4.1. The national vulnerabilities

Figure 2. The risk level of money laundering at the national level

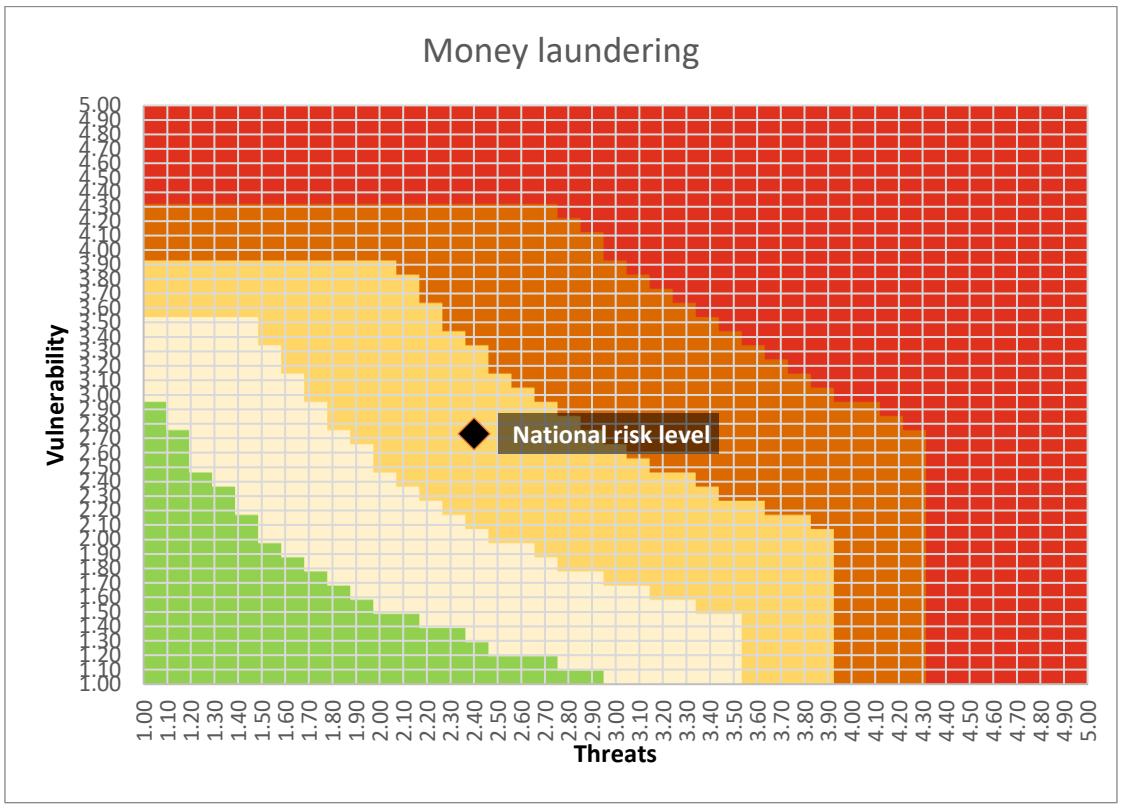
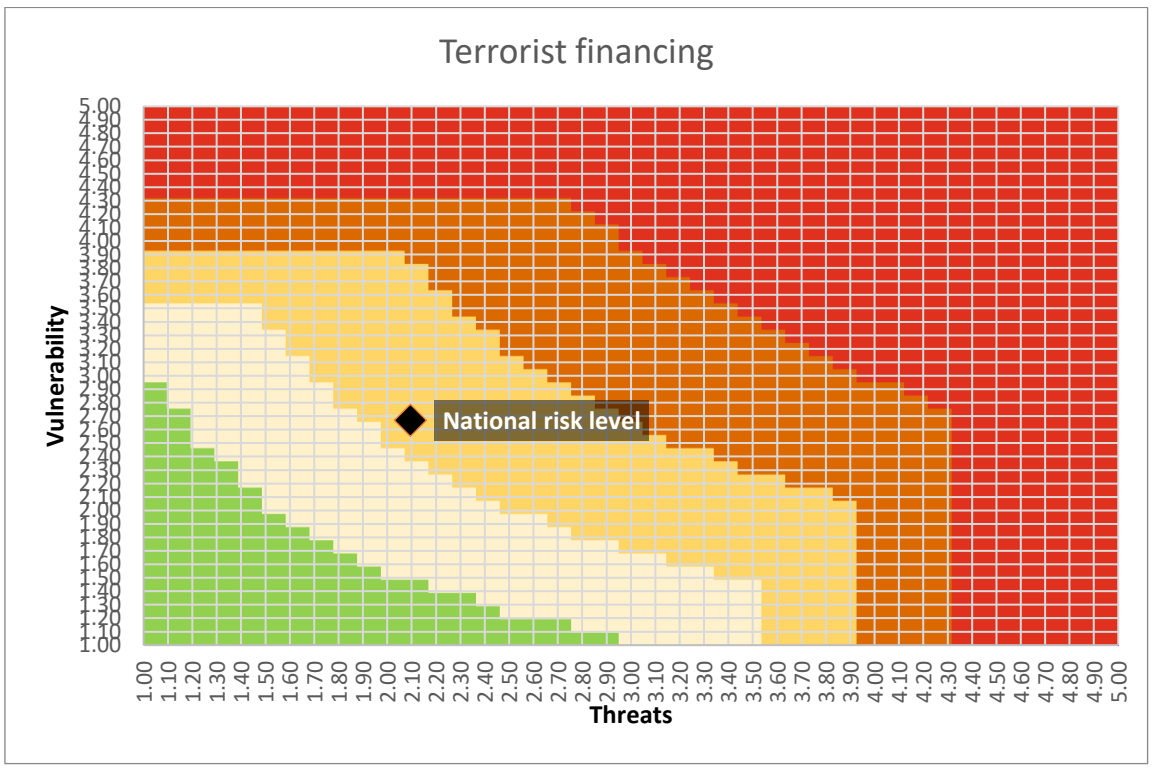


