11.7. Professionals: vulnerability of the company service providers' sector

11.7.1. General description of the sector

Specificity of the sector

Trust and company service providers, called limited partnership funds and company service providers, before the amendment to the law that entered into force on 20.07.2020, may be confused with the field of investment funds and fund management due to their name but these services must be considered separately. Trust and company services are not a service that qualifies as a financial institution, which could be considered as a general term as an activity related to fund management, and the nature of the service is opened by § 8 of the MLTFPA:

A trust and corporate service provider within the meaning of MLTFPA is a natural or legal person who, in the course of his or her economic or professional activities, provides at least one of the following services to a third party:

1) the establishment of a company or other legal person, including acts related to the transfer of holdings;
2) acting as a director or a member of the management board in a company, partner in a general partnership or in such a position in another legal person, as well as arranging for another person to take up the above position;
3) enabling the use of the address of the seat or place of business, including enabling the use of the address as part of the contact information or the use of the address for receiving postal items and the provision of other services related to the aforementioned to a company or other legal person, partnership or other association without a status of a legal person;
4) acting as a trustee or as a representative of a civil law partnership, community, or other association of persons without the status of a legal person or appointing another person to this position;
5) acting as a shareholder's representative or arranging for another person to act as a shareholder's representative, except in the case of companies whose securities are admitted to trading on a regulated securities market and to which disclosure requirements or equivalent international standards in compliance with the European Union legislation are applied.

It is not possible to single out in the law all activities that can be considered as trust and company services when providing a service, so this approach leaves room for interpretation and disputes, in particular as to whether the specific service provided qualifies as a provision of a service in that field or simply as a provision of legal advice. Including, in some cases, offered by an advocate bureau. It is also unreasonable for supervisory authorities to keep an exhaustive list of activities, i.e., what are specifically the activities of transfer of shareholdings that are provided as services or services related to the provision of an address service, and in practice, situations have to be assessed on a case-by-case basis. It is important that the provision of at least one of the services listed in the above-mentioned clause as an economic activity qualifies as obliged entity within the meaning of the MLTFPA (professional activities are rather rare).

In the case of a trust and company service provider, it is an obliged entity within the meaning of the MLTFPA, and a corresponding activity license must be applied for in order to provide the service. The Financial Intelligence Unit (hereinafter FIU) issues an activity license and supervises compliance with the requirements of the MLTFPA.

Pursuant to § 72 of the MLTFPA, an activity license is issued to an enterprise if:

- the undertaking, a member of its management body, procurator, beneficial owner, and owner do not have any unexpired conviction for a criminal offense against the authority of the state, offense relating to money laundering or other wilfully committed criminal offense;
- the persons specified in the above clause have a good business reputation;
- the contact person appointed by the undertaking on the basis of § 17 of the MLTFPA meets the requirements provided for in the MLTFPA;

According to the valid MLTFPA, trust and company services are not the same services that are provided by financial authorities, i.e., liability for operating without an activity license is determined by misdemeanour proceedings pursuant to § 372 of the Penal Code.

The following table summarizes the market participants identified in this risk assessment as trust and company service providers on the basis of the data of the Register of Economic Activities (REA):

Table 100. Description of the sector of company service providers

Market participants	Number of market participants as of 31.12.2017	Number of market participants as of 31.12.2018	Number of market participants as of 31.12.2019	Number of market participants as of 31.12.2020	Existence of a professional association or umbrella organization
Trust and company service providers	115	226	283	316	N/A

Pursuant to subsection 63^1 (2) of the Commercial Code, if the management board of a company or a body substituting therefor is located in a foreign state, the company must designate a contact person. In such a case, a trust and company service provider specified in § 8 of the MLTFPA may be appointed as a contact person. Pursuant to subsection (5) of the same provision, the Estonian address must be submitted to the commercial register for the service of, inter alia, procedural documents of the undertaking and statements of intent addressed to the undertaking. Due to the above requirements, the sector is characterized by servicing foreign customers, which certainly has an impact on the risk level of the service as a risk-increasing factor. At the request of customers, companies are mainly established as a service, as well as the organization of the position of a member of the management board, during which a suitable candidate for the company's management is sought, and the necessary formalities are performed in the commercial register.

