

---

## 8. Vulnerability of the NPO's sector

---

### 8.1. General description of the sector

#### **Specificity of the sector**

The non-profit sector in Estonia consists of non-profit associations (NPOs) and foundations (Fs) entered in the commercial register and unregistered partnerships operating under the Law of Obligations Act. The last decade has also been characterized by unregistered activities, e.g., as social media groups, which, like partnerships, can raise money for their activities, e.g., on behalf of a private person. As of 01.12.2020, 22,520 NPOs and 809 Fs (together, hereinafter also referred to as non-governmental organizations) have entered the register; the number of partnerships and other groups is unknown.

In addition to the laws on non-profit organizations and foundations, several sub-categories of non-profit associations also have their own laws, e.g., churches-congregations, artistic associations, trade unions, and other various types of associations. Thus, in addition to these 23,000 NPOs/Fs, nearly there are 24,000 apartment associations that are not included in the sector.

Non-profit associations also include political parties. There are currently 13 political parties in Estonia. The Estonian Political Parties Act defines a political party as a voluntary political association of Estonian citizens, the objective of which is to express the political interests of its members and supporters and to exercise state and local government authority. A political party is by nature a non-profit association, but for registration, it is subject to the minimum membership requirement – an association registered as a political party must have at least 500 members.

**Table 42.** Distribution by fields of activity among NPOs and Fs

| <b>Field of activity</b>   | <b>NPOs</b> | <b>Fs</b> |
|--|-------------|-----------|
| Agriculture, forestry, and fishing                                   | 721         | 1         |
| Manufacturing  | 47          | 0         |
| Electricity, gas, steam, and air conditioning supply                 | 6           | 1         |
| Water supply; sewerage, waste management and remediation activities  | 122         | 1         |
| Construction   | 126         | 3         |
| Wholesale and retail trade; repair of motor vehicles and motorcycles | 130         | 3         |
| Transportation and storage   | 96          | 7         |
| Accommodation and food service activities                            | 88          | 8         |
| Information and communication  | 374         | 30        |
| Financial and insurance activities                                   | 22          | 14        |
| Real estate activities   | 1252        | 28        |
| Professional, scientific, and technical activities                   | 786         | 55        |
| Administrative and support service activities                        | 329         | 18        |
| Public administration and defence; compulsory social security        | 168         | 1         |
| Education  | 2094        | 99        |
| Human health and social work activities                              | 906         | 115       |
| Arts, entertainment, and recreation                                  | 7666        | 160       |
| Other service activities   | 7570        | 265       |

|   |              |            |
|---|--------------|------------|
| Activities of households as employers; undifferentiated goods and services-producing for households own use | 1            | 0          |
| activities not defined  | 16           | 0          |
| <b>Total</b>  | <b>22520</b> | <b>809</b> |

The largest sectoral groups among NPOs are various sports-related associations (over 3,000), recreational providers (around 2,500), cultural and educational associations (over 2,000 each), and promoters of regional and local life (around 2,000).

The main accountability of NPOs to the state is the annual report, which must be submitted within six months as of the end of the financial year and is similar in structure to the report submitted by companies. Foundations with a sales revenue or income or total assets of more than 15,000 euros also have an obligation to review the annual accounts by a sworn auditor.

As of 01.12.2020, the list of charitable non-profit associations, foundations, and religious associations benefiting from income tax incentives maintained by the Tax and Customs Board (TCB),<sup>1</sup> contains 2554 associations, of which the largest groups are sports associations and religious associations (the latter in Estonia are approximately 700 in total). The TCB does not exercise significant control over those on the list. Non-profit associations, foundations, and religious associations included in the list of income tax incentives are required to report gifts, donations, and other income received in a calendar year in monetary value together with the method of use and to submit data thereon to the TCB on form INF 9.<sup>1</sup> The form must be submitted by the first of July even if no donations have been made or no income or expenses occurred during the last calendar year. By the first of February, the members of the list may (but do not have to) submit to the TCB on form INF 4 the known personal identification or registry codes of domestic donors and the amounts donated. There is no information on anonymous and foreign donations, as no tax relief is obtained from them.

Almost every sector has its own umbrella organizations or networks. For example, most umbrella organizations operating in the public interest are united by the Network of Estonian Nonprofit Organizations, the umbrella organization of sports associations is the Estonian Olympic Committee, religious organizations are concentrated in the Estonian Council of Churches, the Estonian Roundtable for Development Cooperation is active in the field of humanitarian aid and development cooperation. The sector has established a self-regulatory code of ethics<sup>2</sup> and described good practices in fundraising<sup>1</sup>. Neither document addresses the issues of prevention of money laundering and terrorist financing, but they do help to shape honest and ethical activities.

Although the total turnover of the sector is reported to be 600-700 million per year and the declared donations over 40 million per year, most of the associations are small organizations, e.g., less than one-fifth have employees on salary. About the same number of associations get public subsidies, and donations are stably declared by 1,300-1,400 associations. It can be concluded that, on average, the number of active civil society organizations is within a few thousand.

According to Estonian law, from the year 2012 the non-profit associations are obliged entities under the regulation of prevention of money laundering and terrorist financing, if they are paid or they pay over 5,000 euros in cash or an equivalent sum in another currency, regardless of whether it is paid in a lump sum or by way of several linked payments over a period of up to one year. However, there is no reliable data on the use of cash in the sector.

As the data sources of the sector and the classification characteristics of associations do not meet the needs of risk assessment, the sub-sectors of the target group have been further defined by combined criteria based on risk typology. Non-governmental organizations active in the fields of sports, culture,

<sup>1</sup> <https://www.emta.ee/eng/business-client/registration-business/association-list-associations-benefiting-income-tax-incentives>

<sup>2</sup> <https://www.terveilm.ee/leht/umarlaud/liikmed>

and education, and charities, or that are religious associations were included in the sample.

In addition, it is important to note that the survey conducted in the sector was forwarded according to the sample to a total of 2300 representatives. The response rate was significantly high in the whole sector (across the three sub-sectors), with the exception of charities.

**Table 43.** Data from a survey conducted in the NPO's sector.

| Subsector   | Number of market participants | Sample size | Sample size/number of responses required | Number of invitations sent out | Number of responses received | Response rate |
|---|-------------------------------|-------------|--|--------------------------------|------------------------------|---------------|
| Sport: Classification of Economic Activities (CEA code) 9311, 93121 | 1865                          | sample      | 319                                      | 798                            | 337                          | 105%          |
| Religious associations: CEA 94911, 94919                            | 625                           | sample      | 238                                      | 625                            | 276                          | 116%          |
| Culture and education: CEA 9499, 94995, 94991, 94994                | 2396                          | sample      | 331                                      | 828                            | 344                          | 104%          |
| Charities   | 49                            | all         | 44                                       | 49                             | 20                           | 45%           |

One of the preliminary questions of the survey was whether during the last year the NPO/F has settled with its client/supplier/member/donor/donation recipient or another transaction partner in a payment lump sum or aggregated over several payments more than EUR 5,000 in cash or an equivalent sum in another currency. The results of the survey showed that we were able to speak to a very small proportion of obliged entities: in the case of the sampled target group, the answer was yes: only one respondent in the charity sector, 9 in the culture sector, 6 in the sports sector and 10 in religious associations. In total, 26 out of 977 respondents answered in the affirmative to the first preliminary question about cash settlement, which is less than 3% of the respondents.

