs control at the Estonian-Russian border. No cases of terrorist financing [Penal Code § 237 (3)] were identified during the assessment period, but financial investigations were conducted for intelligence purposes to identify possible terrorist financing.

6. Vulnerabilities

6.1. National Terrorist Financing Vulnerabilities

The assessment of national vulnerabilities is based on the analysis of the following factors: 1) the country's ability to prevent terrorist financing threats, 2) sectoral vulnerabilities, and the presence, effectiveness, and awareness of control measures among market participants. National vulnerabilities are examined by category: internal, outgoing, incoming, and transit threat. The national vulnerability assessment is influenced by the country's ability to prevent specific threats and the overall sectoral²⁷ vulnerability.

National vulnerabilities by category:

- **National vulnerability to internal terrorist financing – below average**
 - Overall sectoral vulnerability – below average
 - The country's ability to prevent internal terrorist financing – above average
- **National vulnerability to outgoing terrorist financing – below average**
 - Overall sectoral vulnerability – below average
 - The country's ability to prevent outgoing terrorist financing – above average
- **National vulnerability to incoming terrorist financing – below average**
 - Overall sectoral vulnerability – below average
 - The country's ability to prevent incoming terrorist financing – above average
- **National vulnerability to transit terrorist financing – average**
 - Overall sectoral vulnerability – below average
 - The country's ability to prevent terrorist financing arising from transit – average

The criteria that were evaluated are as follows:

- The quality of the policy and strategy for preventing terrorist financing,
- The effectiveness of the definition of the crime of terrorist financing,
- The effectiveness of customs and border controls in preventing terrorist financing,
- The quality of information collection and processing related to terrorist financing,
- The quality of investigations into terrorist financing,
- The quality of prosecution for terrorist financing,
- The quality of adjudication for terrorist financing,
- The quality of mechanisms for confiscating and seizing assets related to terrorist financing,
- The quality of targeted financial sanctions related to terrorism and terrorist financing,
- The control of strategic equipment, goods, and services related to conflict areas.

These criteria also had sub-criteria.

²⁷ The overall sectoral vulnerability assessment (below average) takes into account the vulnerabilities of the sectors in conjunction with the presence, effectiveness, and awareness of control measures among market participants (see 6.2).

Table 3. National Capability to Prevent Terrorist Financing

Category	Threat	Vulnerability	Capability to prevent	Residual risk
Internal	low	below average	above average	below average
Outgoing	medium	below average	above average	medium
Incoming	medium	below average	above average	medium
Transit	above average	medium	medium	above average

Major Vulnerabilities

The legislation governing the prevention of terrorist financing in Estonia is well-regulated. The relevant law is the Money Laundering and Terrorist Financing Prevention Act (hereinafter “MLTFPA”). The Penal Code defines terrorist crimes in almost all possible aspects. Under Penal Code § 237³, the punishment is proportional and has a sufficient deterrent effect²⁸.

From 2020 to 2024, no criminal cases of terrorist financing (i.e., crimes qualifying under Penal Code § 237³) were initiated in Estonia. During the assessment period, the prospect of initiating criminal cases under Penal Code § 237³ (financing and supporting terrorist crimes and activities aimed at committing them) was repeatedly considered based on reports forwarded by the FIU. However, as these cases generally involved the provision of correspondent relationships by virtual asset service providers to companies operating in third countries for individuals in conflict areas, the likelihood of interrogating, involving in judicial proceedings, and convicting them is almost non-existent. The possibility of conducting criminal proceedings as joint investigations within the framework of international cooperation was also considered.

In close cooperation between the FIU and the Estonian Internal Security Service, an alternative measure was adopted: in addition to sharing information within the framework of international cooperation, the Financial Intelligence Unit restricted the availability of funds suspected of terrorist financing to the mentioned individuals in conflict areas (with reference to the Council of the European Union Regulation No. 2580/2001, Article 2(1) of 27 December 2001).

The area of preserving terrorist propaganda, which is not regulated by the EU’s TCO (terrorism content online) regulation, needs additional regulation. Terrorist financing is a first-degree crime, which allows for sufficiently stringent punishment²⁹. Courts have the opportunity and obligation to reclassify the crime if necessary, in accordance with the Code of Criminal Procedure (§ 306) and case law. Estonia has judges and prosecutors specialized in financial crimes, and the prosecution has financial analysis support. The competence for pre-trial investigation of criminal cases related to terrorism lies with the Estonian Internal Security Service. The level of independence and reliability of courts, prosecution, procedural, and supervisory authorities is high. Both the Estonian Internal Security Service and the prosecution have experience in handling criminal cases related to terrorism.