No information is available when providing the trust service. A trust in the meaning of the MLTFPA is a legal relationship established on the basis of or arising from the law of the country recognizing it, according to which trust property formed by a settlor is administered a trustee in the trustee's own name, but in the interests of beneficiaries or for another defined purpose, as well a legal arrangement specified in the consolidated list published the European Commission on the basis of Article 31(10) of Directive (EU) 2015/849 of the European Parliament and of the Council.

The trust and company service provider must apply due diligence measures on the bases specified in § 19 of the MLTFPA:

1) when establishing a business relationship;
2) upon making or mediating occasional transactions outside a business relationship where a transaction with a value of over 15,000 euros or an equivalent sum in another currency is made, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments over a period of up to one year unless otherwise provided by law;
3) upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;
4) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions, or limits provided for in the law.

It is not characteristic for this sector that services are occasionally provided as transactions without establishing a business relationship within the meaning of the MLTFPA, and therefore due diligence measures apply. However, it cannot be ruled out that certain services may be provided without establishing a business relationship. As a result, a transaction of less than 15,000 euros may be left without the application of appropriate risk assessments and mitigation measures. Such a service may be a single transfer of a business (the sale of the so-called "shelf" company), as long as such a sale does not enter into a long-term contract. If the company's service provider continues to provide, for example, a contact person service in addition to the service previously provided, a business relationship will be established with the customer.

Table 101. Data from a survey of company service providers' sector

Sector	Number of market participants	Sample volume	Sample size/ number of responses required	Number of invitations sent out	Number of responses received	Response rate
Company service providers	297	sample	168	297	103	61%

Despite the lack of an organization of market participants in the sector, the sector actively participated in the NRA survey.

11.7.2. Description of risk typologies

Possible risk scenarios that trust and company service providers may be exposed to in the context of money laundering prevention:

1) The services may be used to organize figureheads onto the board of the company in order to disguise the real managers and the beneficial owners;
2) Arranging the service required for the intermediary execution of money laundering in the form of the creation of companies (network) and the creation of a complex acquisition and management model;
3) Enabling the use of a fictitious business address in business operations;
4) Concealment of the company's actual economic transactions and reduction of transparency;
5) Services necessary to disguise links with legal persons used in money laundering schemes after the commission of illegal acts;
6) As a trustee, management of assets of unknown origin, including management of contaminated assets;
7) As a trustee, making decisions related to the management of assets under the guidance of the trustee, which is done for the purpose of money laundering.

11.7.3. Threats

11.7.3.1. Threats of money laundering

In practice, during the period under review, this national risk assessment has not identified any cases of money laundering in the sector where relevant convictions have taken effect.

The main money laundering threats in the trust and company service providers' sector are:

1. Services ordered to hide the beneficial owner (high);
2. The origin of the capital used in the economic activity of the enterprise or entity is not identifiable, including foreign assets (average);
3. Use of figureheads as a service (high);
4. Acquisition of companies for use as shell companies (high);
5. Concealment of the company's actual place of business by means of an address service (average);

6. Use of forged identity documents in the application of due diligence measures (average);
7. Willingness of politically exposed persons (related parties) to use services for non-transparent transactions (average);
8. Avoidance of the measures of the MLTFPA (apparent non-establishment of a business relationship) (high);
9. Improper knowledge of the requirements of the law by market participants and as a result not weighting the risk of risky transactions against the established internal risk appetite (high);
10. Provision of the services of the sale of shelf companies to non-residents and e-residents (high).

Conclusion

The risk of using services for money laundering is average to high depending on the nature of the services and practice. Examples of lower-risk services include the less common trust management service. A provision of an address service can be considered an average-risk service, in which case the company is registered in Estonia, but the actual activities take place elsewhere, and the persons using the service are non-residents. A higher risk service is, for example, the provision of the services of a member of the management board, in the course of which it is possible to conceal the beneficial owners and members of the management body. There are situations where trust and company service providers appoint as members of the management board persons who do not have knowledge of the company's business model and transactions, as well as situations where the origin of the company's capital cannot be established due to its foreign origin. When suspicious transactions are identified, it is difficult for supervisors to identify and prosecute the organizers of the transactions. The provision of shelf companies' sales services to non-residents and e-residents, including the sale of companies and applying for an FIU activity license to provide services in high-risk sectors (virtual currency service providers, financial authorities, as well as company service providers), can also be considered high risk. Estonian e-residency for natural persons from third countries as well as the Estonian activity license gives the company apparent credibility and gives the impression of actually operating in the market. Thus, there is a risk of exploitation of the company (as a front or buffer company in service-based money laundering schemes and tax fraud schemes, respectively). Acquirers of licensed companies include both real FinTech entrepreneurs and those who use Estonian companies as shell companies.

