5. Vulnerability of the financial sector

5.1. General description of the sector

Description of the sector

In international comparison, the financial sector of Estonia is relatively small, however, unlike in the rest of the European Union, Estonia's financial sector has grown strongly in the recent years. The financial sector of Estonia is bank-centred. As of the end of 2019, the share of the assets of the banking sector in GDP was 101% and 63%, respectively[1]. The financial sector is one of the pillars of the economy which requires the sector to be stable and reliable. Within the meaning of the Money Laundering and Terrorist Financing Prevention Act (MLTFPA), obliged entities are all persons that are active in the financial sector, namely:

1) credit institutions;
2) financial institutions.

§ 6 of the MLTFPA provides a list of obliged entities. The table below indicates the market participants that are treated as the financial sector in the present risk assessment of money laundering and terrorist financing in Estonia.

Table 20. Overview of the financial sector

Market participants	Number of market participants as at 31 Dec 2019	Number of market participants as at 30 Nov 2020	Number of obliged entities	Existence of a professional association or umbrella organisation
Credit institutions	15	14	100%	Estonian Banking Association
Creditors	59	56	100%	Estonian Leasing Association, FinanceEstonia
Credit intermediaries	14	15	100%	FinanceEstonia
Investment firms	5	5	100%	
Fund managers	15	16	100%	
Small fund managers without an activity licence	27	37	100%	
Investment and pension funds	34	40	100%	
Securities market	2	2	100%	
Life insurance companies	5	5	100%	Estonian Insurance Association, Estonian Insurance Brokers Association
Insurance brokers	10	10	100%	
Payment institutions	11	13	100%	
Paying agents	11	10	100%	
Paying agents of cross-border payment service providers	3	3	100%	
Currency exchangers (based on MTR activity)	44	38	100%	

[1] https://www.eestipank.ee/finantsstabiilsus/ulevaade-finantssektori-struktuurist

Other financial institutions[2]	276	285	100%	No general umbrella organisation, only for some service types, e.g., Estonian Union of Credit Cooperatives
Total	**531**	**549**	**100%**	

In the context of risk assessment, the providers of electronic communication services (telecommunications company) who offer their customers consumer credit services (payment by instalments) and hold a creditor's activity licence prove to be the most distinctive group in this sector. The electronic communication services providers perform payment transactions which are excluded from the activity licence obligation due to the exclusions provided in § 4 of the Payment Institutions and E-money Institutions Act (PIEMIA) (no activity licence is needed and they are also not the subjects of the MLTFPA), following also the limit values provided in § 4 (4) of the PIEMIA (a payment transaction may not exceed €50 and the total sum of payment transactions per one user per one month may not exceed €300) and the content of the payment transactions.

Legal framework

In addition to the legal acts of the European Union[3], for instance Regulation (EU) 2015/847 of the European Parliament and of the Council, at the time of preparation of the assessment, the financial sector of Estonia is subject to, *inter alia*, the following legal acts:

- Money Laundering and Terrorist Financing Prevention Act (MLTFPA),
- International Sanctions Act (ISA),
- Tax Information Exchange Act (TIEA), Regulation No. 25 on the "Technical Requirements and Procedures for Identification of Persons and Verification of Data by Means of Information Technology" of the Minister of Finance of 23 May 2018.

In addition to the legal acts above, the activities of the participants of the sector are regulated by special laws: Credit Institutions Act, Creditors and Credit Intermediaries Act, Payment Institutions and E-money Institutions Act, Insurance Activities Act, Investment Funds Act, Securities Market Act.

The sector participants are subject to supervision by the Financial Supervision Authority (FSA) and for financing institutions also the Financial Intelligence Unit (FIU). Therefore, the companies active in the financial sector are also subject to the guidelines issued by the FSA and FIU:

- recommended guide for the "Organisational Solution for Credit and Financial Institutions and Preventive Measures for Preventing Money Laundering and Terrorist Financing" of the FSA applies to credit institutions, creditors, and credit intermediaries, insurers, insurance brokers, investment firms, fund managers, investment funds founded as public limited companies, and the central register of securities. Pursuant to the MLTFPA, all financial sector participants are obliged entities and must follow the following FIU guides in their activities: the FIU reporting form, the procedure for filling in the reporting form submitted to the FIU, the guide to the characteristics of suspicious transactions, the recommendations of the FIU for managing risks arising from the activities of obliged entities, the recommendations of the FIU for drafting procedure rules and internal control rules.

[2] According to the field of activity of "acting as a financial institution" of the Register of Economic Activities
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847

Table 21. Data from the survey conducted in the financial sector

Subsector	Number of market participants	Sample scope	Sample size / number of required responses	Number of outgoing calls for participation	Number of incoming responses	Response rate
Credit institutions	14	All	13	14	10	77%
Creditors	55	All	48	55	26	54%
Credit intermediaries	14	All	13	14	3	23%
Investment firms	5	All	5	5	4	80%
Fund managers	15	All	14	15	8	57%
Small fund managers without an activity licence	28	All	26	28	3	12%
Securities market participants	1	All	1	1	1	100%
Insurance companies	5	All	5	5	5	100%
Insurance brokers	46	All	41	46	11	27%
Currency exchangers	43	All	39	43	9	23%
Payment institutions and paying agents	21	All	20	21	12	60%
Telecommunications companies	3	All	3	3	2	67%
Paying agents of cross-border payment service providers	3	All	3	3	2	67%
Other financial institutions	268	Sample	158	268	54	34%

Generally, the financial sector actively participated in the survey conducted in the framework of the NRA. If necessary, additional interviews were conducted with the representatives of the subsectors with an insufficient response rate.

5.2. Description of risk typologies[4]

General preconditions for committing money laundering crimes in the financial sector

- The monitoring systems of financial service providers are not efficient enough to identify cash flows of criminal origin. Above all, the following crimes serve as the sources of criminal money:
  - fraud (payment and bank card fraud, skimming[5], BEC scam[6], other scam (including pyramid schemes, so-called investment services, money mules);
  - corruption crimes and tax crimes (bribery, VAT and income tax fraud, etc.);
  - cybercrimes (attacks on computer systems, data compromise (data thefts, manipulations), attacks on infrastructures, attacks on the systems of the financial sector, infecting websites with viruses, illegal crypto mines, attacks on mobile wallets);
  - offences related to narcotic substances;
  - organised crime (types of crimes listed above, organised by criminal organisations);
  - human trafficking.