The state’s strategy for preventing terrorist financing (the Ministry of the Interior’s Internal Security Development Plan, STAK) is formulated with sufficient detail and is regularly updated. This is complemented by the internal action and intelligence plans of the agencies responsible for preventing terrorism.

²⁸ It is important to note that in the 2022 MONEYVAL report, Estonia’s technical compliance with FATF Recommendation 5 (the criminalization of terrorist financing) was rated as LC (Largely Compliant). The report states that although most of the offenses listed in the annex to the International Convention for the Suppression of the Terrorist Financing are criminalized in Estonia, their financing is not considered a terrorist financing offense. This deficiency remains.

²⁹ The penalty for terrorist financing can be up to ten years of imprisonment (similar to Finland and Germany).

The institutions responsible for preventing terrorist financing are primarily the FIU, the Financial Supervision Authority, and the Estonian Internal Security Service, whose tasks are clearly defined and regulated. The cooperation and information exchange between competent authorities within the country work very well. The resources and capabilities of the FIU have increased during the period under review, which is reflected in the number of employees, the availability of necessary analytical tools, and training. The mandate to obtain information is good. International cooperation and information exchange with Western partner institutions are very good, with participation in various international cooperation projects and EU working groups.

Law enforcement agencies have access to both state and independent databases, as well as information on beneficial owners. The infrastructure related to information databases in Estonia is very good. The public also has access to some state databases (commercial register, beneficial owners' register, land register, court decisions database, etc.).

The control of cash movements at the Schengen external border and the control of strategic goods at the border by the Tax and Customs Board are effective.

In the areas discussed above, the country's capacity to prevent terrorist financing is **above average**.

Areas where the country's capacity to prevent terrorist financing needs improvement:

- **Effectiveness of international counter-terrorism cooperation** – vulnerability level **higher than average**.
The exchange of information between countries/allied countries sharing the same values is good and fast. The problematic area is the exchange of information with third countries outside the EU and those with which there is no legal cooperation (including Russia). Unfortunately, these countries have the largest number of terrorists and terrorist organizations.
- **Confiscation and freezing of assets** – vulnerability level **lower than average**.
The legislative framework is in place and largely functional. The system's drawback is that assets can only be confiscated upon a conviction. In the case of terrorist financing crimes, the suspect/offender may not be in Estonia at all, and their case cannot be prosecuted in Estonia, i.e., they cannot be convicted. The court practice of administrative confiscations is still developing.
- **Imposition of international sanctions** – vulnerability level **lower than average**.
Adding to the EU sanctions lists is simple, but it is complicated through the UN due to the risk of veto. Estonia implements UN Security Council resolutions without delay, and there is an appropriate domestic legal framework for this. Minor deficiencies remained in the regulation of asset freezing, such as limited cases and types of assets that can be frozen. There are also restrictions on the prohibition of making assets available, and there are minor deficiencies related to updating guidance materials for obligated entities.
- **Resources and capabilities needed to handle criminal cases of terrorist financing** – vulnerability level **lower than average**.
From the perspective of the Penal Code and criminal procedure, the situation is good. There were setbacks during the period in terms of the ability to obtain evidence – European Court decisions limited the collection of communication data. The capacity of law enforcement agencies to collect evidence deteriorated, and the possibilities for obtaining evidence decreased.

6.2. Sectoral Vulnerabilities

All sectors considered as obligated entities³⁰ were examined, with a more detailed analysis conducted on selected sectors. The selection was based on the volume and turnover of the sector's services, previous cases, and risk typologies. The following sectors were chosen for more detailed assessment: virtual asset service providers (VASPs), credit institutions, payment institutions, including cross-border payment services (money transfer service providers and currency exchangers), and e-money institutions³¹ (both domestic and foreign), as well as crowdfunding service providers. No significant terrorism risks were identified in other sectors.³² A separate comment is added regarding corporate service providers and the e-residency program (see point 6.2.5).