According to FATF Recommendation No. 8, obliged entities are also those who primarily engage in raising or distributing funds for purposes such as charitable, religious, cultural, educational, social, or fraternal purposes, as well as the carrying out of other “good works” In Estonia, therefore, companies with income tax benefits would primarily comply with the FATF recommendation, but not all NPOs that meet the description are included in the list of the TCB. There is also no precise information on, for example, those operating in high-risk countries or near an active terrorist threat, but most of the associations in the respective field are concentrated in the Estonian Roundtable for Development Cooperation<sup>3</sup> or receives support from the Ministry of Foreign Affairs<sup>4</sup>. To gain additional information, we compiled another preliminary question for the target group questionnaire: “Has your NPO/Fs carried out transactions with foreign countries during the last five years, or have you received funds from foreign countries?”

The associations that had business with foreign countries in the last five years were divided as follows: charity 6, culture/education 48, sports 60, religious associations 100. It turned out that more than 50% of respondents from religious associations performed transactions with foreign countries.

<sup>3</sup> <https://www.terveilm.ee/leht/umarlaud/liikmed>

<sup>4</sup> <https://akta.mfa.ee/index.php?language=eng>

### **Legal framework**

Legal persons are divided into legal persons in public law and legal persons in private law (§ 24 of the General Part of the Civil Code Act). Legal persons in private law have been founded in private interests and in accordance with the Act of Parliament concerning the corresponding type of legal person (§ 25 (1) of the General Part of the Civil Code Act). According to Estonian law, a non-profit association is a legal person. Examples of different types of NPOs are apartment associations, land improvement associations, political parties, building associations, churches, and congregations.

The establishment and dissolution of a non-profit association, membership, entry in the register, and management are regulated by the Non-profit Associations Act (NPAA). The passive legal capacity of a non-profit association commences as of the entry of the NPO in the non-profit associations and foundations register and terminates as of deletion from the register (§ 2 of the NPAA). The highest body of the NPO is the general meeting of its members (§ 18 (1) of the NPAA). The NPO must have a management board. The management board represents and manages the NPO (§ 26 (1) of the NPAA). Every member of the management board has the right to represent the NPO in concluding all transactions unless otherwise provided by the articles of association or law (§ 27 of the NPOA). The management board and the specifications of the right of representation of the management board shall be entered in the register (§ 10 (1) 5) of the NPOA).

Members of the management board who cause damage to the NPO by violation of their obligations are solidarily liable for compensation for the damage caused. A member of the management board is released from liability if he or she proves that he or she has performed his or her obligations with the due diligence normally expected from a member of the management board (§ 32 (2) of the NPAA). Non-profit organizations also include religious associations, the activities of which are regulated not only by the NPAA but also by the Churches and Congregations Act as a specific law. The area of prevention of money laundering and terrorist financing is regulated by the Money Laundering and Terrorist Financing Prevention Act (MLTFPA).

Specific laws do not prescribe any additional rules or requirements for NGOs. Thus, it can be said that the specific laws applicable to NPOs and their different types generally do not take into account the risks of money laundering or terrorist financing. § 2 (3) of the MLTFPA names non-governmental associations as obliged entities of the MLTFPA.

NPOs are generally obliged entities within the meaning of MLTFPA. Due diligence measures arising from the MLTFPA must be followed by NPOs due to the nature of the specific transactions in which they participate (cash transactions).

A special procedure for the application of due diligence measures is prescribed for non-profit associations that are obliged entities (§ 29 of the MLTFPA): the due diligence measures specified in clauses 20 (1) 1) -5) of the MLTFPA apply. The due diligence procedure applies to NGOs if they exceed the statutory limits in their activities, i.e., if they are paid, or they pay in cash over EUR 5,000 in installment, lump sum, or by way of several linked payments over a period of up to one year. Application of the due diligence measures for the NGO mainly means paying increased attention to the identification of transaction partners and reporting to the FIU in case of suspicion. An NGO that is an obliged entity must register and store information about the conclusion of transactions (§ 46 of the MLTFPA).

NPOs must publish and keep up-to-date information on their beneficial owners in a dedicated register. This requirement applies to all NPOs regardless of the amount of their cash flow (§ 77 (2) of the MLTFPA). NPO that is an obliged entity must register the information on the operations made for the purpose of establishing the identity of the beneficial owner (§ 46).

### **Responsibility**

Misdemeanor liability is prescribed for violation of the obligations provided in the MLTFPA. In the

case of a legal person, a fine of up to 400,000 euros is prescribed as a penalty for violation of the obligation. In the case of legal persons, including NPOs, a high-level representative of the legal person, i.e., a member of the management board, is held liable as the perpetrator of the misdemeanor. It is also possible to sanction a legal person criminally for committing a money laundering offense. Money laundering offenses are money laundering (§ 394 of the Penal Code) and money laundering agreement (§ 394<sup>1</sup> of the Penal Code). Punishable is the financing and support of acts of terrorism and activities directed at it (§ 237<sup>3</sup> of the Penal Code), organizing, funding, and supporting travel for terrorist purposes (§ 237<sup>6</sup> of the Penal Code). A court may impose a pecuniary punishment on a legal person.

## 8.2. Description of risk typologies

### **General typology**

Use of the sector for terrorist financing or money laundering without the sector's own knowledge, taking advantage of the sector's low awareness.

### **Case typologies**

- Collection and subsequent distribution of assets by persons operating in the sector in a way that does not make it possible to identify the origin or destination of the assets, including sending assets abroad and also collecting assets from abroad.  
For example, the classic collection of donations- alms (zakaat), one of the five pillars of Islam: the obligation to donate 2.5% of one's annual income to the poor. Traditionally, the local religious leader (imam) identifies those most in need. The imam allocates a certain amount of the funds collected by the congregation as donations to the person in need, who in turn passes it on to a person with Islamic extremism. Typically, it can be realized through a religious association.  
For example, there is a common call to raise funds for those who lost their homes in the Beirut explosion through a local Islamic organization. Due to a lack of awareness, donors do not realize that the Islamic fundraising organization is a sub-organization of a terrorist group (such as Hezbollah).  
For example, a call to support children and women living in difficult conditions in the Al-Hol camp (Syria) (families of foreign fighters). During Friday's prayer at the Islamic Centre, it will be decided that (NPO or religious association) will support the Al-Hol camp for EUR 500, which will be sent in virtual currency to the contact person. In reality, the contact person is the person with Islamic extremist views who is responsible for recruiting new foreign fighters.
- Use of assets allocated to a person operating in the sector for personal purposes.  
For example, cases where earmarked funds for the community are used (for example, by a religious leader) to improve their standard of living.<sup>5</sup>  
For example, in case of dishonest intentions, NPOs can be exploited in the money-laundering scheme in a way where the amount illegally obtained is to be donated to a related NPO in order to start using a vehicle or real estate purchased for the money received by the NPO. Apparently, the vehicle or real estate is not the property of the user, but the property of the NPO that acquired it using donated funds received from unknown donors.

### **Background**

Due to incomplete data, it is difficult to estimate the exact number of Muslims in Estonia, which according to estimates, can range from 1,500 to 10,000 people.<sup>6,7</sup> According to the population census, the number of people belonging to the Estonian Islamic Congregation increased by approximately 100 in 11 years to 1,508 members in 2011. The continuous activity and natural growth of the Estonian Muslim community attract the interest of organizations cultivating conservative and radical Islamic (or Islamist) thought in Estonia. This can be manifested, for example, in the financial support given by some foreign and radical Islamic organizations, or in the opposite direction, where a religious

<sup>5</sup> <https://epl.delfi.ee/artikkel/81295729/eesti-peaimaam-ostis-koguduse-raha-eest-suua-basseini-ja-valivoodi?>

<sup>6</sup> <http://www.islam.pri.ee/index.php?id=66>

<sup>7</sup> [http://dspace.ut.ee/bitstream/handle/10062/63358/lepa\\_ege.pdf?sequence=1&isAllowed=y](http://dspace.ut.ee/bitstream/handle/10062/63358/lepa_ege.pdf?sequence=1&isAllowed=y)

association or non-profit organization operating in Estonia starts raising funds for a foreign legal or natural person (donation, zakat). In 2019, the Estonian Internal Security Service (ISS) identified nearly 50 persons related to extremist Islamic and terrorist organizations who arrived in or moved through Estonia. Representatives of organizations promoting fundamental Islam regularly visit Estonia, but their activities in Estonia have not achieved the desired effect. These are not internationally wanted persons. Islamic extremist terrorist organizations operating in the Syrian-Iraqi conflict zone have lost a significant part of their local sources of income, which is why funding is sought further afield. Among others, European Muslim communities and non-profit organizations are used for this purpose.