[4] The typology is based on the work results of the NRA financial sector working group
[5] skimming or copying bank card data
[6] Business E-mail Compromise

- A financial service provider cannot identify the beneficial owners due to the complex ownership structure of the customer or that of the other party of the transaction or due to a lack of information about the beneficial owners in the register.
- A financial service provider cannot identify a transaction where the other party is a politically exposed person (PEP) due to either the deficiency of the screening system or the deficiency of the lists of PEPs.
- Risks related to the correspondence relations of the financial service provider, including a situation where a credit institution has a customer – a company offering cryptocurrency intermediation services – who has not performed the required due diligence measures applied to its customers.
- A financial service provider cannot implement the required due diligence measures applied to its non-resident customers or e-resident customers due to the complexity of identifying their actual risk level.
- A financial service provider cannot identify either a fictitious transaction (fictitious documents related to the transaction) or a fictitious person (fictitious identification documents).
- When Estonian credit institutions and payment service providers refuse to perform foreign transactions, a person can use cross-border financial service providers for money laundering.
- Due to the complexity of identifying specific mechanisms for terrorist financing, a financial service provider cannot identify the transactions intended for terrorist financing.
- Due to the complex specificity of proliferation, a financial service provider cannot identify the transactions intended for the proliferation financing.

5.3. Threats[7]

5.3.1. Money laundering threats

The threat of criminal money entering the Estonian financial system

Criminals use the financial sector for moving the assets they have earned in a criminal way for at least one of the three stages of money laundering (placement, layering, integration). The aim is to use economic transactions to hide resources with criminal origin and their real owner. In Estonia, any crime serves as a predicate offence to money laundering, specific offences are not distinguished. However, more important is what types of crime can be used to earn a larger income which needs to be placed in the financial sector, so that the benefits could be consumed as publicly as possible.

In Estonia, (cyber) fraud is the most prevailing type of crime through which the largest amount of criminal income reaches the financial system. Infringements related to tax evasion are also common, whereas this is common as a both domestic as well as a foreign predicate offence[8]. Criminals take advantage of Estonia's convenient and fast banking system which can be used while not physically being in the country.

However, the reflection of the money laundering scandals related to Estonia in the previous years in the global media and heightened attention may keep the criminals away from using the Estonian financial system. In the light of the above, the threat of criminal money entering the system can be considered "average".

Threat of opacity of transactions

Opacity of transactions helps the criminal to quickly move assets in the financial sector, for instance, moving money between different financial institutions or making transactions with financial instruments. If it is not checked why the money is moved and for what, it gives the criminals an opportunity to exploit the financial sector to launder their criminally obtained funds.

[7] Based on the knowledge of the authorities and the criminal proceedings conducted so far

[8] For instance, a court judgement in criminal case No. 1-19-1400 (legalisation of assets obtained through tax fraud and accounting crimes by the responsible persons of the Finnish company Xxx OY, using Estonian financial institutions to withdraw cash in the total amount of 4,273,272 euros). Also, a court judgement in criminal case No. 1-18-6825 (legalisation of assets obtained through tax fraud and accounting crimes in Finland by using the Estonian financial system). Criminal case No. 1-15-9048 serves as an example of money laundering through avoiding Estonian taxes.

In the larger credit institutions of Estonia, it is impossible to move large sums in a way that the credit institution does not pay any attention to it or does not identify the purpose and content of the transaction. If more complex systems are used, the risk of the lack of sufficient transparency still exists – especially in the case of companies with an especially complex ownership structure and a specific field of activity. Also, the probability of the threat is higher when the field of activity of the company changes or when the transactions take place between the related parties. In smaller financial institutions such transactions may be left without respective attention due to the lack of competent human resources. In the light of the above, the threat of opacity of transactions can be considered "average-high".

Threat associated with companies with non-resident and e-resident owners

In Estonia, non-residents and e-residents can easily and affordably establish companies. There are also a number of company service providers who establish companies which are either sold to non-residents or e-residents, whereas the seller itself remains to be the recipient of documents in Estonia, offering the company a seeming connection with Estonia. In reality, there is no connection with Estonia and it is unclear or extremely difficult to identify, what activities are used to move the funds. For non-residents and e-residents from third countries, the problem also lies in the fact that the overview of the previous activities of the persons is limited or non-existent.

Estonian credit institutions do not easily open bank accounts for non-resident companies or Estonian companies which have a non-existent or a very vague connection with Estonia. Other financial institutions[9] do not make the same strict requirements in this matter. In the light of the above, the threat associated with companies with non-resident or e-resident owners can be considered "average-low".

Threat associated with virtual assets

In relation to the digital movement of assets, the use of cryptocurrencies has become more topical. In Estonia – similarly to the rest of the world – criminals are increasingly using the opportunities to legalise their money by using virtual assets. There is less transparency related to the owners of cryptocurrency wallets and although the transactions are technically public for everyone, the persons behind it still remain anonymous. Blurring methods which do not allow to track the movement of assets are used to hide the transactions. If cryptocurrency is changed to money (so-called Fiat money[10]), the person behind the payment is usually an intermediary and the beneficial owner of the assets may not be evident. It is difficult for credit institutions and other financial service providers to control the origin of the assets, if the company offering virtual assets brokerage services has not properly performed their due diligence measures. In the light of the above, the threat associated with virtual assets can be considered "high".

Threat associated with payment intermediaries

The purpose of payment intermediaries is to offer its customers only the payment service. The number of intermediaries is high and it is not possible to limit the movement of criminal money through them, since the transferred assets do not stay on the account of the intermediary and are moved between the originator and the recipient of the payment. In Estonia, the threats associated with payment intermediaries are high primarily in cases where consumers use the services of cross-border payment service providers whose activities are controlled in the country where they are registered in, which means that the background and activity of the criminal customers is more difficult to check. In the light of the above, the threat associated with payment intermediaries can be considered "average-high".

Threat of cash transactions

Cash is anonymous in nature and therefore there is a risk of exploitation of the financial system when illegal cash is placed in the financial sector. The risk of money laundering is also present when criminally obtained income is withdrawn as cash for the purpose of losing the trace between the criminal income and its beneficial owner.

[9] Companies that act based on the activity licence "acting as a financial institution" issued by the FIU

[10] Fiat money is a currency with no internal value, i.e., it is not secured with "physical goods" (e.g., gold)

In Estonia, the cash turnover in legal economy is small[11]. In the Estonian context, tax evasion or tax return fraud and income earned with (cyber) fraud, drug trafficking and smuggling are the most possible points of threats, where the financial sector may come in contact with large quantities of cash of unclear origin, which is sought to be hidden or directed into legal economy.
In the light of the above, the threat of cash transactions can be considered "average-low".

Threat of transit of money from other countries

The opportunity to use the fast financial system of Estonia simply as a stopover gives criminals more options for layering criminal money or money of unclear origin. Fast cross-border cash flows from countries that do not effectively cooperate internationally give criminals the opportunity to direct their criminally earned income into legal business through our financial system.

The Estonian business community has business relations with both the former Soviet Union and other Eastern European countries[12] for whom the financial system of Estonia used to be a link for moving the funds. Also, there used to be remarkable cash flows with some financial centres with whom the cash flows are currently minimal. The most relevant of the cash flow threats are the cash flows related to external trade. It is difficult for the credit institutions to check the origin of the funds and the persons if the goods or services do not move through Estonia and there are no business activities in Estonia, which is why proper completion of the documents related to the transaction and the veracity thereof often cannot be verified in order to make certain that the data and information submitted to financial institutions are accurate. In the light of the above, the threat of transit of money from other countries can be considered "average-high".