The main vulnerability remains that participants in the Estonian financial system and their service environments may be used for the **transfer of funds**. A considerable risk is associated with transactions made with foreign contracting partners, such as the nested service offered by service providers with an Estonian operating license (in the case of the VASP sector) and **correspondent relationships (in the case of the credit institution sector)**, where one account may serve hundreds or thousands of client customers, whose monitoring relies significantly on the processes and systems of the respondent institution, to service providers registered in offshore areas. Risks continue to be posed by those VASPs that provide nested services in third countries where due diligence measures are not adequately applied and payment options are offered in privacy coins.

The level of sectoral vulnerability is influenced by 1) **the inherent vulnerability of the sector** and 2) **the quality of terrorist financing prevention controls**, which are further divided into sub-criteria.

The criteria examined for these two assessments were as follows:

- the sector's suitability/usefulness for terrorist financing,
- the volume and turnover of the sector,
- the profile of the customer base,
- outgoing international transactions,
- outgoing international transactions to higher-risk jurisdictions,
- incoming international transactions,
- incoming international transactions from higher-risk jurisdictions,
- use of cash,
- use of agents, service providers, and intermediaries,
- other vulnerability factors,
- the quality of the terrorist financing prevention policy and strategy,
- the quality of terrorist financing prevention practices and activities.

These criteria were further divided into sub-criteria.

6.2.1. Virtual asset service providers

The sector's threat level is average, **the vulnerability level is below average**, and the residual risk level is average.

³⁰ MLTFPA § 2. <https://www.riigiteataja.ee/akt/113032019126?leiaKehtiv>

³¹ E-money institutions include services such as Paysera, Revolut, Koronapay, OpenPayd, Papaya, Paysafe, Payward, etc.

³² A separate analysis will be prepared regarding non-profit organizations (associations and foundations).

The main threats concern nested services, where the sector of Estonian virtual asset service providers has been used for terrorist financing (see example case 5 below). Most of the threats originate from foreign nationals living abroad. The greatest threat concerns transit, but incoming and outgoing threats are also possible.

Major Vulnerabilities

- It allows for anonymity and is therefore attractive, among other reasons.
- Correspondent relationships.

Transactions are made through the legal entity client of the Estonian service provider, i.e., the respondent institution, which operates in another jurisdiction. The client of the respondent institution, the so-called end client – usually an individual who wishes to send funds – also resides elsewhere. Among the end clients of Estonian service providers, individuals with links to terrorism who conduct transactions from other jurisdictions have been identified.

- The sector's turnover is very large.

The transaction value of VASPs with an Estonian operating license across various services provided in our jurisdiction is significant, exceeding 30 billion euros annually.³³ However, VASPs with an Estonian operating license constitute a small part of the global market. Most transactions are carried out on the platforms of global companies.

- The ability to conduct transactions quickly, anonymously, and internationally.

The ability to establish client relationships and conduct transactions remotely (including the risk of deepfakes) and relatively anonymously; the speed and international nature of transactions, tokens and services that allow anonymity, including the possibility of hiding transfers (mixers), make the sector very suitable from the perspective of terrorist financing. There are many currencies with different characteristics and uses on the market, and it is currently not possible to keep statistics on their use.

- The ability to track activities in the blockchain system applies in practice only to the most common virtual currencies.

This requires that service providers with an Estonian operating license provide their employees with the necessary training to use the tool, comply with the due diligence measures required by law, and report suspicions of terrorist financing as prescribed by law.

- Only a small portion of service providers submit reports on the risk and suspicion of terrorist financing.

The number of reports submitted by virtual asset service providers (reports on the risk and suspicion of terrorist financing) has increased (see Table 4), but only a small portion (less than ten) of all service providers still submit reports. This may indicate the sector's low and uneven awareness of the possibilities of terrorist financing and the low and uneven ability to detect such transactions, including the inadequate application of due diligence measures.

³³ More detailed statistics on the VASP sector can be found in the NRA money laundering report chapter.

Table 4. Reports indicating terrorist financing submitted by VASPs to the FIU

	2020	2021	2022	2023	2024
TFR-1³⁴	44	67	144	87	48
TFR-2³⁵	3	0	3	34	11
Total	47	67	147	121	59

Source: FIU.

- Companies licensed in Estonia but operating mainly outside Estonia.

Such companies generally do not have sufficient knowledge of the Estonian legal system, do not follow local guidelines in their activities, and do not properly implement due diligence measures, making them vulnerable.