Calls to support jihadists and their families in conflict zones are mostly disseminated through social media and communication applications. With reference to anonymity, donations are also collected through payment service providers and virtual currency intermediaries.

In 2019, the FIU prepared guidelines on the characteristics of suspicious transactions, which helps obliged entities to notice suspicions and risks in the provision of services, to report them, and to take appropriate measures.<sup>8</sup> The FIU has divided the terrorist financing suspicion indicators into two: risk indicators and suspicion indicators. While risk indicators describe situations with a potential risk of terrorist financing that does not constitute a specific suspicion, suspicion indicators indicate a serious suspicion that a transaction constitutes terrorist financing, and the transaction must be postponed until the decision of a competent authority.

The guide only highlights a selection of risk indicators relevant to the sector, that is based on the persons or transactions related to the high-risk area (high-risk country).

Unusual transaction risk indicators:

- The execution of the transaction is supervised by an outsider
- Insufficient explanation regarding the origin of the money
- Insufficient knowledge of the counterparty
- The first transaction with a natural/legal person in a high-risk country
- Receipts are followed by systematic cash withdrawals and/or transfers
- The purpose of payment is not in accordance with the company's economic activity
- The transaction with a non-profit organization operating in a high-risk country
- The explanation of the international transaction contains a reference to a donation, alms, support
- What is stated in the explanation of the international transaction cannot be understood (translatable)
- The nature of international transactions refers to the collection of funds
- Bank cards associated with an account (an additional card) are simultaneously used in different countries
- Linking bank cards/accounts to international financial service platforms
- Purchase or sale of virtual currency in cash

The guide sets out transaction indicators that indicate suspicion of terrorist financing:

- The party to the transaction is associated with a terrorist organization
- According to public sources, criminal proceedings have been initiated against a party to the transaction under § 237-237<sup>6</sup> of the Penal Code.
- Public sources or a competent authority have/has referred to a party to the transaction as a person with radical views and/or who supports the activities of a terrorist organization
- What is stated in the explanation of the transaction refers to the above-listed features
- There are other indications of terrorism or terrorist financing.

<sup>8</sup> <https://www.politsei.ee/files/Rahapesu/juhendkahtlastetehingutunnustekohta.pdf?222a84e8fa>.

### 8.3. Threats

#### 8.3.1. Threat of money laundering

##### **Threat due to low-risk awareness<sup>9</sup>**

Low awareness of risks and potential threat scenarios are manifested in many cases in the sector. One of the conclusions of the survey is that the sector is not able to identify risky transactions and is not able to assess the background of the counterparty's transaction partner. Risk mitigation measures are not known or if known, are used in extremely rare cases.

The European Commission's risk assessment SNRA points out that so-called service NPOs (health care, education, housing, or social service associations) operating in the sector may be exploited for terrorist financing due to their low awareness.

In its analysis practice, the FIU has not identified any significant attempts to use Estonian NGOs for money laundering. The sector's low-risk awareness is primarily related to the threat of terrorist financing, the probability of which is more detailed in the analysis of terrorist financing threat.

The following is the statistics of reports to the FIU from other sectors concerning NGOs and suspicions of money laundering or terrorist financing related to associations from 2017 until 2019:

**Table 44.** NPOs and Fs that were mentioned in the reports to the FIU in 2017-2019 by the type of report

| Year         | CTR      | ISR      | UAR       | UTR       | STR       | TFR      | TF_UTR   | Query     | Total      |
|--------------|----------|----------|-----------|-----------|-----------|----------|----------|-----------|------------|
| 2017         |          |          | 5         | 11        | 11        |          |          | 8         | 35         |
| 2018         | 1        |          | 1         | 19        | 21        |          |          | 4         | 46         |
| 2019         | 7        |          | 16        | 9         | 18        | 1        |          | 2         | 53         |
| <b>Total</b> | <b>8</b> | <b>0</b> | <b>22</b> | <b>39</b> | <b>50</b> | <b>1</b> | <b>0</b> | <b>14</b> | <b>134</b> |

The threat of money laundering related to low-risk awareness is **low** in Estonia.

##### **The threat of non-transparency of transactions**

Due to the sector's wide range of activities, there is a threat of money laundering due to the non-transparency of transactions. In addition, there may be a threat of inadequate controls and the inability of those responsible and involved in the sector to actively monitor the background of transactions. The threat is **average** in Estonia.

##### **The threat of criminal infiltration<sup>10</sup>**

Given the number of legal entities operating in the sector and the different areas of activity, there is a probability that criminals will infiltrate the economic activities of NPOs. In Estonia, such a threat exists in the context of money laundering, but this threat is **low**.

<sup>9</sup> The SNRA also addresses the same issue: „Some types of "Service non-profit organisations" ["Services NPOs" are NPOs involved in diverse activities, such as programmes focused on providing housing, social services, education, or health care.] are more directly vulnerable due to the intrinsic nature of their activity. This is due to the fact they may involve funding to and from conflict areas or third countries identified by the Commission as presenting strategic deficiencies in their anti-money laundering/terrorist financing regimes. Non-profit organisations are vitally important for providing humanitarian assistance around the world. To safeguard the legitimate objectives of such assistance, more information about terrorist financing risks is needed within non-profit organisations to improve risk awareness“.

<sup>10</sup> The SNRA also addresses the same issue: „Risk analysis from a threat perspective is complicated by the diversity of the sector. "Expressive non-profit organisations" ["Expressive NPOs" are NPOs predominantly involved in expressive activities, which include programmes focused on sports and recreation, arts and culture, interest representation, and advocacy.] present some vulnerability because they may be infiltrated by criminal or terrorist organisations that can hide the beneficial ownership making the traceability of the collection of funds less easy

### **Threat arising from cash transactions**

The state does not have a complete overview of the volumes and nature of cash transactions in the sector. In Estonia, in general, the number of cash transactions is in decline. The results of the survey show that less than 3% of the respondents (26) state that the NPO/foundation has settled with its client/supplier/member/donor/recipient of donation or another transaction partner in one lump sum or over several payments in cash over 5,000 euros during the last year.

The threat arising from the use of cash is rather low in Estonia. However, it can be concluded from the case study of the FIU that some NPOs have not notified the FIU of transactions exceeding the cash threshold. According to the FIU's supervisory unit, non-compliance with the notification obligation is sector-wide.

### **Threat associated with professional sports**

The risks associated with sports are constantly being considered at the EU level. For example, professional football has been valued as a sport that operates as a global industry and has a significant economic impact. The complex organization of professional football and the lack of transparency have created a fertile ground for the use of illegal resources. For example, there have been cases where questionable sums of money have been invested in sports for which there is no understanding of their legal origin.

At the EU level, the threats associated with sports clubs have been consistently analyzed, and cases of misuse of the sector have been identified. In Estonia, the threat is rather low. This assessment has been issued by the FIU as a supervisory authority. In the information collected by the FIU, cash deposits to the accounts of sports associations have been noticed in very few cases, and foreign law enforcement agencies have also shown little interest in local sports clubs but no systematic use of the sports sector (including football) for money laundering and terrorist financing has been identified in Estonia.