Threat of non-implementation of due diligence measures on customers

By applying suitable due diligence measures on customers, persons who could abuse the financial sector could be kept away from it. Otherwise, the criminals may be able to move funds through front men/companies and not revealing the identity of the beneficial owner to the financial institutions.

In Estonia, the respective threat for credit institutions is small. The hypothetical threat exists when creating customer relationships online. In this case, the major threat lies in greater misuse of personal identification documents and hence the opening of accounts for persons who have not requested it. However, in such cases the opportunity for large-scale money laundering is limited with transaction limits set by the country. Smaller financial institutions may have problems for identifying non-resident customers to the desired extent and therefore funds may be transferred to our financial system the owner or the origin of which is not clear.
In the light of the above, the threat of non-implementation of due diligence measures on customers can be considered "low".

Conclusion

Generally, the threat level of money laundering in the financial sector can be considered average. The biggest threats for the Estonian financial sector are cash flows that are related to:

- transit from former Soviet Union and other Eastern European countries;
- movement of funds obtained from cybercrimes through Estonian virtual assets service providers;
- activities of the Estonian registered business entities of non-residents or e-residents which are not conducted in Estonia;
- intermediation activities which are related to the provision of certain services for companies active in foreign countries;
- services provided by company service providers;
- tax evasion at both local as well as the international level.

[11] Based on the statistics of the European Central Bank, approximately 5% of the payments in Estonia are made in cash (2019)
[12] External trade statistics published by Statistics Estonia

Table 22. The money laundering threat level in the financial sector

Sector	The money laundering threat at the sectoral level	
Financial sector	2.74	**average/low**

It was generally found that the money laundering threat level in the financial sector is **average/low**.

5.3.2. Terrorist financing threats

Insufficient awareness of financial service providers and the related threat of insufficiently implemented due diligence measures against terrorist financing

Due to its geographical location and small Muslim community, Estonia as a small country is not a priority for Islamic extremists to commit terrorist attacks. At the same time, in the near vicinity of Estonia – the Nordic countries and Russia – there are large Muslim communities which is why Islamic extremists use Estonia as a transit country. The favourable economic environment and the real estate market in Estonia have raised active interest in the above-said communities. Among the providers of traditional financial services, awareness of the threats of terrorist financing has improved within the past few years and the work of money laundering authorities has become more effective. The due diligence measures implemented and a conservative approach towards non-residents and e-residents considerably lowers the terrorist financing threat level for the providers of traditional financial services. However, in a competitive environment, the providers of traditional financial services are also under pressure to keep up with innovation, cooperating with payment and virtual assets service providers. The innovative and advanced financial sector of Estonia may be attractive for Islamic extremists for terrorist financing and supporting, which is why the threat level must be considered average.

- Threat associated with payment intermediaries and virtual assets

Instead of using traditional terrorist financing channels (banks, currency exchangers), Islamic extremists and groupings have started to use alternative and anonymous cross-border payment services and virtual assets service providers. If the transaction parties are partially hidden when using the services of payment service providers, virtual assets grant full anonymity. This has led to a trend where terrorist organisations publicly call to support their activities either in a combined manner ("payment service provider + virtual assets") or only in virtual assets. Also, the implementation of enhanced due diligence measures only when exceeding transaction limits is no longer relevant or efficient (many market participants still follow the limit of 10,000 euros). Most of the suspected terrorist financing transactions are made in small sums (often under 10 euros). In the light of the above, the threat associated with payment intermediaries and virtual assets can be considered "high".

Conclusion

In the financial sector, the terrorist financing threat is different as regards the market participants: the threat level can be considered low for the market participants offering insurance and investment services, average for credit and financial institutions, payment and currency exchange service providers, however, when the market participants service the providers of virtual assets service providers, the threat level can be considered high.

5.4. Vulnerabilities

5.4.1. Vulnerabilities of prevention of money laundering

5.4.1.1. Exposure to threat

- Threat of entry of criminal money: the statistics on crimes issued by the Ministry of Justice indicates that in 2019, there were 10,657 crimes registered in Estonia, whereas the criminal income from those crimes may serve as a hypothetical source of money laundering. Such crimes include corruption and bribery, extortion, fraud, tax crimes, cybercrimes, forgery, theft, illegal trafficking

of drugs and psychotropic substances, etc. In 2019, assets with the total value of 7.86 million euros were seized in such crimes.

- Threat of opacity of transactions: 80% of the credit institutions who participated in the market participants survey carried out in the framework of the NRA answered "yes" to the question whether the market participants have identified "suspicious cash flows and/or cash flows of unclear origin, the purpose of which is to hide the beneficial owners and/or the origin of assets"[13].
- Threat associated with non-resident and e-resident owners: pursuant to the data forwarded by the Centre of Registers and Information Systems (CRIS), the following companies have been registered in Estonia[14]:

Table 23. Number of business entities with non-resident BOs in 2018-2020

	2018	2019	as at July 2020
Business entities with at least one non-resident BO	10,206	15,408	14,610
Share of business entities with non-resident BOs of the total number of business entities	5.26%	7.26%	6.62%

- Threat associated with virtual assets: the results of the survey "Survey on Virtual Assets Service Providers (VASPs)", conducted by the FIU, indicate that as at 1 August 2020, there were a total of 611 valid virtual assets service provider activity licences (295 service licences for exchanging VA for money, 261 for wallet service, and 55 VA service licences)[15]. The results of the survey also indicate that the total turnover of the services of virtual assets service providers active in the Estonian market has grown rapidly. While in 2018 it was approximately 590 million euros, in the first half of 2019 it was already twice as much – 1.2 billion euros.[16]
- Threat associated with payment intermediaries: since the threat is mainly related to payment service providers, the responses regarding the volume of the services, provided for Estonian residents (asked in the framework of the NRA as at 2017), indicate that the respective figure totals 250 million euros.
- Threat of cash transactions: the Tax and Customs Board's statistics on cash declaration on the Estonian border indicate that in 2017-2019 the total sum declared was 193.4 million euros (from third countries to Estonia and from Estonia to third countries).
- Threat of transit of money from other countries: the Bank of Estonia's statistics on the payments submitted by credit institutions indicate that in the 3rd quarter of 2017, the volume of cross-border payments was 11.7 billion euros for payments made and 14.6 billion euros for payments received, and in the 3rd quarter of 2020, the volumes were 14.1 billion euros and 18.8 billion euros, respectively (including the payments of all the customers, incl. the central government, customers who are financial institutions, etc.).
- Threat of non-implementation of due diligence measures on customers: if the respective threat is associated with the use of front men, 60% of credit institutions who participated in the market participants survey carried out in the framework of the NRA answered "yes" to the question "whether you have identified cases where you have a suspicion that there are front men involved".
- In the light of the above, it can be concluded that the financial sector of Estonia has real exposure to the above said threats, whereas the level of exposure can be considered "average-high".