Figure 3. The risk level of terrorist financing at the national level



4.1.1. National money laundering vulnerabilities

1. Policymaking and application

The aim of the state is for the policies, coordination, and cooperation to decrease the risks of money laundering and terrorist financing. The Money Laundering and Terrorist Financing Prevention Act which entered into force in 2017 establishes the general framework, including the activities of obliged entities, the cooperation and coordination within the state – with the preparation of the National Risk Assessment at its fore.

As there is a clear legal obligation to draw up a risk assessment, including with consideration to the results of the European supra-national risk assessment, a governmental committee has been formed to resolve all coordination and cooperation issues. The obliged entities also have a statutory duty to take the published results of the National Risk Assessment into account[1]; the organizational framework of policymaking and application has been regulated at the legislative level, transparent, in compliance with international standards and EU law, and the application thereof is also easy to monitor. The aforementioned points have a definite alleviating influence on the vulnerability of the state and have a major impact on the vulnerability assessment of this aspect.

The political will and support to fighting money laundering is apparent in the statements of the top state officials, the wording of the coalition agreement, as well as the decisions made during the negotiations of the state budget – additional resources have been directed into reinforcing the prevention of money laundering in 2019, 2020 as well as 2021. At the same time, there is no common approach across political parties, nor a consensus regarding the importance and prioritization of the issue, therefore it would be arbitrary to conclude that such a political will and support would always be ensured unconditionally and in every situation. Therefore, the existence of certain vulnerabilities regarding political will and support cannot be entirely ruled out, negatively influencing the assessment of these aspects.

The national strategy and policy of money laundering prevention[2] are not currently clearly worded nor updated. To a notable extent, national development plans (for example the internal security development plan[3]) also contain references to the areas of money laundering prevention, but not across all aspects and not specifically. The lack of such a strategic and/or political document has a certain negative impact on the vulnerability of the state. The results of this National Risk Assessment shall be considered as a nationwide strategic and political document, as an action plan containing specific activities and goals will also be created on the basis of this National Risk Assessment.

For the reasons listed above, the overall assessment of the vulnerability pertaining to money laundering policy and coordination activities is low (1.4).

2. International cooperation in criminal matters

As a result of the analysis conducted when drawing up this National Risk Assessment, it was concluded that an adequate legal framework has been established in Estonia, creating the foundation for productive international cooperation. Productive international cooperation is possible first and foremost via mutual legal assistance requests and European Investigative Orders, and Estonia is an active user of both of these channels. The existing legal framework also allows for coordination of activities with colleagues from other countries via the option of forming international investigation teams. There is active[4] use of such

[1] MLTFPA §§ 11, 12, and 13.
[2] Due to the NRA 2020 methodology, money laundering and terrorist financing are also addressed separately in this chapter in order to highlight the differences in assessed vulnerabilities. This does not indicate a conclusion that it would be prudent to handle the issues of money laundering and terrorist financing separately in practice. Any aspects supporting such a conclusion were not identified in Estonia.
[3] https://www.siseministeerium.ee/et/STAK2030
[4] Enquiries of Europol, Interpol (incl. Sirene data) via PPA that contain a reference to proceedings related to money laundering:

international law enforcement networks as Egmont[5], Interpol, Europol, Sirene, Eurojust, and the police also have their own communication channels for cooperation (SIENA – for sharing intelligence). Also, there is active cooperation with the communications officers of the law enforcement units of partner states. In addition, we use CARIN, an EU and global network of offices for identifying criminal proceeds. Cooperation always occurs when it is for the benefit of the proceedings and there is a need to cooperate with foreign law enforcement facilities in order to gather proof of a criminal offence or identify the movement of assets[6].

European Investigative Orders (EIO) and mutual legal assistance requests (MLA) drawn up in the Republic of Estonia and issued to the Republic of Estonia in relation to proceedings regarding money laundering crimes between 2017-2019:

Table 9. Statistics on EIOs and MLAs related to money laundering proceedings in 2017-2019

	Received by the Republic of Estonia		Sent by the Republic of Estonia		
	EIO	MLA	EIO	MLA	
2017	12	55	1	15	
2018	35	2	11	2	
2019	65	3	39	22	

The statistics of European Investigative Orders and mutual legal assistance requests show that the primary partners in international cooperation use the EIO framework, wherein the number of MLAs sent from Estonia is roughly equal to the number of EIOs sent from Estonia in 2019. Therefore, Estonia is seeking for active cooperation outside of the European Union, while the primary interest in information held by Estonian law enforcement entities when talking about proceedings in money laundering offences is within the European Union. Refusals to cooperate internationally occur only in justified cases, an overview of which is in the following table:

Table 10. Statistics of cases of refusal in international cooperation

	Estonia refused		The executing state refused		Average due date of execution (in days)	
	EIO	MLA	EIO	MLA	EIO	MLA
2017	2	7	2	1	80	46
2018	5	2	1	0	42	

	2019	2018	2017
To Estonia	946	713	523
From Estonia	471	504	327

[5] Egmont Secure Web is a tool of the FIU, more information about the FIU's cooperation with other countries is available in the FIU's Yearbooks: https://www.fiu.ee/aastaraamatud-ja-uuringud/aastaraamatud

[6] The Tax and Customs Board is also involved in international cooperation, including in criminal matters – there is no statistical data regarding the types of crime from this unit but 90% of all enquiries are concerned with tax crimes.