### **Conclusion**

**Table 45.** The threat level of money laundering in the NPOs sector

| Sector | Threat level of money laundering at the sectoral level |                    |
|--------|--|--------------------|
| NPOs   | 2.0  | <b>average/low</b> |

Looking at the probability of the realization of the threat scenarios described above and relying on the information obtained from the target group through a survey and from supervisory authorities, it can be concluded that the threat of money laundering in the sector is **below average**.

## **8.3.2. Threats of terrorist financing**

### **The threat of exploiting religious associations for terrorist financing**

Religious associations are defined in Estonia by the Churches and Congregations Act, and an association must be entered in the Commercial Register. As of 01.01.2012, almost 600 religious associations have been registered in Estonia, most of which belong to associations of churches or congregations. Only NPO Estonian Muslim community (Eesti Islami Kogudus) is registered as a religious association uniting Muslims in Estonia.

The threat of financing terrorism through religious associations can be considered low due to the small size of the Estonian Muslim community (about 500 visitors to the place of worship) and the resources collected from the community as donations are mainly used for the daily subsistence and expenses of the place of worship. Islamic clergy operating in Estonia are also moderate in their views, which is why Islamic extremist views are not promoted in the community, and fundraising campaigns are not carried out.

It is more probable that the commission of a terrorist crime in a foreign country (especially in conflict hotspots) may be financed through a local religious association in Estonia. Such funding may be rather out of ignorance. For example, there may be a case where a community member comes out in a joint prayer or on social media with an emotional call to support his or her religious brother, and the background of the beneficiary is not sufficiently known. Such campaigns may take the form of anonymous cash collection at places of worship, and the money raised may be passed on through alternative payment service providers. Nor can it be ruled out that donations to Estonian religious associations may be made by religious associations from foreign countries (for example, a mosque promoting Islamic extremist views) or charitable foundations, with a request to transfer part of the money to a third party abroad.

The threat that a religious association will be used to finance (Islamic) terrorism is currently **low** in Estonia but not non-existent.

**The threat of exploiting charity organizations for terrorist financing**

The threat of charitable NGOs being used to finance (Islamic) terrorism is currently **low** in Estonia. Many charitable non-profit organizations (for example, NPO Mondo, Estonian help to refugees (Eesti Pagulasabi) NPO, etc.) operate in crisis hotspots and countries nearby, but their purpose is mainly to provide humanitarian aid within the framework of the international umbrella organizations. In addition to collecting voluntary donations, such NGO projects are also funded by state authorities (for example, the Ministry of Foreign Affairs of the Republic of Estonia). In such cases, projects are implemented in accordance with certain rules and subject to additional monitoring, which significantly reduces the risk of terrorist financing.

**The threat of exploitation of sports associations for terrorist financing**

The threat of sports connections being used to finance (Islamic) terrorism is currently **low** in Estonia. There are no such cases.

**The threat of exploitation of other NGOs for terrorist financing**

The threat of an organization operating for cultural, educational, social, or family purposes being used to finance (Islamic) terrorism is currently **low** in Estonia. There are no such cases.

**Conclusion**

Based on the expert opinions and the answers of the target group survey, it can be concluded that the threat level of terrorist financing through non-profit organizations in Estonia is **below average**.

**Table 46.** The threat level of terrorist financing in the NPOs sector.

| Sector | Threat level of terrorist financing at sectoral level |                    |
|--------|---|--------------------|
| NPOs   | 2.30  | <b>average/low</b> |

**8.4. Vulnerabilities**

**8.4.1. Vulnerabilities of prevention of money laundering**

**8.4.1.1. Exposure to threat**

The biggest vulnerability of NGOs is the lack of awareness necessary to prevent money laundering and terrorist financing, on the one hand, and the lack of a legal framework where the grounds for due diligence do not always overlap with the needs in practice: currently, NGOs are obliged entities, if the sum of cash in a single transaction is more than 5,000 EUR. Thus, the current regulation of MLTFPA does not address the risk of terrorist financing related to the NGOs.

A very small part of the sector (approximately 1.5% of respondents according to the survey) have

submitted reports to the FIU.

Vulnerabilities in the NGO sector due to the threat arising from the cash transactions are difficult to identify, but it is known that the share of cash in use is declining.

The sector is vulnerable in checking the background of transactions with foreign countries: the summary of the survey clearly showed that NPOs do not make great efforts to clarify the background of a transaction partner. At the same time, there are no special state guidelines, guidelines, nor training for NPOs that would describe, among other things, sector-specific risk indicators that indicate the unreliability of a transaction partner. The sector can follow the general guidelines of the FIU, but it would also be necessary to establish specific guidelines that take into account the vulnerability of the sector.

Exposure to the risk of criminal infiltration is rare.

#### 8.4.1.2. Risk awareness

##### **Management commitment and leadership**

###### **Survey results on awareness:**

The results of the NRA survey show that the sector's awareness of anti-money laundering is moderately low. Assessing the awareness of the sector is methodologically somewhat complicated, as there are more than 22 thousand legal entities in the sector, but it is not known which of them would be obliged entities in terms of measures to prevent money laundering and terrorist financing. There are also no official statistics, which is the share of obliged entities in the whole sector because the sector today has no obligation to inform the state about major transactions. The sector has also made very few reports to the FIU. Reasons can be traced to the sector's insufficient awareness of AML/TF measures, but on the other hand, it must be taken into account that only a certain part of the sector is the obliged entity, and this requirement has been in force for not so long time (from 2012 an amendment was made in the law according to which NPOs that have made cash transactions over 10,000 euros became obliged entities, and from 2017 the limit was reduced to 5,000 euros).

Based on expert opinions, the target group of the survey was the riskiest sub-sectors, which were sports, charity, religious associations, and culture/education. The response rate was very high in the sector, which shows the sector's commitment and good ability to cooperate. A total of 977 responses were received to the survey, which was sent to 2,300 NGOs in the sector, of which 20 were from the sub-categories of charity, 344 from culture and education, 337 from sports, and 276 from religious sub-categories.

###### **The following main conclusions** can be summarized:

- 35.79% of respondents (35) indicated that the awareness of the problem in society should be increased. It can be concluded that a lack of information could be considered as a major factor in the associations' low awareness on the topic of the prevention of money laundering and terrorist financing. It can be concluded that more effective informing and guidance is a key to improve compliance with the legislation and standards in this area.
- 26.6% of the respondents perform a background check when recruiting employees. Charitable organizations stood out, where 45% of the respondents perform a background check. The background control measures used by NPOs can be divided into 12 types. There was no dominant method, but the most popular were Google, social media, interviews, and aptitude tests.
- A total of 226 NPOs answered the question, "Has your organization taken steps to make employees aware of their money laundering obligations?" 17.3% answered in the affirmative. The result was lower than average in NPOs engaged in sports (less than 10%, elsewhere about 20%). The requirements are mainly introduced, explained, and people are made aware of the requirements, employees and transactions are checked, and training is attended. However, a large number of NPOs did not provide an answer to this question.
- The feedback from all four questionnaires (charity, culture and education, sport, religious

associations) is summarized by the fact that all answers to the questions, which largely concerned the identification of higher risk transactions, indicate that respondents have generally not answered questions in a substantive manner or have not answered questions at all, which makes it difficult to compile an analysis based on this data. In most areas, there is a lack of individuals who deal only with the prevention of money laundering and terrorist financing, and it is regarded as a shared responsibility in the framework of other tasks.