- Companies operating in the so-called grey area.

Some virtual currency companies are registered in Estonia and offer services here, but they operate under the VASP license of another jurisdiction, following the laws of that country. This type of business not only poses a security threat but also causes reputational damage to Estonia in case of problems, rather than to the country that issued the license.

- Many companies have payment accounts outside Estonia.

The transparency of the sector's activities is reduced by the fact that a significant portion of payment accounts are located in Lithuania, the United Kingdom, and Malta.

Factors mitigating vulnerability:

- The market for virtual asset service providers has been significantly regulated and national regulations have been thoroughly updated.

As of December 31, 2020, there were 846 licenses for virtual asset service providers (of which 473 were active), but by December 31, 2024, this number had decreased to 42. Additionally, ATMs intended for the purchase and sale of virtual currency, of which there were 10 at the beginning of the period, were closed in Estonia.

- The sector-specific guidelines updated in 2022 in cooperation with the FIU and the Internal Security Service.

The guide on the characteristics of suspicious transactions, which helps market participants better recognize the risk and suspicion of terrorist financing transactions, highlights the relevant indicators from the perspective of virtual asset service providers. In addition, in 2022, a list of countries with a higher

³⁴ **TFR-1** – a report indicating the risk of terrorist financing. It must be submitted when a party involved in the transaction (an individual, legal entity, or other association) is connected to a high-risk country, a risk indicator is present, and there is an aspect of unusualness. The transaction or operation may continue if enhanced due diligence measures are applied. Additionally, all known risk indicators must be submitted. <https://fiu.ee/terrorismi-rahastamisele-viitava-teate-esitamise-rahapesu-andmepuuroole>

³⁵ **TFR-2** – a report indicating suspicion of terrorist financing. It must be submitted when a suspicion indicator is present. A suspicion indicator is sufficient to submit a TFR-2 report; the connection with a high-risk country does not play a role. Such a transaction must be stopped until further instructions from the competent authority, and the obligated entity is prohibited from making any funds available to the client. Additionally, all known risk indicators must be submitted. <https://fiu.ee/terrorismi-rahastamisele-viitava-teate-esitamise-rahapesu-andmepuuroole>

risk of terrorist financing from the Estonian perspective was made available to the public and market participants as an appendix to the guidelines. This list is updated annually or as needed.

- Significantly improved awareness and ability to apply due diligence measures among market participants.

This has been contributed to by increased regulation, robust supervisory activities, and training activities³⁶. Problems still exist – only a small portion of the sector submits reports indicating suspicion of terrorist financing, and there are also issues with the quality of the reports³⁷. However, the reports submitted by the sector show that active service providers are able to recognize suspicions of terrorist financing and suspicious individuals, skillfully using the relevant tools and methods, including public sources.

Case Study 5: Attempt by a network associated with the terrorist organization Palestinian Islamic Jihad to move virtual currencies through an Estonian service provider

In 2023, individuals who had previously conducted transactions on other platforms with the terrorist organization Palestinian Islamic Jihad attempted to deposit funds with an Estonian virtual currency service provider. This was an 18-member network identified thanks to the due diligence measures applied by the service provider.

The Estonian-licensed virtual currency service provider had a legal entity client located in another jurisdiction as part of a correspondent relationship, which in turn had individual clients (the so-called end clients) who also resided in another jurisdiction. These individuals had sent funds to various crypto addresses of the terrorist organization on other platforms. Additionally, they had received funds from terrorist organizations, directly indicating their actions in the interest of the organization. The transaction amounts were very large from the perspective of terrorist financing: in the hundreds of thousands of euros.

Subsequently, members of the network attempted to conduct transactions through the Estonian jurisdiction by depositing funds in small amounts. The funds of the network located in the Estonian jurisdiction were frozen in the total amount of 8,205 euros (8,963 USDT, cryptocurrency Tether).

6.2.2. Credit Institutions

The sector's threat level is below average, the **vulnerability level is below average**, and the residual risk level is below average.

According to Europol³⁸, funds are still commonly moved through banks for terrorist financing. However, this occurs less in countries where strict control mechanisms and risk profiling are applied or where anti-money laundering laws have been strengthened. The Estonian banking sector meets these conditions.

The main threat is the use of credit institutions to support terrorist financing through VIBAN accounts and correspondent relationships. This is primarily a transit-based threat.