2019[7]	4	NA	NA	NA	45	148

The Republic of Estonia has refused to execute the EIOs and MLAs of foreign countries for different reasons (i.e. the applying country does not reply to additional questions within a year; the translation cannot be understood; the person regarding whom the execution of proceedings is requested is not in the Republic of Estonia or is in a state of mental incompetence; the requesting country has used the wrong instrument, such as it should have used an European Arrest Warrant; the due date of the requested proceedings was impossible to adhere to). In case of basis for refusal, the Office of the Prosecutor General first initiates consultations with the requesting country for rectifying the issues and upon refusal to comply with MLAs or EIOs, the document stating the grounds of refusal is also always sent to the requesting country.

The implementation became obsolete in two MLAs drawn up in the Republic of Estonia in 2017 due to the entry into force of a court judgment, thus Estonia sent a relevant notice to the implementing country. The other case where implementation became obsolete regarding an MLA, a joint investigation team (JIT) was formed with the implementing country. In 2018, an implementing country refused to execute an EIO sent by the Republic of Estonia due to the fact that another country had already sent information regarding the same issue. The remaining MLAs and EIOs were all executed.

The internal coordination mechanisms of international cooperation and the enforcement thereof are efficient and allow Estonia to offer substantial and valued cooperation to international partners, therefore the level of international cooperation has an impact decreasing the overall national vulnerability. There were no legislative issues identified as the law provides for sufficient measures to carry out international cooperation. Obviously, effective cooperation also requires the application of similar principles and measures by the international partners, so that the cooperation would also bear the desired fruit in practice. The inevitable complexity and difficulty of international cooperation is largely down to factual circumstances. In practice, problems arise in international cooperation due to the fact that sending and responding to MLA requests is a time-consuming process. Receiving information about circumstances requested in the first MLA request is often the basis from which to ask additional information from the requesting country. As international cooperation with other countries is already time-consuming by nature, sending consecutive letters extends this process even more. Money laundering proceedings are often very large and the initial focus on the proceedings of another country also takes resources in order to figure out what kind of information the other country wants. Another problem arises with politically sensitive proceedings, namely that countries may want to keep certain information to themselves and are not always willing to cooperate in a transparent manner. As money laundering is a severe covert crime by nature, international cooperation is complicated by the fact that criminals are attempting to hide all information that is of interest to law enforcement authorities. What also has caused problems in practice are cases where the investigated predicate offence is not criminalized in the other country which therefore refuses to cooperate.

When assessing the vulnerability of cooperation mechanisms from the point of view of the Estonian legal framework and the organizational side of authorities, the overall assessment of vulnerability is low (0.6).

Issues arising from the cooperation mechanisms of other countries cannot be influenced by improving further the Estonian cooperation mechanisms, therefore it is proposed to amend the Penal Code with a separate clause providing for a punishment for violation of duties related to money laundering prevention in order to decrease the impact of vulnerabilities arising from the problems described above, by establishing a criminal liability for failure of an obliged entity to knowingly apply measures of due diligence and rules of procedure. This measure also allows to mitigate vulnerabilities related to the capabilities of supervisory authorities (see the next section of this chapter).

[7] At present, 12 LRs and 28 EIOs of those drawn up in the Republic of Estonia in 2019 have been executed. As international cooperation in criminal matters is often time-consuming, more responses may still arrive.

3. Capability of supervisory authorities

Pursuant to the MLTFPA, supervision over the performance of requirements established in the MLTFPA and acts established on the basis thereof is exercised by the Financial Intelligence Unit (FIU), the Financial Supervision Authority, the Board of the Estonian Bar Association, and the Ministry of Justice, which has delegated supervision to the Chamber of Notaries pursuant to Notaries Act § 44 (1) 1^1) and (2) 3^1). The Financial Intelligence Unit supervises the subjects that have been granted an activity licence by the FIU. The Bar Association supervises the professional activities and the performance of requirements of professional ethics of the members of the association and foreign attorneys operating in Estonia. The Chamber of Notaries supervises the performance of requirements established in the MLTFPA and legislation established thereunder by notaries. The Financial Supervision Authority performs state financial supervision of banks, life insurance companies, insurance brokers providing life insurance, investment associations, fund managers, investment and pension funds, payment institutions, e-currency institutions, creditors, and credit intermediaries, and the central securities depository, which have received an activity licence from the Financial Supervision Authority. Branches of banks, creditors, insurance companies, and investment associations are supervised across the group by the supervisory authorities of the country of location of that bank, insurance company, or investment association. Supervision of money laundering and terrorist financing prevention over structural units in another member state is efficient, as evidenced by the invalidation of the operating licences of the Estonian branch of Danske Bank A/S and Versobank AS (due to their branch operating in Latvia partly illegally). In order to ensure that the money laundering and terrorist financing prevention requirements are followed, in addition to day-to-day communication with the supervisory authorities of other countries, the Financial Supervision Authority has concluded several cooperation agreements for supervisory cooperation over banking groups. For example, the cooperation agreement between Nordic countries: *Memorandum of Understanding on Cooperation and Coordination on cross-border financial stability between relevant Ministries, Central Banks, Financial Supervisory Authorities and Resolution Authorities of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden.* The Financial Supervision Authority is a permanent member of various colleges of foreign credit institutions with Estonian branches.