Table 102. Level of money laundering threat in the company service providers' sector

Sector	Threat level of money laundering at the sectoral level	
Company service providers	2	**low**

11.7.3.2. Threats of terrorist financing

Terrorist financing and related threats were not identified in the practice of provisioning trust and company services. A theoretical threat can be seen in the possibility of using services to disguise the real beneficial owners of companies in order to carry out economic transactions aimed at terrorist financing. Due to the nature of the services, the use of the service is rather inappropriate for terrorist financing.

Conclusion

Based on the available information, the threat of terrorist financing is low for trust and company service providers.

Table 103. The level of terrorist financing threat in the company service providers' sector

Sector	Threat level of terrorist financing threat at the sectoral level	
Company service providers	2.30	**low**

11.7.4. Vulnerabilities

11.7.4.1. Vulnerabilities of prevention of money laundering

11.7.4.1.1. Exposure to the threat

The vulnerability of trust and company service providers to money laundering is linked to the type of service provided. Recently, these market participants have primarily served customers who are interested in offering services related to virtual currencies in Estonian jurisdiction. As a result, the transfer of companies' holdings to non-resident customers with a foreign background has increased. In some cases, it is offered with an address service or the service of arranging for the appointment of a member of the management board.

Vulnerability can be caused by regulatory ambiguity and incorrect application of risk mitigation measures, such as incorrect identification of risks or failure to take appropriate action. One indicator of vulnerability is the high-risk appetite of market participants. As risk appetite is defined by the company's management and the main motivator for lowering high-risk appetite is the risk of losing one's reputation as a service provider, one of the vulnerabilities is the indication that the risk of reputational loss alone may not be motivating enough to reduce appetite.

The survey of market participants conducted during the national risk assessment asked to describe the theoretical and practical typologies of risks related to the prevention of money laundering and terrorist financing in the sector. 103 companies participated in the survey, of which 63 did not answer the question, and 11 could not point out the typologies. The responses were distributed as follows:

Table 104. Typologies of risks identified in the survey

Typology	**Number of respondents**
Transactions concealing the beneficial owners	2
Fictitious transactions	2
Large cash transactions	10
Transactions related to the public sector and PEPs	1
The other party to the transaction is not identifiable	2
Tax evasion	5
Unusual/suspicious business	6
Transactions with third parties with which there is no business relationship	3
Not understandable loans/write-offs	3
Unclear financial sources	4
The beneficial owners do not live in Estonia	1
Transactions with figureheads	8

The survey revealed that approximately 3/4 of the respondents could not name the typologies of risks related to the prevention of money laundering and terrorist financing in their field. The above indicates that service providers are unable or unwilling to effectively assess and identify risks in the sector.

11.7.4.1.2. Risk awareness

Management commitment and leadership

The results of a survey of market participants conducted during the national risk assessment show that in 77 of the 103 companies, a member of the management board is responsible for preventing money laundering and terrorist financing. The result shows that a board member plays a leading role in this area.

The results of the survey show that approximately 40% of respondents do not carry out background checks when recruiting their employees and do not monitor their activities during the employment relationship. Also, an equivalent number of companies do not assess the reliability of their employees in the middle of the employment relationship. When companies that assess the reliability of employees were asked to specify the principles, frequency, and implementation of the assessment, 55% did not provide details. Management's commitment to verifying the reliability and competence of employees is lacking. This situation poses a risk that the knowledge of the employees of the companies operating in the sector does not correspond to the level required for working in the field. Only 51 respondents have provided regular training for their employees. The rest of the service providers consider regular training to be reading amendments to the law, discussions, or no training at all and are not able to specify how the training is provided.