- Individuals who have not fulfilled the obligation to notify argue that the need to submit a notification has not emerged.
- The low level of notifications can also be caused by the fact that only a small proportion of NPOs have been exposed to higher risk activities and are unable to answer whether specific measures are used to identify risks (charity (1), culture, and education (7), sport (2), religious associations (8). Of the few who have referred to the need for mitigation in higher-risk cases, the most important solutions have been Internet databases and, in some cases, requesting customer data.
- In wider terms, it can be concluded that only a few associations in the sector check the lists of sanctions to reduce the suspicion of terrorist financing. The number of respondents who take into account possible threat scenarios when preventing terrorist financing is also below 10%. Most respondents do not feel involved - do not have exposure, or do not consider it. The overarching feature is the lack of assessment of the terrorist financing risks associated with the sector - the majority (over 90% throughout) answered that they do not conduct background checks. When risks are assessed, it is mainly through the application of the “know your customer” principle. However, it remains unclear what procedures are conducted to implement this principle.
- Most donations not made by a member of the association have been received by religious associations – 70% are those, who do not or rather do not see the need for additional checks in such cases.
- NPOs do not check the background of the other party (the recipient of the donation) in the case of disbursements made by themselves (risks adjacent to those described in the SNRA).
- Alternative payment services are most used by religious associations. More than 50% of respondents answered affirmatively about their use. Other subsectors tend not to use this service. First, the religious association’s sector uses donation boxes; to some extent, the sector also uses the Transferwise service. For these transactions, the background of the transaction partner is not checked.

#### **Brief summary**

The sector survey revealed that the respondents were not able to answer the questions related to the awareness of money laundering and terrorist financing, measures or the identification of risky transactions<sup>11</sup>.

### **8.4.1.3. Legal framework and control**

#### **Quality of supervision**

The control measures for the prevention of money laundering in the NPOs sector mainly consist of two aspects, the level of regulations and the adequacy/inadequacy of supervision.

The supervisory authority of non-governmental organizations in monitoring the requirements of MLTFPA is the Financial Intelligence Unit. The FIU follows a risk-based approach to supervision, in the course of which:

- the risks associated with the sector,
- the risks associated with transactions and activities carried out by the sectors,
- the risks of potential transaction partners in the sector and the risks of the sector arising from the information known to the FIU are assessed.

<sup>11</sup> The questionnaire was divided into questions on maintenance and supervision related and general questions; the questions in the first category were asked only from the obliged entities, who became clear by answering the preliminary questions). Thus, due diligence questions were asked from only a small number of the target group of the survey, and many other questions may have remained strange to the rest of the sector.

In addition, the FIU assesses the conclusions and summaries that emerged as a result of the analyses prepared. Due to the risks of money laundering and terrorist financing related to NPOs, as well as the risk assessment performed internally by the supervisory authority, the FIU supervised non-profit organizations in 2016. In all proceedings initiated at that time, it was established that since the NPOs selected as subjects had not carried out such cash transactions that would have made them subject to the MLTFPA, the proceedings were terminated due to the fact that the selected NPOs were not viable subjects. Later, due to the application of the risk-based supervisory system, there is no presumption of performing supervision in terms of NPOs.

The MLTFPA regulate the designation of NPOs as obliged entities only in the case of cash transactions over 5,000 euros. Defining obliged entities on the basis of threshold-based cash transactions does not adequately address the risks associated with NPOs, in particular the risk of terrorist financing.

In order to increase efficiency in this situation, a declaration obligation should be created by which NPOs that make or agree to make transactions that would make them obliged entities must register themselves so that the state has knowledge of potential risks and the supervisory authority would be able to perform risk-based supervision.

#### **Brief summary**

- ✓ The supervisory authority FIU and the representative organization Network of Estonian Non-profit Organizations should intensify cooperation in order to significantly raise the awareness of the sector through training, information days, and guidance materials.
- ✓ An obligation to register/declare should be introduced for NGOs that enter or agree to enter into transactions that make them obliged entities so that the supervisory authority can identify obliged entities and better plan and apply risk-based supervision.
- ✓ Where possible, consideration should be given to supplementing the Guidelines on the Prevention of Money Laundering and Terrorist Financing so that NPOs can and should take into account criteria concerning risk areas when sending or receiving assets in order to take the necessary mitigation measures.

#### **Effectiveness of compliance control systems and reporting**

All NPOs in Estonia are subject to accounting reporting obligations. With regard to donations and grants that receive more attention in the case of NPOs, separate disclosure is provided in the annual report, which presents the recipients and donors of donations and grants. There is no obligation to audit, which means that submitted data is not systematically verified.

Based on the analysis of the document, NPOs are recommended to prepare risk analyses before operating in a new environment or cooperating with new partners. It is also recommended to implement a corporate governance code, effective financial management, and the implementation of internal and external controls.

The results of the survey confirm that Estonian NPOs and Fs have little exposure to a large amount of cash and also have few or no employees. Therefore, most NPOs and Fs do not have the means to procure IT tools for risk management. It can also be considered an investment if an employee is assigned the task of implementing the prevention of money laundering. More than half of the respondents had not appointed an obliged person. About a third answered that a member or members of the board had been appointed as obliged persons. Only 1% of the respondents had appointed a staff member in charge, and some also mentioned an accountant, partner, lawyer, or auditor. Almost exclusively, the obliged person had other responsibilities in addition to those related to risk management.

Questions about politically exposed persons (PEPs) were asked only from those respondents who have made large cash transactions in the last year or who have had transactions with foreign countries,

or have received funds from foreign countries in the last five years. Only four of them replied that they use sources of information to identify politically exposed persons. In the NPOs sector, almost no one checks whether the other party to a contract or transaction is a PEP.

NPOs and Fs rely heavily on the activities of the financial sector in preventing money laundering. In case of larger amounts of cash, the NPO or the Fs itself must implement due diligence measures. The results of the survey show that few NPOs and Fs are exposed to large amounts of cash. About 3% of the respondents answered that they have settled with a transaction partner in the last year in one lump sum or in several related payments in the total amount of 5000 euros or more. However, if an NPO or Fs is exposed to a large amount of cash in a transaction, given the relatively low awareness of money laundering, the NPO or Fs may not always have the ability to identify a complex or unusual transaction. However, these are rather exceptional situations.

The survey's target group was asked some questions regarding the existence of complex and unusual transaction mechanisms. For example, it was asked whether the NPOs that carried out the transaction with alternative payment sources check the background of the transaction partner separately. It was also asked whether and how the NPO checks the background of the recipient of the donation in the case of disbursements made by the NPO itself and whether the NPO carries out additional checks on receipts from public sources from NPO members (membership fees, donations, etc.). In addition to sector-specific questions, the existence of complex transaction mechanisms was also addressed in the Terrorist Finance Prevention Questionnaire (question: does your organization assess the risks of terrorist financing during customer background checks?). And it was also investigated what methods the NPO uses to identify the origin, purpose, and beneficial owners of funds in higher-risk cases? Overall, the design of the mechanisms and awareness of these measures was rather low. The NPOs participating in the survey do not check the background of the other party (recipient of the donation) in the case of disbursements made by them (adjacent risks as described in the SNRA) and do not perform additional checks to find out the background of the counterparty's transaction partner.

### **Brief summary**

So far, NPOs and Fs in Estonia have not made many preventive efforts, which would allow them to improve the identification of higher-risk situations. This is partly due to low awareness, partly due to limited resources, and the fact that there is no exposure to large amounts of cash.