The Financial Supervision Authority, the Board of the Bar Association, the Ministry of Justice, and the Chamber of Notaries cooperate with the Financial Intelligence Unit, sharing information both at an operative and at a strategic level. The Financial Intelligence Unit and the Chamber of Notaries also exchange information about reports forwarded by notaries. An overview of the reports made is currently provided annually. The Financial Intelligence Unit and the Financial Supervision Authority also cooperate with other competent authorities such as the Police and Border Guard Board, the Tax and Customs Board, the Internal Security Service, and the Prosecutor's Office.

The supervisory authorities have identified risks related to money laundering and terrorist financing in sectors which they supervise: the instruction materials and training of the Financial Intelligence Unit highlight a risk-based approach and solutions for execution[8]. The instructions of the Chamber of Notaries specify the principles of risk assessment which the notaries can utilize in their work. The Financial Supervision Authority has developed a set of recommendations on the *Organizational solution for credit and financing institutions and preventive measures for the prevention of money laundering and terrorist financing*, which address the identified risks of money laundering and terrorist financing and provide for the necessary preventive measures.

In general, the activities carried out, guidance developed and the preventive work done by supervisory authorities have been efficient and in proportion with the tasks and responsibilities of the authorities. However, handling the changing conditions has been challenging – both the increased number of subjects of supervision and the changing legal environment. It has been necessary to increase the number of officials performing supervision in order to ensure it. For example, the supervisory resources of the Financial Intelligence Unit have grown from three to ten employees over two years (2017-2019)[9]. The

[8] The guidance issued by the Financial Intelligence Unit: https://fiu.ee/oigusaktid-ja-juhendid/juhendid

[9] The number of supervision subjects of the FIU cannot be uniformly assessed as several types of obliged entities qualify as subjects based on transactions (i.e., when handling a certain amount of cash). As of 31 December 2019, there are approximately

Bar Association deploys 1.3 positions for money laundering and terrorist financing prevention supervision[10], the Chamber of Notaries has 1 dedicated position since 2019[11]. On 1 January 2021, the Financial Intelligence Unit was moved under the Ministry of Finance as an autonomous authority so that the planned budget of 2021 of the Financial Intelligence Unit without the expenses of the IT department is 3.1 million euros, thereby more than doubling the budget of the authority in comparison with the year before. The Financial Intelligence Unit used to hold 32 positions, which grew to 47 in the new year, meaning that the number of employees will also grow by nearly a half.[12] In 2018, a strategic analysis unit was created within the structure of the Financial Intelligence Unit, based on which a strategic analysis department is being formed in 2021. At present, the Financial Intelligence Unit uses the RABIS[13] database in its daily operation, which is efficient in terms of managing received reports, although still in need of development. Significant information system developments are also planned for 2021. As the function of strategic analysis is developed, the IT resources of the Financial Intelligence Unit are equipped with relevant technological solutions.

The Financial Supervision Authority had 3 positions allocated to money laundering and terrorist financing prevention supervision in 2017, 4 positions in 2018 (as at 31 December 2018, the Financial Supervision Authority employed 91 people). In 2019, a separate department was formed in the Financial Supervision Authority for improved supervision of money laundering, at which 7 persons worked at the end of the year (as at 31 December 2019, the Financial Supervision Authority employed 100 people). In addition, other structural units have been involved in money laundering prevention in the Financial Supervision Authority, including the legal department (fit-and-proper assessment, second opinion, withdrawal of an activity licence), capital supervision department (assessing operating risks, carrying out SREPs) and the enforcement department. The budget of the Financial Supervision Authority has also been growing steadily (from 6,675,000 euros in 2017 to 7,286,000 euros in 2019).
In money laundering and terrorist financing prevention supervision, the Financial Supervision Authority uses internally developed risk analysis solutions as well as a technological solution created on the basis of the SAP software to monitor risks. The Bar Association has 1.3 positions allocated to the topics of money laundering and terrorist financing prevention supervision in 2019. The Ministry of Justice has 2 supervisory officials. The Chamber of Notaries has 1 supervisory official, the dedicated position of money laundering and terrorist financing supervision was created in 2019.

An additional 1.6 million euros was allocated to the field of money laundering and terrorist financing prevention in the state budget of 2019, used to improve the efficiency of the PBGB's economic crimes unit (a separate financial investigation unit), criminal proceeds identification unit, and to recruit additional FIU officials.