³⁶ During the period under review, the Financial Intelligence Unit organized 13 training sessions for the virtual asset service provider sector, which covered, among other things, the sector's due diligence measures and reporting obligations. Four of these training sessions specifically addressed the prevention of terrorist financing from the perspective of virtual assets. Additionally, the sector was involved in all cross-sectoral training sessions.

³⁷ Quality-related statistics are available for the period 2022–2024 and cover all types of reports submitted by the sector. The percentage of problematic reports was 14%, 12%, and 11%, respectively.

³⁸ Europol: European Union Terrorism Situation and Trend Report 2023. Publications Office of the European Union, Luxembourg 2023, p. 21.

Major Vulnerabilities

- Correspondent relationships.

The sector's greatest vulnerability is similar to that of the VASP sector. Transactions are made through the legal entity client of the Estonian service provider, i.e., the respondent institution, which operates in another jurisdiction. The client of the respondent institution, the so-called end client – usually an individual who wishes to send funds – also resides elsewhere. Among the end clients of Estonian service providers, individuals with links to terrorism who conduct transactions from other jurisdictions have been identified.

- Service provision through VIBAN accounts.

This is generally associated with cross-border payment service providers and virtual asset service providers. The application of due diligence measures appears satisfactory in such cases, but reporting may sometimes be too slow due to the correspondent relationship.

- High turnover and customer base.

Factors mitigating vulnerability:

- The number of banks with correspondent relationships for providing VIBAN services is small³⁹.

A few credit institutions offer settlement accounts to other credit and financial institutions for serving their own clients within the framework of correspondent relationships. The risks associated with correspondent banking in Estonia are concentrated in the hands of only a few market participants.

- Good awareness of the threats of terrorist financing.

Good awareness is evident from the fulfillment of reporting obligations, willingness to cooperate, and participation in working groups. The approach to non-residents is conservative. E-residents are treated as non-residents. About 5% of the clients of Estonian credit institutions are non-residents, and the proportion of clients from higher-risk countries has decreased⁴⁰ during the period under review.

- Good investment in the field of anti-money laundering and counter-terrorist financing, and regular training of employees.
- The sector has an actively functioning umbrella organization in the form of the Estonian Banking Association, and information related to counter-terrorist financing is exchanged between banks in a separate working group.

³⁹ For more details see the chapter on financial sector vulnerabilities in the NRA 2025 money laundering report.

⁴⁰ For more details see the chapter on financial sector vulnerabilities in the NRA 2025 money laundering report.

CASE STUDY 6: Opening of a VIBAN account for a foreign national convicted of terrorist financing

In 2022, a virtual account number (VIBAN account) was opened for a foreign national within the framework of a correspondent relationship in the Estonian financial system. The individual had been convicted of terrorist financing in another jurisdiction and was imprisoned there. They had attempted to join fighters in Chechnya, sent funds to support fighters in Syria, and tried to purchase materials for making an explosive device. However, the individual's background was identified before they could make payments through the Estonian financial system.

6.2.3. Payment institutions, including cross-border payment services (money transfer service providers, currency exchangers)

The sector's threat level is average, the **vulnerability level is medium**, and the residual risk level is average.

The main threat is the use of Estonian payment institutions to send funds to countries with a higher risk of terrorist financing. This threat is outgoing threat.

Major Vulnerabilities

- Cash shipments through cross-border payment service providers and financial institutions licensed in foreign countries.

The use of cash remains widespread in so-called high-risk countries where the banking sector is weak or inaccessible to most of the population.

The service allows for cash transfers to countries with a higher risk of terrorist financing, where conventional channels may not function adequately or where there is a deliberate intention to avoid them. Identifying the parties involved in transactions conducted through such alternative payment channels in third countries is generally difficult. The final recipient of the funds may not be clearly identifiable. Transactions may also be conducted to avoid more transparent channels. Money transfer services are a convenient channel for terrorist financing, with Western Union and Moneygram being preferred due to their extensive global network of payment agents. Several transactions suspected of terrorist financing have been identified in cooperation with both Western Union service providers and the local payment agent Omniva.

- For currency exchange, identification is not required for amounts below 1000 EUR.

However, terrorist financing generally occurs in small amounts. Reports from market participants are few and usually come from only one service provider, which may indicate the sector's overall low awareness of the risks of terrorist financing.