### **Quality of the framework of due diligence measures applied to the customer**

#### **General description of the due diligence measures**

According to MLTFPA, NPOs and Fs must implement due diligence measures in cases where they are obliged entities within the meaning of MLTFPA or have a suspicion of terrorism or money laundering. There are no exceptions for this sector compared to the traditional package of due diligence measures. The implementation of due diligence measures may be difficult in the sector due to some factors. Many organizations in the sector are value-based, with higher than usual levels of trust, which in turn means a lower level of internal control. Long logistical chains and often changing volunteer staff mean less control over the use of an organization's resources.

#### **Vulnerabilities identified in the survey on the quality of the customer control framework**

- Of those respondents who are obligated under the MLTFPA and/or who had transactions with foreign countries, only 8% answered that they use measures to identify the origin, purpose, and actual beneficiaries of funds in higher-risk cases. 23% could not answer this question, which indicates low awareness. At the same time, it should be taken into account, that the majority of the respondents did not expose to such an amount of cash that would make him or her an obliged entity within the meaning of MLTFPA.
- Almost exclusively, in high-risk situations, an Internet search was used to obtain additional information. More than half of the respondents who used this method considered it to be effective enough.
- 78% of the respondents could not assess whether the information on the beneficial owners in the national register is reliable. Most were also unable to assess the availability of the relevant

information. Two respondents thought that the information was chargeable, but this was not true. However, those who could evaluate considered the information to be reliable and easily accessible. There were also those respondents who considered the data available but did not answer that they considered the data reliable.

- In general, the respondents could not assess the reliability of Estonian information systems and the adequacy of data, but those who did know responded that information systems were rather thorough and reliable.
- About a quarter of the obligated respondents (about half of the religious associations) use the services of alternative payment service providers, which may make it more difficult to perform customer due diligence.
- As so few obliged entities identify politically exposed persons, it is not possible to assess whether information on politically exposed persons is easily available from the point of view of NPOs and Fs.
- NPOs and Fs are rather small in Estonia, but as Estonia is a small country/market and open economy, more than a third of the respondents had made cross-border transactions, especially with EU countries. Cross-border transactions generally require higher awareness to identify situations where the application of due diligence measures is required, especially when using cash or alternative payment services.

#### **Brief summary**

The sector's awareness and ability to exercise control over transaction partners are rather low. There are deficiencies in almost all aspects of customer control.

#### **8.4.1.4. Sector-specific risk assessment with the quality of sector-specific controls**

The following vulnerabilities have been identified in the analysis and assessment of sector-specific risks:

##### **1. Vulnerability due to the structure of the legal framework:**

- Based on the summary of surveys, expert assessments, and information obtained from supervision, it can be concluded that the current legal solution, where the NPO is subject to the obligation to implement due diligence measures only in cases where the NPO makes transactions in the amount of 5,000 euros, does not seem to be effective. It is rather a formal requirement, which in practice creates a situation where the state has no information about what is happening in the sector. The number of notifications to the FIU is modest, and, based on expert opinion, it is not in balance with the size of the sector.
- It is necessary to analyze whether it would be beneficial for the sector to impose an obligation to declare transactions. It would also be appropriate to analyze the need to change the basis for the application of the principles on the prevention of money laundering and terrorist financing in order to mitigate potential terrorist financing risks.

##### **2. Vulnerability regarding the performance of supervision:**

- Based on the previous segment, vulnerability also exists in the difficulty of supervision. Accordingly, among other things, the need for a different allocation of resources (identification of obliged entities) should be considered.

##### **3. Vulnerability in terms of transactions related to high-risk areas:**

- One of the main vulnerabilities in the sector is the low awareness of the sector in clarifying the background of transaction partners, with the aim of avoiding undesirable transactions. This vulnerability highlights the low national focus on areas with a higher risk of money laundering - the lack of guidelines and recommendations for conduct in the sector.

##### **4. Vulnerability in terms of resource constraints:**

- So far the anti-money laundering supervisory authorities and relevant policy-makers have not had enough resources to make the necessary commitment to the sector. There is certainly a need for more information about the sector for supervising and policy-making.

**The main vulnerabilities in the sector stem from:**

- ✓ low awareness of the sector;
- ✓ the structure of the legal framework;
- ✓ the complexity of supervision and the lack of resources dedicated to the sector.

**8.4.1.5. Quality of the response to risks identified in previous evaluations**

The results of the NRA 2015 showed that over the past assessment period the level of vulnerability of the sector in the prevention of money laundering and terrorist financing was generally low on average.

The NRA 2015 report classified sources of terrorist financing as legal and illegal. Terrorist financing from legal sources was considered unlikely in Estonia, and the probability was assessed as low. However, the risk of committing crimes for terrorist financing has been assessed as average. The connection of the non-profit sector with conflict areas has also been considered as a separate indicator in the 2015 risk assessment. With regard to the latter indicator, it is noted that there are organizations in the local Muslim community that are actively in contact with countries that have high international terrorism risk and with organizations located in those countries, which is why this indicator has also been given an average as a rating.

However, general and reliable data on the use of cash was found at that time. This shortcoming has not been remedied.

It was also noted in 2015 that NPOs have no contact with international clients and transactions, which is why this indicator was assessed as low at that time. In 2020, NPOs had also exposure to cross-border transactions. Based on the survey the number of associations by sector that had transactions with foreign countries in the last five years was as follows: charity 6, culture/education 48, sports 60, religious associations 100. More than 50% of the respondents of religious associations made transactions with foreign countries. Based on the document analysis done on the SNRA report, we see that the reference to foreign countries is important.

Of the foreign countries with which transactions were made, there were countries both from inside and outside the European Union – for example, a significant number of transactions in the sports sector were made with Russia (12%). It is particularly striking that religious associations have carried out most foreign transactions with the Finnish state.

In 2015, the level of regulation was assessed as average; in practice, this meant that a large number of NPOs that potentially make transactions with large amounts of cash (for example, 5,000 - 10,000) are still excluded from the circle of obliged entities. The level of regulations was thus satisfactory only for an insignificant part of the NPOs, which is why this indicator is assessed with the grade average.

It was also found in 2015 that the capacity of supervision of the FIU in this sector did not meet the expectations of effective supervision. It was found that it is difficult to identify a supervised entity status that depends on variable indicators such as the transaction threshold or the moment at which that threshold is exceeded (for “several linked transactions”).

In conclusion, in 2015, it was found that considering the partial coverage of the sector as obliged entities in the MLTFPA and the accompanying notification obligation, the lack of notifications is rather a sign of low awareness and lack of risk assessments. Thus, the adequacy of the notifications is assessed with a low grade.

Within the framework of the 3rd evaluation round of MONEYVAL, Estonia was proposed to develop guidelines for the identification of suspicious transactions for the NPO sector. The FIU last updated its guide to suspicious transactions in 2019, taking into account, among other things, the relevant

recommendation. In contrast, no separate guidelines have been compiled for NPOs only. Within the framework of the 4th evaluation round of MONEYVAL, a proposal was made to Estonia to reduce the previously valid cash limit for being an obliged entity of NPOs, which was lowered to 5,000 euros as proposed.

#### 8.4.1.6. Conclusion

On a scale of 1-5, the vulnerability level of the NPOs sector in terms of money laundering is 3.38, i.e., it corresponds to the **average** score.