[13] In this case, the example provided is from among credit institutions because the share of this sector is dominant in the cash flows (approximately 99% based on the statistics of the Bank of Estonia and the FSA).
[14] The response for the inquiry provided by CRIS in the framework of the NRA.
[15] According to the register of economic activities, as at 31 Dec 2020, there were a total of 478 valid activity licences issued for VA service providers (39 service licences for exchanging VA for money, 34 for wallet service, and 405 VA service licences).
[16] FIU's "Survey on Virtual Assets Service Providers" 22 Sep 2020

5.4.1.2. Risk awareness

Management commitment and leadership

Survey results regarding awareness

The results of the survey carried out in the framework of the NRA indicate that the awareness of the sector on the prevention of money laundering is high. This may be due to the fact that the financial sector is bank-centred but credit institutions can be considered as the most advanced sector in this regard. Credit institutions invest in automatic money laundering and terrorist financing detection solutions, procedure rules as well as in the regular training of employees. They follow the developed guidelines and the instructions issued by the FSA and FIU, which have proved to be of practical value to the banks. At the same time, however, payment institutions have pointed out the need to raise the awareness of the society through training. This indicates the wish and will to achieve better risk detection processes/methods/instructions and the readiness to cooperate with supervisory authorities. Small fund managers without activity licence prove to be an exemption here – their awareness on money laundering prevention is average. The sector is aware that money laundering prevention is an important issue, however, the sector has largely taken a stand that due to the specific nature of the sector, money laundering prevention in this specific sector is not an important issue, i.e., the volume of money laundering risks in this sector is not as large as for other financial institutions (incl. due to the fact that small fund managers do not keep the financial assets of the investors).

The reporting statistics of the sector are supported by the feedback received in the framework of the survey, according to which the majority of the market participants have reported suspicious transactions to the FIU (100% of the credit institutions). The sector is exemplary in following its reporting obligation: reports sent are based on suspicions of money laundering as well as based on the sums: the largest group of institutions reporting to the FIU are credit institutions, who submitted a similar amount of reports in 2017 and 2018 (2,317 and 2,208, respectively), however, in 2019 there were over 600 more reports, a total of 2,905. The increase is due to the volume of reports submitted on unusual activities. The other larger group of reporting institutions are payment intermediaries (1,155 reports in 2017, 962 reports in 2018 and 568 reports in 2019): the large number of reports submitted by payment institutions is related to sum-based reports, whereas such reports are not, for instance, mandatory for credit institutions. The third largest group is formed by settlement and money remitters.

Brief summary

Summarising both the results of the survey and the reporting statistics to the FIU, it can be concluded that the risk awareness of the financial sector is at a very high level and is improving annually. This is expressed by the commitment of the managers and employees of the market participants, which can be seen in the investments in money laundering and terrorist financing detection solutions, training of employees and contributing to the reporting system of the FIU. However, there is still a need to raise the level of awareness among the smaller market participant groups (small fund managers without activity licence, financial institutions).

5.4.1.3. Legal framework and supervision

Quality of supervision

The control measures consist of assessments for mainly two aspects: level of regulations and sufficiency/insufficiency of supervision.

In the financial sector, the level of regulations is very high. The special laws, applicable to the sector participants, stipulate the requirement of an activity licence for the majority of the financial services providers, which helps to ensure the reliability of the companies that are active in the financial sector and the whole sector in general, and supervision over the performance of the established requirements. The activity licence requirement is established for credit institutions, creditors, and credit intermediaries who offer credit for consumers, payment institutions, e-money institutions, insurance companies, insurance brokers, investment firms, fund managers, investment funds founded as public limited companies, and the central register of securities. Special laws regulate the requirements established for companies active in

certain fields of activities in a detailed manner, however, very strict requirements are also established for the participants of the financial sector themselves in order to qualify for the activity licence. In addition to technical and financial readiness, the assessment pays great attention to the reputation and reliability of the company owners and board members of the sector (fit-and-proper requirements) and also sets requirements for key employees. Pursuant to the MLTFPA, all participants of the financial sector are obliged entities, which again sets specific obligations for the sector from the point of view of money laundering prevention. Thus, the assessment of regulations is high.

FSA, who among other functions is engaged in money laundering prevention, performs the role of a regulating body (except for small fund managers without an activity licence and financial institutions) – as at 2020 there are 7 full time supervisory officials specialised in the supervision of money laundering prevention. As at 2020, there are 113 full time employees at the FSA. The quality of supervision in this sector is high. The absence of administrative fines has adverse effects on the efficiency of supervision because it does not allow to establish proportional and efficient sanctions in the event of violations. The problem also lies in the amount of fine sums which do not correspond to the anti-money laundering directive of the European Union.

In addition to the supervisory bodies, professional organisations also contribute to supporting their members and prepare support materials for the performance of the requirements originating from the MLTFPA. The professional organisation joining the credit institutions is the Estonian Banking Association who contributes to the cooperation and training of its member companies. Non-profit association FinanceEstonia, a representative organisation of the financial sector that combines the interests of the public and private sector, has prepared guidelines for creditors and credit intermediaries for preparing risk assessments, which has also been approved by supervisory bodies. The Estonian Insurance Association has prepared the good practice of insurance and the sector has also to a certain extent regulated its activity with the articles of association of the Association and the self-regulation must be considered functional and additional, considering the level of detail of state regulation.

At the same time, payment institutions realize they do not have enough support from professional organisations and they are not sufficiently involved in the discussions related to the prevention of money laundering and terrorist financing. Small fund managers without activity licence, authorized by FIU, do not have a professional organisation who would clarify and form a uniform position on the topics related to money laundering prevention. They have also considered the informative work of the supervisory bodies to be insufficient.

Brief summary

Generally, the regulations and the quality of supervision in the sector is high. Professional organisations contribute to enhance the level of the regulations of the sector and to explanatory work by preparing guidance materials and organising training. However, there is still a small group of market participants who do not have a professional organisation (e.g., payment service providers) or where supervision has been insufficient due to a lack of resources (small fund managers without an activity licence), which needs more attention.

Efficiency of compliance control systems and reporting

The reporting requirements valid in the sector are established in special laws, based on which the market participants submit their reports to the Bank of Estonia and the FSA at the required intervals, where according to the data submitted the money laundering risk analysis is carried out in a service based manner.

Based on the survey results, the efficiency of the compliance control systems of the market participants can be assessed as follows:

- The sufficiency of the compliance control systems is evaluated on a regular basis[17].

[17] Based on the credit institutions, payment institutions, investment firms, life insurance companies survey results

- The monitoring systems of market participants with greatest impact are automated[18], generally the monitoring systems of other market participants are also automated according to the volume of services[19].
- By implementing a risk-based approach, economic crime detection systems are applied for the market participants with greatest impact[20].
- The selection and calibration of the scenarios of the transactions monitoring system are generally consistent with the profile of the unit and the related risks[21], however, for certain market participants there is a room for improvement in this regard, allowing real-time monitoring and stopping of transactions and being more risk sensitive[22].
- The monitoring systems of the transactions of market participants with greatest impact allow to identify certain complex or unusual transactions, but should still be more risk sensitive[23].
- For most market participants, a system which allows a risk-based calculation of the risk level of customers is used[24].
- The majority of market participants invest in the technical solutions of risk management – mainly in programmes and software[25].