- Payment institutions may be used in longer transaction chains, for example, money transfers combined with the use of virtual currencies, which further complicates the detection of terrorist financing.
- The measures to prevent terrorist financing by intermediaries (payment agents) operating in high-risk countries are generally poor or non-existent. Identifying the other party to the transaction in the high-risk country is challenging.

Factors mitigating vulnerability:

- For money transfer services, the party located in Estonia is generally well-documented for both outgoing and incoming payments.
- The volume of incoming and outgoing transactions is not large.

A significant vulnerability of e-money institutions is related to cross-border e-money service providers licensed in foreign countries and their resellers⁴¹. The biggest challenge for e-money service providers is the limited possibilities for information exchange with cross-border e-money institutions and often more lenient know-your-customer requirements in the country of location. Due to the low risk appetite of Estonian credit institutions, e-money service providers are the next choice for individuals residing in third countries.

6.2.4. Crowdfunding Service Providers

The sector's threat level is low, the **vulnerability level is below average**, and the residual risk level is below average.

The main threat is the use of Estonian crowdfunding platforms for terrorist financing due to a lack of awareness. The sector allows for the anonymous collection and transfer of funds to areas where there is no control over the end use of the funds.

Major Vulnerabilities:

- Crowdfunding is an excellent means for raising funds for terrorist purposes.
- The lack of awareness of the terrorist financing threats in the sector.

It is evident in both crowdfunding and broader fundraising⁴² platforms. Generally, global non-profit crowdfunding platforms (e.g., GoFundMe, JustGiving, Fundly, etc.) are used. These platforms do not report any indications of terrorist financing. The same applies to local crowdfunding platforms and investment firms, suggesting that awareness of potential terrorist financing risks is low and there is a lack of ability to recognize them.

- There is a high possibility that funds collected through the abuse of investor or donor trust are used for terrorist purposes. Cases from foreign countries show that funds have been raised through crowdfunding platforms for both Islamist extremists and violent right-wing extremists.
- The possibilities for identifying donors and recipients of funds are limited.

Factors mitigating vulnerability:

- The number of individuals in Estonia who might want to support terrorist financing is small.

⁴¹ The list of e-money institutions and their service resellers can be found on the Financial Supervision Authority's website: www.fi.ee

⁴² Crowdfunding vs. broader fundraising: other forms of financing (fundraising).

6.2.5. Other Sectors

6.2.5.1. Company service providers

Company service providers have not been analyzed in detail, but the sector deserves special mention by the working group as gatekeepers who play an important role in mitigating risks.

It is also worth noting that the services of company service providers, which include company formation, are naturally risky from both a money laundering and terrorist financing perspective. Often, these services are primarily targeted at foreigners in Estonia, and a large part of the sector establishes business relationships and provides services without physically meeting the client, which increases the levels of risks associated with anonymity. **Company service providers may be exploited, especially through e-residency, to establish legal entities for terrorist financing purposes** (see also case study 3). The sector's vulnerabilities may include: low awareness among market participants; inadequate application of due diligence measures, deficiencies in identifying the beneficial owner and the origin of funds, shortcomings in risk assessments and procedural rules (see also deficiencies identified in control procedures)⁴³. Inadequate fulfillment of reporting obligations – the sector has submitted only a few reports⁴⁴ indicating terrorist financing. There is also no official umbrella organization to help coordinate the sector's activities. Although the state has a clear overview of the sector (see also the NRA 2025 money laundering risk assessment), there are shortcomings related to the prevention of terrorist financing. It is likely that this shortcoming affects the national risk picture.

6.2.5.2. The e-residency program

The possible motive for extremists or terrorists to engage in business in Estonia through e-residency is to move their economic activities out of the supervision and jurisdiction of their home country's security agencies. The possible motive for radicalized individuals and terrorists to apply for e-residency is not so much to benefit from the digital state's e-services for promoting legal business, but rather to test the benefits associated with the program. For example, they want to test new financing channels and the expectation of simplified entry into the European Union or to create a legal basis for staying in the European Union. Existing knowledge confirms that if the expectations set before obtaining e-residency status are generally not met, then real business activities in Estonia are not started.