Inadequate background checks, assessment of knowledge and experience, and failure to check reliability make the sector vulnerable, as those who monitor risks may not be competent and committed. The reason for the insufficient training can be considered the lack of specific training, as in the period 2017-2019, the FIU has organized only one training for service providers.

According to only eight service providers, reporting a suspicion of money laundering can have negative consequences for the reporting employee, which is why more than half of the service providers do not have appropriate measures to protect employees. Two service providers have also pointed out that as a measure to protect the employee, the harassed employee will be released.

The foregoing indicates that management is not committed to protecting employees from reporting suspicions of money laundering, which may limit the motivation of employees to report such suspicions to management and to notify to the FIU. This is supported by the number of notifications submitted to the FIU by trust and company service providers.

In the period 2017-2019, the service providers have submitted only four notifications to the FIU. As there are service providers with a rather high-risk appetite operating in the sector, there is a risk that the company has not sufficiently assessed and hedged the risks.

Brief summary

The lack of regular and appropriate training and the lack of protection for employees shows the low level of commitment of the board, which in turn reflects that compliance with money laundering and terrorist financing prevention rules is not a priority for company management and makes the sector vulnerable.

11.7.4.1.3. Legal framework and control

Quality of supervision

In the period 2017 - 2019, a total of 7 on-site and remote inspections have been carried out among trust and company service providers. Given the size of the sector, more supervisory resources should be directed there.

The number of inspections carried out has been influenced by the human resources of the FIU supervision. Since 2019, the number of supervisory staff has increased, which enables to direct more supervisory resources to this Sector.

Brief summary

On a scale of 0-4, the trust and company service providers for the existence and application of the penalty in the aspect of money laundering is 2.5, i.e., average-high. On a scale of 0 to 4, the rating of the effectiveness of supervisory practices in terms of money laundering for the trust and company service providers is 1.88, i.e., average-low. Based on previous data and grades, the quality of supervision needs to be improved by increasing the volume of inspections carried out.

Effectiveness of compliance control systems and reporting

The results of the survey revealed that approximately 75% of service providers do not invest in risk management technology solutions. Also, only half of the service providers consider the available sources to be sufficient to identify a politically exposed person. The foregoing suggests that service providers do not contribute to the effectiveness of compliance systems.

Approximately 50% of service providers do not consider the FIU's notification mechanism to be user-friendly, and five systems consider the system to be too complex. Pursuant to § 50 (2) of the MLTFPA, the notice must be submitted to the FIU via a web form or x-road. In addition to the possibilities specified by law, service providers in various sectors also use e-mail to fulfil the notification obligation. As trust and company service providers (or persons involved in this field of activity) have submitted only four notifications in the period 2017-2019, the assessment of the complexity of the system given in the survey may not be objective.

Brief summary

As the clients of service providers are mostly non-residents, the adequacy of the compliance control system is important. As the risk appetite of service providers is high, but notifications are not transmitted by the sector, it can be concluded that service providers do not sufficiently implement the requirements of the MLTFPA.

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

MLTFPA provides situations and provides for various due diligence measures, in the application of which the trust and company service provider must take the following measures in cases provided by law:

- identification of the customer or the person participating in the occasional transaction and verification of the submitted information;
- identification and verification of the identity and right of representation of the representative;
- identification of the beneficial owner and measures are taken to verify his or her identity to the extent necessary to enable the obliged entity to ascertain who the beneficial owner is;
- understanding the business relationship, occasional transaction, or operation;
- obtaining information on whether the person is a politically exposed person, a member of his or her family, or a person considered to be a close associate;
- business relationship monitoring.

As the provisions of the MLTFPA are mainly applied in the sector in a general manner, the implementation of which must take into account the guidelines of the FIU, the level of application of due diligence measures in the sector cannot be considered appropriate with possible risks. As it is not a financial institution, stricter identification requirements do not apply, i.e., services may in certain cases be provided without identification. For example, in the absence of a business relationship, for transactions below the 15,000 euros threshold and without other legal conditions. In order to mitigate risks, the level of regulation should be raised so that the use of services in the sector without identification is not allowed.

Approximately 50% of the respondents consider the Estonian information systems used for checking customer data to be thorough and reliable. Also, around 65% of respondents consider that the information

needed to identify the beneficial owners is readily available. More than half of the service providers consider that the information needed to identify and verify high-risk customers is not easily available. The reason given is that the source of information is missing or unreasonably expensive.