Even though the lack of resources of supervisory authorities could be criticised at the start of the period under scrutiny (2017 and earlier), the significant increase in resources allocated in recent years has remarkably improved the situation and the increase of resources, incl. hiring additional officials is intended to continue in the coming years. In summary, the capability of supervisory authorities has increased in recent years and it can be said that supervisory authorities monitor, control and regulate the operation of credit and financing institutions and non-financial institutions and professions to their capacity, in order to ensure their compliance with the requirements of money laundering and terrorist financing prevention. Even though the growth of human as well as other resources has been significant and Estonian supervisory authorities have taken a large step forward in the process of increasing capability, the further growth of resources as well as (IT) development activities must continue for even more efficient supervision. Continued attention must be paid to the application of risk-based supervision

66,063 natural and legal persons subject to the supervision of FIU.

[10] The number of supervision subjects as at 1 October 2020 was 219 law firms with 1095 attorneys in Estonia and one operating attorney per 1,545 residents.

[11] The number of supervision subjects is stable: 2017 – 91 notaries, 2020 – 89 notaries.

[12] https://www.rahandusministeerium.ee/et/uudised/rahapesu-andmeburood-ootab-2021-aastal-ees-kiire-kasv

[13] The FIU information system RABIS, adopted in May 2019, allowed to switch to completely digitized report processing in the work of the FIU. A system development is undergoing in 2021, granting more modern tools to the analyst for more efficient proceedings.

principle by supervisory authorities, except for the Financial Supervision Authority (which already fully applies risk based supervision): the present NRA assessment is also a part of it. From the previous statements, the sector of virtual currencies stands out as problematic, as both the legal environment and the organization of supervision are currently in a state of development and progress, and which is significantly increasing Estonia's vulnerability to money laundering in its existing form from the aspect of the capability of supervisory authorities.

The sanctioning options for discovered violations also influence the capability of supervisory authorities, wherein the complexity of addressing misdemeanours in practice is considered to increase vulnerability. Various proposals have been made in 2019-2020 to address this issue[14]. The necessary amendments must be entered into force to decrease national vulnerability.

Law enforcement authorities have, for instance, information about persons who are probably offering money laundering services (e.g., offering the service of founding and managing companies and the use of transit accounts). The amounts of money received abroad, accepted and used for transactions, often indicate at least suspicious origin, but Estonia has no information about predicate offences where the money might come from. At present, persons offering such business cannot be convicted based on existing penal norms, as law enforcement authorities cannot indicate which criminal activities the money originates from. At the same time, the activities of such persons endanger the national economic and internal security environment. Therefore, the Penal Code should be amended with a separate clause punishing for violating obligations related to money laundering, establishing a liability for knowing disregard of an obliged entity to exercise due diligence measures and procedural rules.

The overall assessment of vulnerability arising from the capabilities of supervisory authorities is low (1.5), except in the context of the vulnerability arising from the supervisory capability of the virtual currency sector, which calls for immediate application of concrete counter measures.

4. Reporting suspicious transactions and use of preventive measures

§§ 49 and 50 of the MLTFPA place a reporting duty on all obliged entities specified in § 2 of the MLTFPA in case of suspicion of money laundering. The reporting duty can be performed electronically via an online form or the X-Road service. If the person has no such options, they can also send an e-mail to the Financial Intelligence Unit as a last measure and the information received is registered as a report. There are also instructions regarding the format and filling of the report issued by the Financial Intelligence Unit[15]and the website of the Financial Intelligence Unit contains guidelines on indicators of suspicious transactions, helping an obliged entity in submitting a report.[16]

As preventive measures for money laundering, the MLTFPA specifies the management of risks related to money laundering and terrorist financing (chapter 2) and the application of due diligence measures (chapter 3).

One vulnerability is low awareness of various sectors[17] of requirements for the prevention of money laundering. Not all obliged entities have a proper organisational set-up and insufficient resources are directed into applying these requirements.

The largest risk is the sector of virtual currency service providers, where the performance of the reporting obligation is lacking in comparison with potential transaction volumes in this sector. According to a survey conducted by the Financial Intelligence Unit in 2019[18], the turnover of this sector has grown from

[14] Drafts being processed by the Parliament: 111SE (reform of misdemeanour punishment in the field of finance); 94SE (amendments to the Penal Code, fines pursuant to EU law); the draft of the Administrative Fine Proceedings Act: https://eelnoud.valitsus.ee/main/mount/docList/e0350345-d819-4adc-bc56-37594d5f815f

[15] https://www.riigiteataja.ee/akt/112022020019;

[16] https://fiu.ee/oigusaktid-ja-juhendid/juhendid

[17] Also see chapters on sectors where the awareness of sectors is addressed separately.

[18] https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b

the 590 million euros in 2018 to 1.2 billion euros in the first half of 2019. At the same time, the number of employees who should be involved in applying preventive measures has only grown from 102 to 152 employees during this period. The total number of market participants has dropped from 1234 in 2019 to 353 (as at August 2020), but is still significant. In 2018-2019, this sector sent reports primarily from three companies and most of them are related to refusal to engage in a client relationship. In 2020, reports on suspicious transactions have also been added but the volumes are not large. At the same time, the number of reports has increased to 492 in 2020 (as at 14 December 2020, 8 in 2018, 400 in 2019) and some new market participants have started to send reports. However, in comparison with the turnover volumes and number of obliged entities in this sector, the reporting level is low and information about potential suspicious transactions may not reach the Financial Intelligence Unit[19].