During the observation period, at least 26 individuals associated with Islamist terrorism or extremism were identified in connection with e-residency. Retrospective identification continues to this day. From the perspective of terrorist financing, the following issues related to e-residency were identified in the years 2020–2024:

- It is problematic to obtain verified information about e-residency applicants from countries with which Estonia lacks effective judicial, law enforcement, and security cooperation. This is an ongoing problem, and there are plans to restrict the issuance of e-residency to citizens of such countries.
- At the beginning of the period (2020), there was a combination where e-residents from countries with a higher risk of terrorist financing applied for VASP licenses, and there were serious deficiencies in the fulfillment of know-your-customer (KYC) principles. This was accompanied by risks of terrorist financing. These risks have now been largely mitigated.

⁴³ NRA 2025 money laundering report.

⁴⁴ During the observation period, the sector submitted four reports indicating potential terrorist financing, all in 2024. However, none of these reports were substantively qualified as indicating terrorist financing.

- At the beginning of the period, the overview and follow-up on the actual business activities of e-residents were inadequate. By 2024, the situation had improved as general follow-up on e-residents and their business activities had been enhanced.
- E-residents from countries with a higher risk of terrorist financing had developed the understanding that e-residency also allows easier access to the EU. This perception was indirectly supported by endorsement letters from the Startup Committee. Establishing a company in Estonia provides an indirect basis for obtaining a Schengen visa, which can facilitate visa acquisition if a credible background is established. Therefore, there are cases where individuals applying for e-residency attempt, either knowingly or unknowingly, to use e-residency to gain benefits that e-residency does not directly provide (e.g., the right to reside or enter Estonia or the European Union).
- Applying for e-residency allows for testing how capable an EU member state is at identifying individuals who pose a security threat. If someone's e-residency application is denied with a reference to the threat they pose, the individual receives feedback that their background is known to Estonia.

Annexes

Annex 1. Main typologies of terrorist financing

- **A radicalized individual with ties to a high-risk country** and/or a former fighter with terrorist connections **conducts virtual currency transactions within the Estonian jurisdiction through a correspondent relationship** while residing in another European country.

This means that the person conducting the transaction may not be aware of the Estonian party and may have chosen a platform provider outside the EU, possibly due to lower due diligence measures. In such cases, the background of the identified person is based on public sources.

- **Transactions in small amounts**, hiding the true purpose of the support, under the guise of a social aid or community movement or **a civic initiative** fundraising campaign.
- Collecting donations through **crowdfunding to support a conflict area**, especially during the Hamas-Israel war for the benefit of civilians in the Gaza.

The territory is controlled by a terrorist organization, and well-meaning donors cannot verify who the end user of the funds is. The main risk is that the funds sent by donors end up with the terrorist organization instead of civilians (including extortion, robbery).

- Transferring funds via **cash couriers**.

There is no obligation to declare cash within the Schengen area. At the external border, the declaration threshold is avoided, or attempts are made to transport money in a concealed manner.

Annex 2. Case Studies

CASE STUDY 1: Young people linked to the violent far-right extremist movement Feuerkrieg Division (FKD)

Young individuals radicalized online were engaged in promoting white racial supremacy in Estonia and elsewhere in the world. Through online communication platforms and posters, they incited hatred against immigrants, Jews, people of color, sexual minorities, journalists, and police officers. In addition, based on the ideology of the accelerationist group, they spread hostility toward state authority as a whole. The criminal case did not establish terrorist financing; the youths were supported by their parents, who were unaware of their children's activities.

CASE STUDY 2: Attempts to send funds to Gaza (various cases)

In 2023, several individuals, in connection with the HAMAS-Israel war, sought to send money through the Estonian jurisdiction to both private persons and organizations in the Gaza Strip on humanitarian grounds. Most supporters were foreign nationals, but there were also e-residents and Estonian citizens. Among the organizations, Gaza Now propaganda channels with links to HAMAS were identified. Pending transactions noticed by credit institutions were halted. In clarifying completed transactions and involved parties, legal cooperation was carried out within Estonia with the Internal Security Service and the FIU, as well as with foreign partners. The e-residency statuses of the related individuals were revoked.

CASE STUDY 3: Individuals with extremist links identified among e-residents

In 2021, a case was detected where two individuals, as e-residents, established a company in Estonia offering a streaming service. The service consisted of providing music on a self-created streaming platform whose ideological message aligned with violent far-right extremism. The individuals were associated with the Nordic Resistance Movement (NRM). At the European Union level, NRM is not listed among terrorist organizations; however, it has been designated as terrorist by the United States, and its activities have been banned in Finland. The organization operates mainly in Sweden, but also in Norway and Denmark. The e-residency status of the individuals was revoked.