**Table 47.** Level of money laundering vulnerability in the NPO sector.

| Sector | Level of money laundering vulnerability at the sectoral level |                |
|--------|---|----------------|
| NPOs   | 3.38  | <b>average</b> |

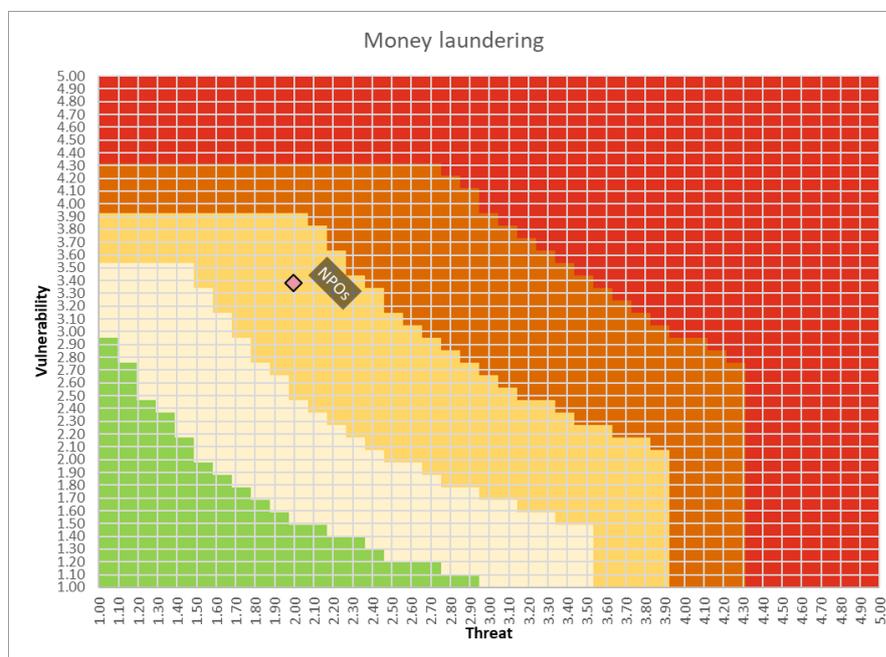
The strengths of the sector include the good organization of the sector and the interest in addressing vulnerabilities.

The most vulnerable areas are the sector’s low awareness of the risks that threaten them, expected significant cooperation with risky foreign countries, the complexity of monitoring, and the lack of resources. One conclusion can certainly be drawn that there is the need to raise the awareness of market participants in this sector, with sector-specific guidelines and training days based on expertise and cases being the most appropriate.

#### Summary

The level of vulnerability of the sector in the national picture is **average**.

**Figure 13.** Heat map of the money laundering risk level of NPOs sector



#### Summary

The level of risk in the sector in terms of money laundering is **average**, which means that risk mitigation needs to be addressed, and concrete measures need to be taken.

Associations in the field of culture, education, and sports in the NPO sector may apply due diligence

measures in a simplified manner. At the same time, the sub-sectors of religious associations and charities have a higher level of risk, potential abuses are more frequent, and therefore enhanced due diligence measures should be introduced in the sub-sectors of the aforementioned NPOs.

#### **8.4.1.7. Risk management strategy**

##### **8.4.1.7.1. Risk mitigating measures at the national level**

Based on the results of the risk assessment, the following suggestions are made to improve the situation at the national level:

- Risk mitigation for vulnerabilities concerning supervision: Supervision by the FIU needs to be strengthened, and supervisory capacity needs to be increased.
- Risk mitigation for the vulnerability of the legal framework: imposing a notification/declaration obligation on NPOs in relation to being an obliged entity or consenting to enter into such transactions should be considered. The purpose of this mitigation measure is, to provide the state with information on what is happening in the sector, which in turn provides a basis for the knowledge about the risks, exercising supervision, and setting the framework for behavioral control of the sector. The issue of the administrative burden on the sector must be taken into account when analyzing the introduction of this obligation. The solution provided should spare the sector and should be technologically efficient for the data provider and the recipient.

Mitigating the risks arising from the vulnerability stemming from low awareness: national options for training that is linked with the sector should be analyzed. It is clear that the sector needs more attention from the state to improve its capabilities in recognition and avoidance of unwanted transactions. Possible topics for training and information days could be cross-border activities, alternative payment services, and the importance of knowing the transaction partner. Developing a sector-specific guideline that describes, inter alia, possible typologies that threaten the sector and thus help to prevent undesirable behavior by recognizing them should also be given consideration. In addition, the guideline could raise awareness of transactions with high-risk countries, focusing on measures that help prevent the exploitation of NPOs.

##### **8.4.1.7.2. Mitigating measures at the level of obliged entities**

Based on the results of the risk assessment, the following proposals are made to improve the situation at the level of obliged entities:

- Developing funding transparency principles - consideration should be given to increase the transparency of funding, including donations and other forms of financing of the activities.
- In the case of large NPOs, recommending an audit - members or funders could request it and would be informed in which cases it is beneficial asking for it. For example, auditing is mandatory for Fs.
- To introduce and develop cooperation opportunities for NPOs with the state, which would increase the transparency of NPO activities.
- To improve cooperation between the professional association and the supervisory authority;
- To engage the sector in the preparation of sector-specific training.

#### **8.4.2. Vulnerabilities of prevention of terrorist financing**

##### **8.4.2.1. Exposure to risk**

Examples of threats in the context of the prevention of terrorist financing related to the organizations operating for charitable, religious, cultural, educational, social, or family purposes include exposure to cash and virtual currencies, regardless of the amount. The way in which terrorist acts are

committed, and the methods of financing them have changed so much in recent years that the thresholds on cash amounts do not give the expected effectiveness. Application-based cross-border transactions via payment service providers and virtual currency service providers create a favorable and anonymous channel of financing the Islamic extremists. Most calls on social applications (such as Telegram) and online environments ask for financial donations in a way that is “secure” for both the sender and the recipient, i.e., through a payment service provider or virtual currency service provider, and preferably using service providers operating in the Russian Federation.

Although the risk of terrorist financing can be assessed as low in the case of a religious association uniting the Estonian Muslim community and foundations not registered in the register of religious associations, certain aspects of vulnerability exist there:

- ✓ the community is supported in cryptocurrency; and
- ✓ starting to collect donations using the payment terminal.

Largely, the collection of donations in cash and their transfer to a bank account depends on the discretion of the company’s governing body. In addition to financial support, the association uniting the community may provide logistical support to persons with Islamic extremist inclinations, either in the form of transport or accommodation, which may take the form of criminal offense provided for in § 237<sup>3</sup> and § 237<sup>5</sup> of the Penal Code.

Based on the survey the awareness about the threats, risks, and measures of terrorist financing is rather low.

#### **8.4.2.2. Risk awareness**

##### **Management commitment and leadership**

A detailed discussion of this topic can be found in section 8.4.1.2.

#### **8.4.2.3. Quality of terrorist financing detection and prevention of financing of proliferation of weapons of mass destruction**

##### **Quality of supervision**

A detailed discussion of this topic can be found in section 8.4.1.3.

##### **Effectiveness of compliance control systems and reporting**

The general description is similar to that of the approach to money laundering in terms of the prevention of terrorist financing. It is relevant to add that, from the standpoint of terrorist financing, the operation of the sector in many countries, including conflict zones and countries with high crime rates, is an additional vulnerability. Terrorist financiers can both use a real charity and imitate charities by creating a seemingly charitable organization to cover up terrorist financing.

##### **Brief summary**

The overview on the prevention of money laundering is also relevant here. With regard to the mechanisms for identifying complex or unusual transactions, the difference is that the NPO must understand exactly how, by whom, and for what purpose the services, products, and money it offers are used. Compared to money laundering, it is even more important here to know the activities of one’s transaction partners and with a special emphasis on their activities after the transaction.

##### **Quality of the framework of due diligence measures applied with regard to customers**

As regards terrorist financing due diligence measures, anti-money laundering due diligence is appropriate. In addition, lists of sanctions are used. It is also beneficial if the organization has a thorough knowledge of its field of activity and the area in which it operates. The better the organization’s knowledge of the cultural, social, and political aspects relevant to its field of activity, the better the organization will be able to select its transaction partners and channel the activity.