Brief summary

Generally, the efficiency of compliance control systems and reporting is high[26].

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

General description of the due diligence measures

The MLTFPA sets out general due diligence measures, the application of which requires, as a general rule, at least the following:

- identification of the customer or a person involved in an occasional transaction and control of the data submitted,
- identification and control of the representative and the right of representation,
- identification of the beneficial owner and taking measures for identifying them in an extent which allows the obliged entity to make certain that they know who the beneficial owner is and understands the ownership and control structure, business relationships, occasional transactions, or operations of the customer or a person involved in the occasional transaction,
- obtaining information about the fact whether the person is a politically exposed person, their family member, or a person considered as a close co-worker, and monitoring of the business relationship.

The MLTFPA also stipulates special requirements which are to be implemented by credit and financial institutions in the meaning of the MLTFPA. For instance, the requirement for appointing a FIU contact person (§ 17 (2) of the MLTFPA), prohibition to create or continue correspondence with shell banks and such credit institutions or financial institutions that are known to allow shell banks to use their accounts (§ 18 (2) of the MLTFPA), requirements for identifying people with information technologic means (§ 31 of the MLTFPA), prohibition to provide services which can be used without identifying the person involved in the transaction and without controlling the information submitted, prohibition to open an account and keep it on behalf of the account owner, prohibition to conclude a contract or make a decision about opening an anonymous account, a savings book, or a safe-deposit box (§ 25 of the MLTFPA).

[18] Based on the credit institutions and payment institutions survey results
[19] Based on the fund managers, investment firms, life insurance companies survey results
[20] Based on the credit institutions and payment institutions survey results
[21] Based on the credit institutions and payment institutions survey results
[22] Based on the fund managers and investment firms survey results
[23] Based on the credit institutions, payment institutions, investment firms, life insurance companies survey results
[24] Based on the credit institutions, fund managers, payment institutions, investment firms, life insurance companies survey results
[25] Based on the credit institutions, payment institutions, investment firms, life insurance companies, creditors survey results
[26] Except for other financial institutions whose compliance control systems need assessment and development

Vulnerabilities identified during the survey on the quality of the customer control framework:

- absence of the register of PEPs; it is difficult to get to know PEPs, their family members, and close co-workers and to achieve the relevant and reliable quality of the monitoring thereof[27];
- lack of control over the data on beneficial owners when entering the data in the register and updating such data[28];
- the process of updating the information on beneficial owners does not correspond to the changing of the data of direct and indirect owners in the commercial register or in the central securities depository[29];
- availability of information on the BOs of non-resident legal entities from registers varies from country to country, the quality of the information varies or is controversial[30];
- access to the information regarding customers with high risk (e.g., embassies, virtual assets providers) is of uneven quality[31],[32];
- the biggest problem regarding the due diligence measures applied to customers by small fund managers without activity licence is determining the ring of customers to whom the due diligence measures should be applied in the first place. There is an understanding in the sector that the customers, they invest in, are small fund investors and not portfolio companies. In the light of the above, several due diligence measures are not applied to many persons (i.e., portfolio companies) who are actually subject to those measures, and the due diligence measures that are applied are not applied consciously. At the same time, each portfolio company is subject to a very thorough inspection, incl. a thorough and high-quality analysis of the business model of the portfolio company, i.e., instead of a formal and procedure-based approach, the due diligence measures are generally applied by using an approach where the customer is thoroughly inspected and analysed[33].

Brief summary

The quality of the due diligence measures framework is high. The biggest problems as regards customer control are the absence of a register of PEPs as well as the complexity of identifying the beneficial owner and a lack of reliable sources.

5.4.1.4. Assessment of sector-specific risks using the quality of sector-based controls

The following vulnerabilities were identified in analysing and assessing the sector-specific risks:

- complexity of identifying the abuse of embassy accounts for money laundering purposes[34],
- complexity of identifying the abuse of non-profit associations and charity organisations for money laundering purposes[35],
- complexity of identifying the cash flows related to human trafficking[36],
- complexity of identifying suspicious transactions related to virtual assets[37].

Brief summary

There are difficulties with the provision of specific services and identifying field-related risks. Awareness of risks related to advanced services and solutions is lower than desired.

[27] Based on the credit institutions, fund managers, payment institutions, life insurance companies, currency exchangers survey results

[28] Based on the credit institutions and fund managers survey results

[29] Result of the working group discussion based on the surveys

[30] Result of the working group discussion based on the surveys

[31] Based on the credit institutions survey results

[32] Result of the working group discussion based on the surveys

[33] Based on the small fund managers survey results

[34] Based on the credit institutions and payment institutions survey results

[35] Based on the credit institutions and payment institutions survey results

[36] Based on the credit institutions survey results

[37] Result of the working group discussion based on the surveys

5.4.1.5. Quality of response to risks identified during the previous assessments

During the previous assessments, it was found that the sanctions of the financial sector and the efficiency of the enforcement of the due diligence measures could be higher. To mitigate risks, the limit of sanctions related to money laundering has been increased in the MLTFPA, i.e., the maximum fine for violating the obligations is now 400,000 euros. However, the mechanism for imposing sanctions is still deficient with several and diverse problems.

It was also outlined that the beneficial owner is difficult to identify when ownership structures are complex. To mitigate the risk, Estonia has established a publicly available register under the commercial register in 2018, where business entities are obliged to submit the data regarding their BOs.

In money laundering crimes, computer fraud has been pointed out in the previous years as the widest and most high-risk area of money laundering. In relation to that, it was also referred that the assets obtained with the crime can be difficult to identify and difficult to distinguish from other assets. Therefore, subsection (4) has been added to § 213 of the Penal Code, pursuant to which the court may impose extended confiscation of assets or property acquired by the criminal offence, i.e., confiscate a part or all of the assets of the person who committed the crime, if there is reason to believe that the person obtained the assets as the result of the crime or at the expense of such assets.

In the 4th round of the Moneyval assessment, the areas focused on in this sector were the banking and securities sector and the topics mainly concentrated on the money laundering risks related to specific services. The FSA took note of the comments made and these are now being followed when performing on-site as well as remote checks.

The table below provides the main SNRA (2017/2019) findings and the related threats and vulnerabilities in the Estonian context, which are not covered in detail in the present chapter:

Table 24. Threats and vulnerabilities identified in SNRA (2017/2019) in the Estonian context

SNRA	Estonia's threats and vulnerability[38]
Private banking and institutional investments (especially through brokers) and safe custody services[39]	In Estonia, the requirements for becoming a private banking customer are very low. Therefore, special attention should be paid on private banking customers with higher value, the number of whom is small in Estonia. Substantially no private banking services are currently offered for non-residents. The threat level is average. Awareness exists and mitigation measures are implemented. Therefore, the vulnerability is low.
Use of 500 and 200 euro bank notes	The share of cash is low in the Estonian economy. Therefore, the risk is average. Awareness exists and risk mitigation processes are implemented. The vulnerability is low.
Professional football, corruption, and money laundering	In Estonia, football is not that highly valued or remunerated.
Free ports	There are free ports in Estonia but in practice their use for money laundering is not known.
Granting citizenship / residential permits for investments ("golden visas")	It is not known that the non-residents would prefer using Estonian residence permits because different requirements are applied and there is control over them. Similar opportunities of other countries are preferred.