Another sector where more reports could be expected from the number of obliged entities and turnovers is the real estate companies, via which non-resident money has also been invested in Estonia, and which may have included funds with suspicious or at least unclear origin. The real estate sector has very vague outlines because there is no obligatory procedure to follow before entering the market. In the Commercial Register, 2578 undertakings are registered as real estate firms, 1800 undertakings have registered real estate as their main area of activity, an online search results in roughly 160 undertakings operating in the sector. The sector itself does not perceive the actual risks present in the sector adequately and considers the statutory due diligence measures as excessive. Thus, the conclusion that the sector is not sufficiently involved in the money laundering prevention system. [20]

The third sector is providers of company services, whose services are directed at creating new companies. Here, companies sold particularly to non-residents, including e-residents are at risk, by easily being used to carry out suspicious transactions, as the basis for applying due diligence measures is not very uniformly established in the law. In order to ensure money laundering and terrorist financing prevention and considering the increased risk, the application of due diligence measures should be mandatory not only when forming a business relationship, but also when the transaction amount is below 10,000 euros[21]. It is common for the companies of e-residents to use the providers of company services with and without activity licences. 8% of the companies of e-residents have or have had connections with service providers without activity licences according to the Commercial Register. In practice, the providers of trust and company services (both those operating with a licence and those without) offer similar services, namely, the use of the address of the service provider and offering a service of contact persons for the entrepreneurs. The vulnerability analysis related to e-residency is in section 3 of this chapter.

The legal framework which regulates the reporting obligation and risk assessments is in compliance with international standards and EU law. The duties of obliged entities on identifying the risks, applying relevant mitigation measures, and reporting suspicious transactions are clear and understandable in the MLTFPA.

Financial institutions and designated non-financial businesses and professions apply relevant measures for money laundering and terrorist financing prevention, the extent of which generally complies with their risks, and they report suspicious transactions, but insufficiently at times (to an unjustifiably small extent) and/or at an insufficient level (the content and quality of the report is inadequate). Financial institutions and designated non-financial businesses and professions have established operating principles, management mechanisms, and actions that allow them to manage and mitigate the identified risks; these operating principles, management mechanisms, and actions are regularly updated, there is a clear legal framework for this purpose (MLTFPA § 14, but also 13, 15, 17) and guidance by supervisory authorities. However, the statutory basis for applying due diligence measures is not clear enough for a riskier-than-average sector – company service providers –, thereby necessitating amendments of the law.

The consolidated assessment of vulnerability arising from the reporting duty and the application of

[19] Read more about the sector of providers of virtual currency services in chapter 7 of this Report.
[20] Read more about the real estate sector in chapter 6 of this Report.
[21] Read more about the sector of company service providers in chapter 11.7 of this Report.

preventive measures is average-low (2).

5. Opportunities of using legal persons

There are no measures and centrally coordinated activities at the national level that would clearly be directed against the abuse of legal persons and legal units for the purpose of money laundering or terrorist financing. Information on beneficial owners is organized with the Commercial Register, but these are not entries of legal meaning in the Commercial Register (court register), therefore the quality of the data has been severely criticized. These shortcomings have already been partially addressed with the amendments adopted in summer 2020 (creating a separate database of beneficial owners). Information on actual beneficial owners is available to competent authorities via the commercial register application. At the same time, activities must continue to increase the quality of data on beneficial owners.

A more detailed analysis of using legal persons is in section 2 of this chapter.

Vulnerability arising from opportunities of using legal persons is average (2.75).

6. Supervisory authorities' access to information

Financial Intelligence Unit

The right and timeliness of the Financial Intelligence Unit in accessing information is ensured by law across sectors and uniformly from the aspect of money laundering and terrorist financing prevention. § 58 of the MLTFPA specifies the rights of the Financial Intelligence Unit in collecting information, the general principle being that to perform the duties arising from law, the Financial Intelligence Unit has the right to receive information from the competent supervisory authorities, other state authorities, and municipal agencies, and, based on a precept, from obliged entities and third parties by the deadline set by the Financial Intelligence Unit. The law ensures access for the Financial Intelligence Unit to bank and business secrets as well as data collected during surveillance. Pursuant to § 58 (4) of the MLTFPA, the right to request information does not apply to an attorney, except if the attorney provides the services specified in § 2 (2) of the MLTFPA or the report issued by the attorney to the Financial Intelligence Unit does not meet the established requirements, is not accompanied by the required documents or is accompanied by documents that do not meet the requirements. The overall opportunity of receiving information is good from the basis of the legal framework, as the rights are ensured and practice shows that in general, responses are sent within 5–10 days. In the case of urgent information requests, the Financial Intelligence Unit can also receive information faster and in the case of large information requests, a longer deadline is granted for performing the request. The Financial Intelligence Unit has access to the primary state registers and information systems, in which the Financial Intelligence Unit can access information without delay, incl. concerning requests about transactions taken place on bank accounts, the majority of credit institutions and investigative authorities use the electronic system of information inquiries and arrest mediation (e-Arrest)[22] since September 2020, where information can be obtained immediately[23].