Brief summary

The vulnerability of trust and company service providers in the aspect of the availability of reliable identification mechanisms and information on beneficial owners in terms of money laundering is average-low. The vulnerability of trust and company service providers in the aspects of the effectiveness of customer due diligence measures in high-risk situations with regard to money laundering is high.

11.7.4.1.4. Sector-specific risk assessment with the quality of sector-specific controls

The survey revealed that eleven service providers had identified companies in the course of their activities that help to hide a person's participation in a business transaction or to hide the owner of the property and the beneficial owners. Fraud related to the bankruptcy or compulsory liquidation of persons has also been observed. Due to the number of notifications submitted to the FIU, the relevant information has not been submitted within the notification obligation.

Brief summary

The vulnerability of trust and company service providers in the aspect of money laundering is average-low, with only 11 of the 103 companies surveyed reporting that they have observed concealment of owners and beneficial owners.

11.7.4.1.5. Quality of response to risks identified in previous evaluations

The results of the NRA 2015 showed that the level of vulnerability of the sector was average during the previous assessment period. The recommendations made to address the situation were as follows:

- training;
- supervision,
- changes in legislation.

The NRA 2015 recommendations are also relevant in this risk assessment.

11.7.4.1.6. Conclusion

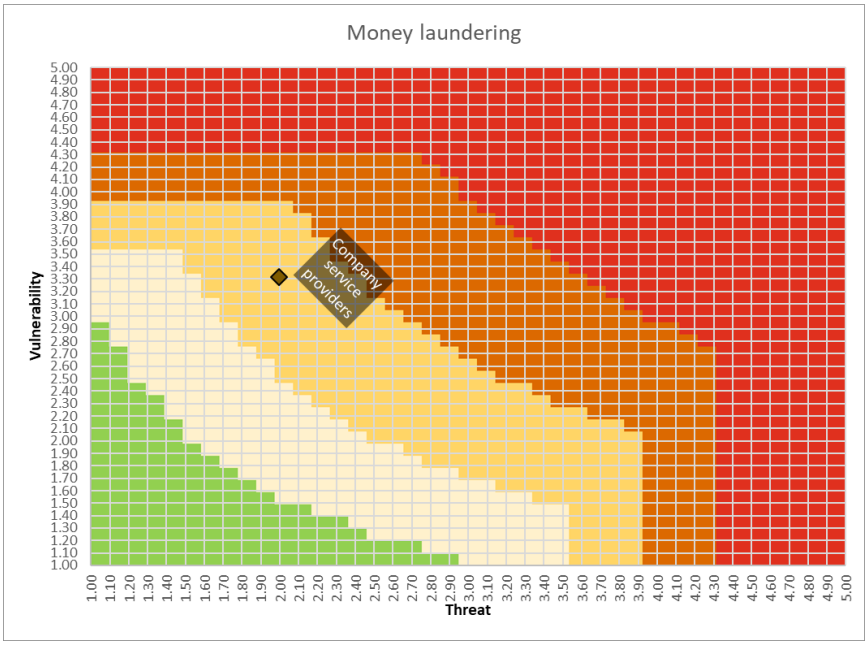
The level of vulnerability of the trust and company service providers sector to money laundering is above the average.

One of the strengths of the sector is that the number of service providers is rather low at the moment. The most vulnerable areas are the high-risk appetite of companies operating in the sector, the lack of training, and non-compliance with the notification obligation. The additional vulnerability is that persons get a feeling of impunity, which means that in order to be punished under criminal law, it is necessary to show, from which criminal activity the money that is being concealed, comes from. It can be concluded from the above that there is a need to raise the awareness of market participants in this sector. This aspect needs to be addressed at the state level.

Table 105. Level of vulnerability of money laundering in the company service provider' sector

Sector	Level of vulnerability of money laundering at the sectoral level	
Company service providers	3.31	**average**

Figure 33. Heat map of the money laundering risk level of the company service providers' sector



Summary

The location of the level of vulnerability of the sector on the state heat map is rather among the sectors with a higher risk level and an above average assessment level. Enhanced due diligence measures need to be implemented in this sector.