[38] The assessments are based on the work results of the NRA financial sector working group

[39] Safe custody services include offering a safe deposit box or another secure storage room for storing the valuable items of customers

Human trafficking	Estonia is not very strongly represented as a potential target or transit country. We have had single cases where attempts were made to direct immigrants from Russia to Western Europe, however, these are just individual and unrelated cases.
Wildlife trafficking	No such cases have been identified in Estonia and the demand for exotic flora and fauna is unknown in Estonia.

5.4.1.6. Conclusion

On a scale of 1 to 5, the financial sector vulnerability level from the aspect of money laundering is 2.69, i.e., **below average**.

Table 25. The level of money laundering vulnerability in the financial sector

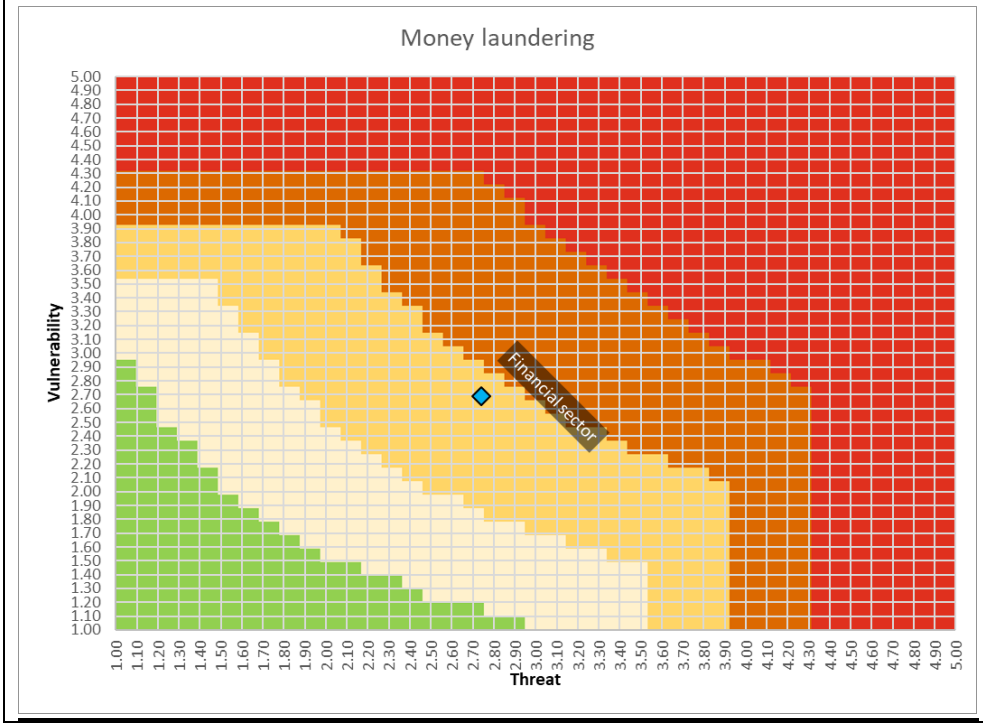
Sector	The level of money laundering vulnerability at the sectoral level	
Financial sector	2.69	**average/low**

The strengths of the sector include good supervision over the sector participants with an activity licence obligation and a strong legal framework. The large-scale wave of money laundering scandals that hit the Estonian banks has also played an important role here, since the necessary lessons were learnt and the respective systems became more efficient.

As regards supervision, the most vulnerable sections are supervision over small fund managers without activity licence and other financial institutions (i.e., entities supervised by the FIU), from which it can be concluded that the awareness of the market participants of this sector needs to be raised within the sector.

In terms of the implementation of due diligence measures, the weak spots include the reliability of the register of BOs and access to the information related to PEPs both nationally as well as internationally. This aspect needs to be resolved at the national level.

Figure 4. Heat map of the money laundering risk level of the financial sector



Summary

The vulnerability level of the sector on the national map is placed in the middle of other sectors and assessed to be below average. Therefore, the vulnerability of the financial sector to money laundering can be considered acceptable, however, there are market participants whose awareness of money laundering prevention needs to be raised. Nevertheless, for certain market participants there is room for improvement to enhance their capability, allowing real-time monitoring and stopping of transactions. Due diligence measures must be applied in the sector as usual.

5.4.1.7. Risk management strategy

5.4.1.7.1. Mitigating measures at the national level

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

- creation of a database for politically exposed persons;
- intervention/supervision exercised by the FIU must be improved for market participants acting under an FIU activity licence;
- the commercial register: organisation of information related to BOs (100% of the BOs are registered), control (the data corresponds to reality) and tightening and updating of the respective sanctions (changing the legislation). Connecting shareholding with the BOs;
- in the long perspective, the data necessary for the implementation of due diligence measures could be available in one portal;
- establishment of a strategic analysis centre, the work results of which would be shared with the market participants (preparing analyses based on domestic as well as international information)[40];
- to provide obliged entities with the information necessary for the performance of due diligence measures from the state registers free of charge;
- alleviate the legal framework by introducing the following exemption: the payment transactions of electronic communication service users are excluded from among the obliged subjects and from among the notion of financial institutions in the meaning of the MLTFPA, which the electronic communication company performs (in addition to the provision of electronic communication services) if the volume of the respective payments for one user does not exceed 1,000 euros in a month;[41]
- potential loosening of the customer identification and verification requirements, bringing these into line with internationally implemented requirements:
  Identification and verification of identity in the fight against money laundering and terrorist financing ensures that obliged entities are aware of the identity of the customer who consumes their services or performs the official activities. At the same time, in the economic meaning this is a product/measure the production of which is subject to the law of diminishing marginal utility, according to which the first produced unit of goods/services is with the highest utility, whereas with every next produced product unit the utility decreases and reaches a point where the utility of the consumption of the produced unit is smaller than the cost of the product unit. In other words, the resources spent on implementation of the customer identification and verification requirements do not bring much utility to fighting against money laundering and terrorist financing at some point, but are economically costly and prevent competition.
  The anti-money laundering directive and the guidelines of the Financial Action Task Force (FATF) give the member states an opportunity to determine the reliability of the identification of both physical persons as well as the representatives of legal entities and the content of the independent source on their own.

[40] The sharing of the results with the market participants takes place at a level which eliminates the possibility of information leaks about cases which are or are intended to be included in offence proceedings.