The only vulnerability is the opportunity and speed of gaining access to information in a situation where persons have given incorrect contact information. For example, the MLTFPA, adopted in late 2017, established the term of providers of virtual currency service, to whom activity licences were granted on the basis of passing a list of control items, which was the prerequisite of relatively quick authorisation. This resulted in a situation where many authorized companies were only linked to Estonia via the company and authorisation, but the company was not operating here, there were no clients in Estonia, services were not provided here, and the company was managed and represented from abroad. This vulnerability has been attempted to be mitigated with an amendment of the MLTFPA which entered into force on 10 March 2020, establishing a statutory requirement on the providers of virtual currency services

[22] https://www.rik.ee/et/muud-teenused/e-arest

[23] Further development activities of the electronic system of information inquiries and arrests are planned for 2024, which will further expand the opportunities of information mediated via the system.

to operate in and have a management board in Estonia, which decreased in practice the opportunities of the risks materialising due to abuse of this specific vulnerability, but the current additional measures have turned out to be still insufficient in decreasing the overall vulnerabilities of this specific sector[24].

The Financial Supervision Authority

In order to supervise the field of money laundering prevention, the Financial Supervision Authority collects information from market participants directly via on-site inspections, annual remote inspections as well as thematic inquiries. Special acts (the Credit Institutions Act, the Creditors and Credit Intermediaries Act, the Payment Institutions and E-money Institutions Act, the Insurance Activities Act, the Investment Funds Act, the Securities Market Act) have set a reporting duty on the market participants to the Bank of Estonia (Eesti Pank) and the Financial Supervision Authority. The Financial Supervision Authority uses the data collected in reporting for monitoring money laundering risks on an ongoing basis, both quarterly and monthly (e.g., deposit data, data on foreign payments). There is a mutual cooperation and information exchange between the Financial Supervision Authority and the Financial Intelligence Unit. The cooperation agreement between the Financial Supervision Authority, the PBGB, and the Prosecutor's Office was concluded in 2009. Cooperation control is exercised via discussions, setting of priorities, and regular meetings.

The Chamber of Notaries

Supervision over the performance of the requirements established in the Money Laundering and Terrorist Financing Prevention Act and the laws established thereunder by the notaries is exercised by the Chamber of Notaries as ordinary and extraordinary inspections and remote supervision.

Supervision is exercised pursuant to § 5 of the Notaries Act, chapter 10 of the Notaries' Regulation, and the Articles of Association and Supervisory Procedure of the Chamber of Notaries. Ordinary inspection is exercised regularly over all notaries. Extraordinary inspection is carried out when the Chamber of Notaries has learned of a potential violation in performing the requirements of the Money Laundering and Terrorist Financing Prevention Act and the acts and instructions issued thereunder, or if the Financial Intelligence Unit has issued a relevant petition to the Chamber of Notaries. Remote supervision takes place periodically or as *ad hoc* inspections for all notaries via electronic means of communication. If the supervision results in the Chamber of Notaries finding shortcomings in the notary's work, it is brought to the notary's attention. If any shortcomings are common in the practice of many notaries or no uniform legal practice has been developed in this regard, the Chamber of Notaries brings it to the notaries' attention and provides guidance for harmonizing the practice[25]. If supervision results in identifying a situation indicating the suspicion of money laundering or terrorist financing, the Financial Intelligence Unit is notified pursuant to § 67 (1) of the MLTFPA. The liability for failure to exercise due diligence is specified in the MLTFPA. As at 31 December 2019, the Chamber of Notaries had identified no violations of due diligence measures for money laundering prevention in the course of its supervisory activities.

In order to resolve practical issues and exchange information, the Chamber of Notaries cooperates with other obliged entities, first and foremost with the Estonian Banking Association and credit institutions. In order to understand what problems notaries encounter when reporting to the Financial Intelligence Unit, the Chamber of Notaries has requested respective information from the Financial Intelligence Unit. Feedback sent to the Chamber of Notaries is either forwarded to a specific notary or, if the notices are of general nature, to all notaries. Little feedback from the Financial Intelligence Unit has been highlighted as a possible circumstance increasing vulnerability, including on the quality of reports in general. Sector-based feedback was first given in the spring of 2020.

The Bar Association

Only persons who are members of the Bar Association may provide legal services as an attorney. Therefore, there is full supervision over the sector. The Bar Association exercises ordinary and extraordinary supervision over its membership. There is no joint supervision over attorneys together with

[24] Read more about the risk analysis of providers of virtual currency services here – chapters 7 and 13.
[25] https://www.notar.ee/et/teabekeskus/rahapesu

any other institutions (e.g., the Financial Intelligence Unit) at the level of legal acts and practice.
Supervision exercised by the Bar Association is regulated by the legal framework both as a law (the Bar Association Act) and at the level of acts within the association (rules of procedure, rules on the organization of supervision, the code of ethics). Supervision is exercised by the board of the Bar Association and disciplinary matters of attorneys are discussed by the court of honour of the association.

A supervision plan is drawn up for each calendar year. In the course of supervisory proceedings and court of honour proceedings, attorneys are obligated to provide the necessary information, explanations and documents at the association's request, therefore access to information is ensured. Employees of the Bar Association are bound with the confidentiality obligation under the law in regards to the protection of an attorney's professional secrecy, therefore the regulations of protection of an attorney's professional secrecy cannot be considered a hindrance when sharing information. The Bar Association employs three lawyers and one paralegal. 1 lawyer and the paralegal are involved in supervision. The activities of the Bar Association are funded from the membership fees of attorneys and partly also from the state budget as part of provision of state legal aid. The Bar Association has not developed separate IT systems for conducting supervision, there is also no direct need. Every year, the Bar Association provides an overview to the Financial Intelligence Unit on the supervisory activities carried out by the board of the association, about which the association has not received feedback.