11.7.4.1.7. Risk management strategy

11.7.4.1.7.1. Mitigation measures at the state level

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

- Further consider whether, due to the higher risk inherent in the sector, it is necessary to introduce additional regulations to mitigate the risks. One possibility is to make the identification upon application of due diligence measures mandatory for the provision of all sub-services identified under this service, regardless of the amount of the transaction.
- To supplement the regulation of the Penal Code so that it would be possible to hold persons liable for the provision of concealment activities for commercial purposes (without the need to prove that the money, the origin or ownership of which is concealed, comes from criminal activities).
- To consider the need to set up regular reporting, which would characterize the range of services offered by market participants, figures, and customer data. The imposition of this obligation is necessary to enable law enforcement and supervisory authorities to react immediately to any identified risk. It would also allow for a more efficient allocation of public resources to mitigate risks.
- To allocate additional resources to make supervision more effective.
- To develop guidance material for the sector on risk management measures and mitigation. If necessary, draw up guidelines depending on the type of services provided.
- With regard to the identification of politically exposed persons, consider setting up and maintaining a national database with appropriate access. If possible, to find solutions for more effective identification of foreign politically exposed persons.

11.7.4.1.7.2. Mitigation measures at the level of obliged entities

Based on the results of the risk assessment, the following proposals are made to improve the situation within the sector:

- the establishment of an umbrella organization that would enhance cooperation both within the sector and with the FIU and other state authorities;
- arranging training for employees of companies related to meeting the requirements of MLTFPA;
- the description of due diligence measures is kept appropriate and amended in accordance with the company's operations and changes in legislation and guidelines;
- enhancing and developing compliance control systems to increase the effectiveness of identifying both non-residents and politically exposed persons.

11.7.4.2. Vulnerabilities of prevention of terrorist financing

11.7.4.2.1. Exposure to the risk

No direct exposure to terrorist financing has been identified in the activities of trust and company service providers. The risk assessment should pay attention to persons from high-risk countries or persons whose activities may give rise to suspicions that companies are formed to arrange resources for terrorism financing.

11.7.4.2.2. Risk awareness

Management commitment and leadership

As the sector is not characterized by the services related to the transfer of value, which would be riskier in terms of terrorist financing, the national risk assessment did not identify in practice any vulnerabilities with regard to the actions taken by market participants. Risks should be mitigated by raising the awareness of employees and members of management of market participants.

The results of a survey conducted by the NRA show that approximately 80% of service providers assess the risks of terrorist financing during customer background checks and appropriate control measures when monitoring business relationships.

Brief summary

The vulnerability of trust and company service providers to the existence and effectiveness of access controls in terms of terrorist financing is moderately high. The vulnerability of trust and company service providers to employee integrity in relation to terrorist financing is also average-high.

11.7.4.2.3. Quality of terrorist financing detection and prevention of financing of proliferation of weapons of mass destruction

Quality of supervision

The vulnerability of trust and company service providers to the existence and enforcement of sanctions in terms of terrorist financing is average-low. The vulnerability of trust and company service providers in the aspect of effectiveness of supervisory proceedings and customs in terms of terrorist financing is average-low.

Effectiveness of compliance control systems and reporting

Similar to the money laundering assessment, there is no regular compliance monitoring system or reporting in the sector. In order to identify the risks of money laundering, the introduction of a reporting obligation should be considered, but no such conclusion was reached in the current assessment regarding the risks of terrorist financing.

Brief summary
The vulnerability of trust and company service providers in the aspect of terrorist financing in terms of compliance systems is moderately high. The vulnerability of trust and company service providers to the effectiveness of reporting in terms of terrorist financing is average-high.

Quality of the framework of due diligence measures applied with regard to customers
The identification of risks and the taking of necessary measures are carried out analogously to the implementation of money laundering risk management measures.

Brief summary
The rating of trust and company service providers in terms of reliable identification mechanisms and the availability of information on beneficial owners for terrorist financing is average-low. The vulnerability of trust and company service providers in the aspect of the effectiveness of customer due diligence measures in high-risk situations with regard to terrorist financing is average-low.

Quality of the identification of sector-based international sanctions
Trust and company providers are not persons with a specific obligation, so the obligation to impose sanctions is applicable in a general manner.

Brief summary
The vulnerability of trust and company service providers to terrorist financing is average-low.