[41] A respective analysis has been carried out, according to which the threats of money laundering and terrorist financing among the communication services providers is close to zero and there is no vulnerability. The risks have been assessed and it can be concluded that the services provided by communication service providers cannot be compared to those offered by other financial institutions.

During the present risk assessment, no general threat or risk has been identified, which is related to the non-performance of the requirements related to the identification and verification of the customer. Also, the group works of the sector or the conducted surveys have not identified any vulnerabilities related to the identification of persons. There are no real cases to show where wrong identification of the identity of the customer has meant that the customer was laundering money. On the contrary, too strict identification requirements hinder the competition and service provision and therefore force the actual criminals to use non-regulated services, which diminishes the opportunity to detect money laundering and terrorist financing. The supervisory authorities are also aware of cases where obliged entities give up providing services in Estonia because the identification requirements prevent the provision of the service. This is a serious threat to the competitiveness of Estonia and promotes using the services of non-regulated companies, i.e., force the service provision to go "underground". In the light of the above, during the NRA it was concluded that the identification requirements should be reviewed as a whole in order to avoid unnecessary complexity, however, still properly managing the risks with a solution which can actually identify and manage the risks. To conclude, the solutions for verifying the data collected during identification must be reviewed and brought into line with the actual risk and the international practice, i.e., the choice of a reliable and independent source should be left to the risk-based decision of the obliged entity.

- to establish administrative fines for improving supervision and to bring into line the fine rates with the EU anti-money laundering directive. This would allow the FSA as the supervisory authority to implement proportional and effective sanctions.

5.4.1.7.2. 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:

- raise awareness of money laundering typologies and scenarios through training and discussions with the FIU;
- raise the awareness of the sector through training and round tables organised by the supervisory authorities;
- improve cooperation between the professional association and payment services providers;
- improve cooperation between the professional association and small fund managers without activity licence. The representative organisations could bring together the whole sector in order to bring together all sector participants into a uniform information field and thus mitigate the risks related to single sector participants and increase the awareness of the sector of the risks related to money laundering through sector-based round tables and discussions.

5.4.2. Vulnerabilities of prevention of terrorist financing

5.4.2.1. Exposure to threat

- Insufficient awareness of financial service providers and the related insufficiency of the due diligence measures implemented against terrorist financing. The results of the survey conducted among the market participants during the NRA indicate that due to the complexity of the typologies of terrorist financing, the market participants experience difficulties in creating terrorist financing scenarios.
- Threat associated with payment intermediaries and virtual assets. The maximum point of exposure the threat for the market participants of the financial sector is the provision of intermediation payment and virtual assets services. The results of the survey "Survey on Virtual Assets Service Providers (VASPs)" conducted by the FIU indicate that as at 1 August 2020, there were a total of 611 valid virtual assets service provider activity licences (295 service licences for exchanging VA for money, 261 for wallet service, and 55 VA service licences)[42]. The results of the survey also indicate that the total turnover of the services of virtual assets service providers active in the Estonian market has grown rapidly. While in 2018 it was approximately 590 million euros, in the first half of 2019 it was already twice as much – 1.2 billion euros. In terrorist financing, the main threat is also mainly related to the cross-border payment service providers – the responses regarding the volume of the services provided for Estonian residents from year 2017 (asked in the framework of the NRA) indicate that the respective figure totals 250 million euros.

5.4.2.2. Risk awareness

Management commitment and leadership

Survey results regarding awareness

The results of the survey conducted in the framework of the NRA indicate that the awareness of the sector about terrorist financing prevention is above the average level[43]. The reason for this is the existence of the guide by the FIU and the training organised by the FIU and the Estonian Internal Security Service. However, due to a lack of practical cases, the level of awareness only remains theoretical.

The sector is modest in performing its reporting obligation – in 2019, the credit institutions submitted two reports of terrorist financing to the FIU (in 2019, the total number of terrorist financing suspicion reports submitted to the FIU was 4).

To conclude, it can be said that the awareness of the financial sector about terrorist financing is at a very good level, whereas the management contributes to further increasing the awareness. The modest performance of the reporting obligation is more related to a lack of grounds for reporting.

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

Quality of supervision

In the financial sector, the level of regulations is very high. The special laws applicable to the sector participants stipulate the requirement of an activity licence for the majority of the financial services providers, which helps to ensure the reliability of the companies active in the financial sector as much as the whole sector, and supervision over the performance of the established requirements. Pursuant to the MLTFPA, all participants of the financial sector are obliged entities, which again sets specific obligations for the sector from the point of view of terrorist financing prevention. Thus, the assessment of regulations is high.

The FSA has the role of the regulating body (except for the small fund managers without activity licence and financial institutions). The rights and competences of the FSA when exercising supervision are

[42] According to the register of economic activities, as at 31 Dec 2020, there were a total of 478 valid activity licences issued for VA service providers (39 service licences for exchanging VA for money, 34 for wallet service, and 405 VA service licences).

[43] Based on the credit institutions survey results

extensive and in accordance with the necessity for ensuring the efficiency of the regulations of the sector. The quality of supervision in this sector is high.

Efficiency of compliance control systems and reporting

The reporting requirements valid in the sector are established in special laws, based on which the market participants submit their reports to the Bank of Estonia (Eesti Pank) and the FSA at the required intervals. Based on the data submitted to the FSA, the money laundering risk analysis is carried out in a service-based manner.

Based on the survey results, the efficiency of the compliance control systems of the market participants can be assessed as described below.

- The sufficiency of the compliance control systems is evaluated on a regular basis[44].
- The monitoring systems of the most market participants with greatest impact are automated, generally the monitoring systems of other market participants are also automated based on the volume of services[45].
- The selection of the scenarios of the transactions monitoring system and the calibration are generally coordinated with the profile of the unit and the related risks[46], however, for certain market participants there is room for improvement in this regard, allowing real-time monitoring and stopping of transactions and being more risk sensitive[47].
- The transaction monitoring systems of market participants with greatest impact allow to identify certain complex or unusual transactions[48] but should still be more risk sensitive. Developing specific terrorist funding scenarios is problematic due to their complex nature[49].
- For most market participants, a system which allows the risk-based calculation of the risk level of customers is used[50].
- The majority of market participants invests in the technical solutions of risk management – mainly in programmes and software[51].

Brief summary

Generally, the efficiency of compliance control systems and reporting is high in the sector, although problems occur with the developing of specific terrorist financing scenarios due to their complex nature.

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

Vulnerabilities identified during the survey on the quality of the customer control framework:

- the information in the state registers regarding the BOs is not always reliable[52];
- access to information necessary for identifying BOs is difficult[53];
- access to information necessary for identifying and verifying other high-risk customers (e.g., embassies, virtual assets providers, companies providing money services, non-profit associations, etc.) is difficult[54].