Vulnerabilities found in the survey on the quality of the customer control framework:

- With regard to due diligence applied to customers, the above-mentioned shortcomings in the prevention of money laundering have also a similar effect on the prevention of terrorist financing. Only with the difference that for becoming an obliged entity in the context of the prevention of money laundering the preconditions are cash payment in the amount of 5,000 euros, suspicion of money laundering, or doubt about the sufficiency or truthfulness of documents and data. However, with regard to terrorist financing, the only criterion for the application of due diligence measures is the suspicion of terrorist financing. When terrorism is suspected, less than 5% of respondents check the lists of sanctions. Just a few respondents take into account the threat of foreign propaganda and radical movements when drawing up risk scenarios and assess the risks of terrorist financing associated with a transaction partner during a background check (both around 7%). As a rule, a general background check is mentioned as a due diligence measure.

#### **Brief summary**

Awareness of the potential and threats of terrorist financing in the sector appears to be low. Among the measures in place that are used to better “know your client” is background checks (albeit to an unknown extent) and, to a lesser extent, sanctions list.

#### **Quality of the identification of sector-based international sanctions**

Many sanctions are aimed at deterring the activity of terrorist groups. States have identified individuals and organizations involved in terrorism when imposing sanctions. In order for sanctions to work and to have a deterrent effect on terrorism, it is important that the private sector and the third sector apply sanctions effectively. This requires that market participants do not enter into transactions with sanctioned persons and organizations. The easiest way is to check if the transaction partner is on the list of sanctioned persons.

The control of sanctions is mandatory by law, and in this respect, the guideline of the FIU has been adopted and the list of sanctions is available. Only about 2% of respondents said that their organization had a mechanism in place to detect the circumvention of sanctions. At the same time, there were slightly more NPOs and Fs that, according to the results of the survey, made transactions with persons, companies, and/or organizations located in countries where persons, companies, and/or organizations are known to be sanctioned. In addition, it must be taken into account that some sanctioned companies, persons, and organizations also manage to operate in third countries, and it cannot be ruled out that also in Estonia. If weak customer due diligence mechanisms are added here, this combination will not guarantee the enforcement of sanctions.

#### **Brief summary**

The effectiveness of the enforcement of sanctions in the sector is insufficient.

#### **8.4.2.4. Sector-specific risk assessment with the quality of sector-specific controls**

The following vulnerabilities have been identified in the analysis and assessment of sector-specific risks:

1. Regulatory vulnerabilities: To change the applicability of the regulation of NPOs by supplementing it in a way that would make transactions with risk countries a mandatory precondition for the application of the regulation.
2. Vulnerability due to low awareness and high-risk countries: NPOs raise money to help people in third countries. The NPO does not have sufficient knowledge and/or control over the use of money in another country. It may happen that some or all of the resources are redirected unbeknownst to the NPO to activities that support the activities of radical and/or terrorist organizations or the spread of their ideas.

#### **Brief summary**

Risky scenarios that may materialize through the vulnerabilities described above are discussed in more detail in the relevant subchapter of the report on money laundering. In conclusion, the sector is

vulnerable to terrorist financing precisely because the sector’s awareness of the prevention of risky transactions is very low, and the risk scenarios of threats may thus materialize.

#### 8.4.2.5. Quality of response to risks identified in previous evaluations

An appropriate overview is given in section 8.4.1.5.

#### 8.4.2.6. Conclusion

On a scale of 1-5, the vulnerability score of the NPO sector from the aspect of terrorist financing is 3.47, i.e., higher than the average.

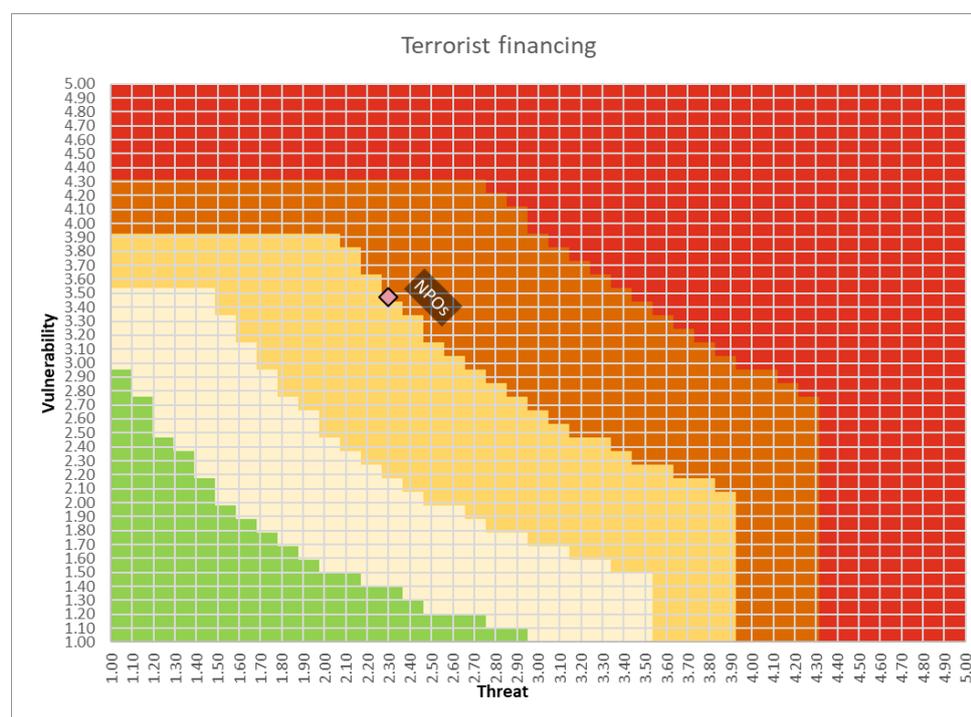
**Table 48.** Level of vulnerability to terrorist financing in the NPO sector

| Sector | Level of vulnerability to terrorist financing at sectoral level |                     |
|--------|---|---------------------|
| NPOs   | 3.47  | <b>average/high</b> |

The strong sides of the sector can be considered the strong will to cooperate and the interest in dealing with problems arising from vulnerabilities.

The most vulnerable areas are low awareness, the complexity of supervision, the lack of sector-specific guidelines, and the allocation of scarce resources to address the sector.

**Figure 14.** Heat map of the terrorist financing risk level of the NPO sector



#### Summary

The level of vulnerability of the sector in the national picture is **average/high**, which requires the implementation of specific risk mitigation measures.

Associations in the field of culture, education, and sports in the NPO sector may apply due diligence measures in a simplified manner. At the same time, the sub-sectors of religious associations and charities have a higher level of risk, potential abuses are more frequent, and therefore enhanced due diligence measures should be introduced in the sub-sectors of the aforementioned NPOs.

#### **8.4.2.7. Risk management strategy**

##### **8.4.2.7.1. Risk mitigating measures at the national level**

Based on the results of the risk assessment, the following suggestions are made to improve the situation at the national level:

- To analyze the possibilities of imposing a declaration obligation on obliged entities in the NPO sector.
- Preparation of sample and instructional materials for NPOs, which would assist in the preparation of a risk management plan and in the management of risks on a daily basis.
- Information days and training for the NPO sector on the most relevant risk scenarios.

##### **8.4.2.7.2. Risk mitigating measures at the level of obliged entities**

Based on the results of the risk assessment, the following proposals are made to improve the situation at the level of obliged entities:

- To change the regulation of MLTFPA in a way that would establish a new precondition of obliged entity for NPOs that collect assets or send assets to risk countries to be subject to the regulation.
- To improve cooperation between the professional association and the supervisory authority.
- Significantly raise awareness through sector-specific training.