11.7.4.2.4. Sector-specific risk assessment with the quality of sector-specific controls

The established regulation on market entry deals with terrorist financing risks together with money laundering risks. No additional quality controls have been established to prevent the vulnerability of terrorist financing. The lack of necessity is also confirmed by the result of this risk assessment.

Brief summary
The vulnerability of trust and company service providers in the aspect of terrorist financing is average-low.

11.7.4.2.5. Quality of response to risks identified in previous evaluations

The results of the NRA 2015 showed that the level of vulnerability of the sector was average during the previous assessment period. The recommendations made to address the situation were as follows:

- training;
- supervision,
- changes in legislation.

The NRA 2015 recommendations are also relevant in this risk assessment.

11.7.4.2.6. Conclusion

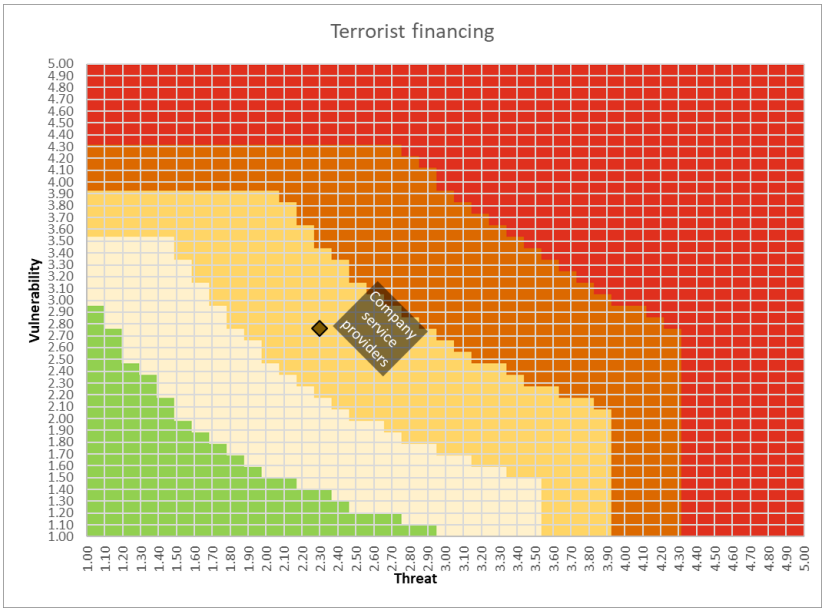
The vulnerability of trust and company service providers in the aspect of terrorist financing is **low.**

The threats associated with terrorist financing are, in practice, rather minimal in terms of trust and company services. The working group is of the opinion that the sector is no more vulnerable to transactions for terrorist financing than other sectors, i.e., the risk is low. The identified vulnerabilities have been compensated by regulation and the requirement of due diligence measures and compliance with the notification obligation, i.e., the service is rather not vulnerable, as due diligence measures are applied on the same principles as in the prevention of money laundering.

Table 106. Level of vulnerability of prevention of terrorist financing in the company service providers' sector

Sector	Level of vulnerability of prevention of terrorist financing at the sectoral level	
Company service providers	2.76	**low**

Figure 34. Heat map of the terrorist financing risk level of the company service providers' sector



Summary

The level of risk in the sector in terms of terrorist financing is **average**, which means that the risk and its consequences must be known, and risk mitigation measures must be implemented to improve the situation. Enhanced due diligence measures need to be implemented in this sector.

11.7.4.2.7. Risk management strategy

11.7.4.2.7.1. Risk mitigation measures at the state level

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

- At the request of market participants, the FIU should provide opportunities for market participants to work together to effectively identify sector-specific risks for services and customers.

11.7.4.2.7.2. Risk mitigation measures at the level of obliged entities

Based on the results of the risk assessment, the following proposals are made to improve the situation within the sector:

- the establishment of an umbrella organization that would enhance cooperation both within the sector and with the FIU and other state authorities;
- arranging training for companies' employees involved in meeting the requirements of MLTFPA;
- the description of due diligence measures is kept appropriate and amended in accordance with the company's operations and changes in legislation and guidelines;
- enhancing and developing compliance control systems to increase the efficiency of identifying both non-residents and politically exposed persons.