[44] Based on the credit institutions, payment institutions, investment firms, life insurance companies survey results
[45] Based on the credit institutions, payment institutions, investment firms, life insurance companies survey results
[46] Based on the credit institutions and payment institutions survey results
[47] Based on the fund managers survey results
[48] Based on the credit institutions and payment institutions survey results
[49] Based on the fund managers and payment institutions survey results
[50] Based on the credit institutions, fund managers, payment institutions, investment firms, life insurance companies survey results
[51] Based on the credit institutions, payment institutions, investment firms, life insurance companies survey results
[52] Based on the credit institutions, fund managers, payment institutions, life insurance companies, currency exchangers survey results
[53] Based on the credit institutions, fund managers, payment institutions, life insurance companies, currency exchangers survey results
[54] Based on the credit institutions, payment institutions, creditors and other financial institutions survey results

Brief summary
The quality of the due diligence measures framework is generally high. The biggest problems as regards customer control are the absence of the register of PEPs as well as the complexity of identifying the beneficial owner and a lack of reliable sources.

Quality of identification of sector-based international sanctions
Vulnerabilities identified during the survey on the quality of identification of international sanctions:

- mechanisms for detecting the evasion of sanctions are not always efficient (e.g., due to the data quality problem of the lists)[55],[56];
- awareness of applicable sector-based sanctions and the implementation thereof is not sufficient for all market participants[57];
- mechanisms for freezing the assets are not always efficient[58].

Brief summary

The quality of determining international sanctions is generally high. The biggest problem lies in the data quality and identity of the information in the lists of sanctions.

5.4.2.4. Assessment of sector-specific risks using the quality of sector-based controls

The following vulnerabilities were identified in analysing and assessing the sector-specific risks:

- problematic detection of companies providing money services that facilitate terrorist financing[59];
- complexity of identifying the abuse of consumer loans and small value loans for terrorist financing purposes[60];
- complexity of identifying the abuse of embassy accounts for money laundering or terrorist financing purposes[61];
- complexity of identifying the abuse of non-profit associations and charity organisations for money laundering or terrorist financing purposes[62],
- complexity of identifying suspicious transactions related to virtual assets[6364].

Brief summary
The quality of sector-based risk assessment is generally above average. The problem lies in the lack of terrorist financing scenarios due to the diverse and complex nature of terrorist financing.

5.4.2.5. Quality of response to risks identified during the previous assessments

In the financial sector, terrorist financing assessments as a whole have been rather deficient in the past.

The constituent elements of a criminal offence of terrorist financing were found to be somewhat deficient. The qualification of terrorist financing was amended in 2019 (§ 5 of the MLTFPA and § 237.3 and 237.6 of the Penal Code).

[55] Based on the fund managers and currency exchangers survey results
[56] Result of the work of the working group
[57] Based on the fund managers, payment institutions, creditors and other financial institutions survey results
[58] Based on the credit institutions, fund managers, payment institutions, investment firms, creditors, and other financial institutions survey results
[59] Result of the work of the working group
[60] Result of the work of the working group
[61] Based on the credit institutions and payment institutions survey results
[62] Based on the credit institutions and payment institutions survey results
[63] Based on the fund managers and payment institutions survey results
[64] Result of the work of the working group

As regards this sector, SNRA (2017/2019) found that "small loans in the context of terrorist financing are a potential threat" across Europe. It is relevant to mention that in Estonia no such cases have been identified. The levels of threat and vulnerability are low.

5.4.2.6. Conclusion

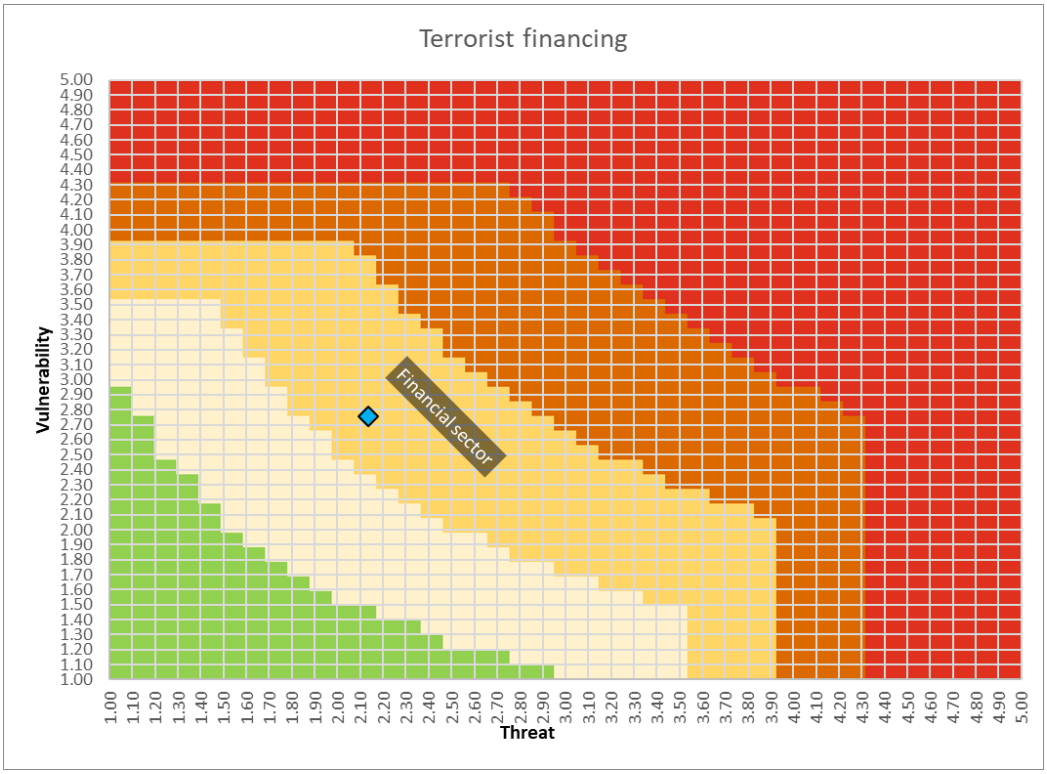
On a scale of 1 to 5, the financial sector vulnerability level from the aspect of terrorist financing is 2.75, i.e., **average-low**.

Table 26. The level of terrorist financing vulnerability in the financial sector

Sector	The level of terrorist financing vulnerability at the sectoral level	
Financial sector	2.75	**average/low**

Since the level of terrorist financing vulnerability is low, improving the efficiency of regulations or supervision is probably irrelevant for this sector for the reason stated above, and focus should be targeted on maintaining the achieved level.

Figure 5. Heat map of the terrorist financing risk level of the financial sector



Summary

The vulnerability level of the sector on the national map is placed in the middle of other sectors and assessed to be **below average**. Therefore, the focus should be on developing a larger number of scenarios for terrorist financing and on maintaining the level of supervision. Due diligence measures must be applied in the sector as usual.

5.4.2.7. Risk management strategy

5.4.2.7.1. Mitigating measures at the national level

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

- Performing full-scale periodic monitoring of customer bases of virtual assets service providers and/or creating a database of customers (customer + contact data), informing credit and payment institutions.

5.4.2.7.2. 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:

- training and discussions on terrorist financing typologies and scenarios together with the FIU and the Estonian Internal Security Service.