CASE STUDY 4: Short-term workers suspected of links to ISIS-K

In 2022, individuals from Central Asia arrived in Estonia for short-term employment, and connections to ISIS-K were identified. Their employment inevitably involved a financial component, i.e., payment of wages and subsequent use of those funds. Foreign workers from Central Asia typically send part of their salary back to their home country. In this case, terrorist financing was not detected. All foreign workers involved in this case have since left Estonia.

CASE STUDY 5: Attempt by a network linked to the terrorist organization Palestinian Islamic Jihad to move virtual assets via an Estonian service provider

In 2023, individuals who had previously conducted transactions on other platforms with the terrorist organization Palestinian Islamic Jihad sought to deposit funds with an Estonian virtual asset service provider. The network consisted of 18 members and was identified thanks to due diligence measures applied by the service provider.

The Estonian-licensed virtual asset service provider had, through a correspondent relationship, a legal entity client located in another jurisdiction, which in turn had individual clients (so-called end clients) also based abroad. These individuals had previously sent funds on other platforms to various crypto addresses belonging to the terrorist organization. In addition, they had received funds from terrorist organizations, which directly indicates acting in the interests of the organization. The transaction amounts were very large from a terrorist financing perspective: in the hundreds of thousands of euros. Subsequently, members of the network attempted to make transactions through the Estonian jurisdiction by depositing small amounts of funds. The funds located in Estonia were frozen, totaling €8,205 (8,963 USDT, the cryptocurrency Tether).

CASE STUDY 6: Opening of a VIBAN account for a foreign national convicted of terrorist financing

In 2022, a virtual IBAN account (VIBAN) was opened within the Estonian financial system under a correspondent relationship for a foreign national. The individual had been convicted of terrorist financing in another jurisdiction and was serving a prison sentence there. They had attempted to join fighters in Chechnya, sent funds to support fighters in Syria, and tried to purchase materials for making an explosive device. The person's background was identified before any payments were made through the Estonian financial system.

Annex 3. Guidance for Sectors

Competent authorities will prepare a separate action plan to address the conclusions of this risk assessment report. Below are some examples of measures that sectors can implement to mitigate risks:

- **When establishing correspondent relationships**, ensure in practice that the client applies due diligence measures (with data available when needed) that comply with Estonian jurisdiction requirements. Attention should also be paid to the client's area of activity to determine whether they require a license to provide services and, if so, in which jurisdiction it was issued. From a terrorist financing perspective, extreme caution should be exercised with foreign service providers that use nesting services via an Estonian company to enter the EU market or are registered and operate in **offshore jurisdictions**. It is important that the Estonian service provider assesses the organizational solution and effectiveness of terrorist financing prevention measures applied by its respondent institution.
- **When identifying transactions indicative of terrorist financing**, the updated **guidance** from the FIU on suspicious transaction indicators and its annex—the **list of countries with higher terrorist financing risk** (so-called risk countries)—is helpful. However, the indicators in the guidance are not an exhaustive list but rather a supporting material. Therefore, monitoring terrorist financing **trends**⁴⁵ is necessary.
- **For the financial sector and VASPs**, it is critical that Estonian service providers have **procedural and technological solutions and tools appropriate to their risks and transaction volumes, both for blockchain analysis and for using public sources**.
- Tools should also include **monitoring scenarios** that, in addition to guidance indicators, take into account the **specific sector and service provider's threats and vulnerabilities**, trends, and typologies.
- **Market participants should identify virtual asset transaction initiators** based on a valid identity document and periodically verify their contact details. In addition to documents, **communication data** (all email addresses and phone numbers) and **social media** accounts used should also be recorded as contact information.
- Encourage and enable employee specialization in terrorist financing prevention as a specific field distinct from anti-money laundering.

⁴⁵ Useful reports are published, in addition to the annual reports, guidelines, and studies of the Financial Intelligence Unit, the Financial Supervision Authority, and the Internal Security Service, by the following organizations among others: FATF, RUSI, Project CRAFT, EUROPOL, EGMONT, Global Terrorism Index, International Centre for Counter-Terrorism, UNOCT, UNODC, UNCTED.



REPUBLIC OF ESTONIA
MINISTRY OF FINANCE