Based on the above, it can be concluded that opportunities of accessing information, regulations and practice have no negative impact on the vulnerability of supervisory authorities and the vulnerability arising from the speed and access to information of the supervisory authorities is low (1.2).

7. Application of criminal penalties

It was concluded as a result of the analysis conducted to prepare this Report that a sufficient legal framework has been established in Estonia in order to ensure the efficient and independent functioning of the work of investigating authorities, courts, and the Prosecutor's Office. More analyses on the application of the definition of money laundering in practice can be found in the chapter discussing national threats[26]. As the Estonian definition of money laundering has also been adapted to meet international standards, the problem is not so much in the definition of money laundering, but the constraints set by the Supreme Court's practice. For instance, the Supreme Court has established a constraint on the elements of money laundering via its resolutions regarding the influence on the economic system, the standard of proof and the crime of self-laundering.

1) The Supreme Court of Estonia has set constraining requirements on the elements of money laundering. In order to discuss the use of any criminal proceeds as money laundering, the subsumable act needs to have actual potential to damage the regular functioning of the economy. The subsumable act must have the potential to damage the functioning of the fiscal or economic system as a whole. Any use of criminal proceeds wherein the unlawful origin is attempted to be hidden cannot be handled as a money laundering crime (3-1-1-68-10, items 13, 14).

2) Even though the Warsaw Convention allows countries to not criminalize self-laundering, it is still treated as a crime in Estonian law. At the same time, several resolutions of the Supreme Court have resulted in an acquittal on the grounds that the Supreme Court has considered the concealment activity or purpose to be insufficient and has written that the concealment of the unlawful origin and the actual owner thereof must have a central role in the legal activities made with the criminal proceeds, because money laundering is not the case when, for instance, the concealment of the unlawful origin of the assets and the actual owner thereof is only a secondary objective or a consequence of the acts undertaken with the asset (3-1-1-34-05, item 25).

3) The Supreme Court has established the requirement that the standard of proof of a predicate offence cannot be too low. If the predicate offence is identified by the court conducting proceedings in a matter

[26] Chapter 3.

of money laundering, the prosecution on money laundering must meet the same requirements in regards to the predicate offence as held to other elements of the offence, i.e., the circumstances concerning the predicate offence must be highlighted in the prosecution. The court conducting proceedings in a matter of money laundering must identify the occurrence of a predicate offence in the resolution alongside the other elements of an offence (3-1-1-94-14, item 170).

Even though the law contains a provision, according to which money laundering occurs also when the details of criminal activity that resulted in obtaining assets used in money laundering have not been identified, there is no court practice regarding the application of this provision. In the past, the requirement for the precise establishment of the predicate offence has been a hindrance particularly when the predicate offence has been committed abroad.

The aforementioned issues could be addressed at various round tables and training by both national and international lecturers, to ensure harmonized approach regarding the elements of money laundering offence. So far, the participation rate of judges in training has been relatively low.

A three-level court system has been established for all criminal proceedings. Even though the penalty rates provided for by the law are sufficient, the court practice of penalties imposed for economic crimes could be considered somewhat lenient in the Republic of Estonia. On average, penalties imposed for money laundering range within 2–4 years of imprisonment. At the same time, penalties imposed for money laundering crimes are in proportion with the penalties imposed for other economic crimes.

Safeguards have been established to ensure the integrity of judges and prosecutors. Judges are appointed for life, security checks are in place when they are appointed, their background and suitability of personality traits and values are checked[27]. With prosecutors, integrity is ensured by supervision of the higher level of the Prosecutor's Office, inspections of senior prosecutors, basis for recusing prosecutors, the option of disciplinary proceedings, and analyses of acquittals. The independence of prosecutors is ensured by the opportunity of reporting of any disturbances and threats addressed against prosecutors via a separate channel, the unlawful influencing of a prosecutor is also criminalized.

In regards to investigation authorities, the fight against money laundering has been improved as an additional department of economic crimes has been formed in the central criminal police of the Police and Border Guard Board; the Internal Security Service also supervises areas related to financial security. The Department of Internal Control is separate and under direct supervision of the head of the PBGB, with the task of performing service supervision over police officials and employees and conducting proceedings over the offences that they have committed. They are also involved in the application of preventive measures. The PBGB has also established measures to ensure the integrity of officials: a background check is performed before an investigator is employed.

In 2017–2019, the PBGB received additional resources for fighting against financial crimes. The additional resources were primarily used to increase the number of investigators of economic crimes and the officials in the Financial Intelligence Unit. In recent years (2018–2019), there has been a significant increase in officials who are involved in investigating white-collar crimes, incl. money laundering, and identifying criminal proceeds; specialization on tactical analysis of white-collar crimes is possible in intelligence analysis. Together with increased resources, additional resources were also allocated to train officials and acquire technical means. The PBGB has focused on increased efficiency of proceedings-related analysis and surveillance, better helping to identify persons who may be related to the commission of offences, and identifying criminal proceeds. The aim is to direct more investigations in discovering more complex and severe financial crimes. Efficiency is supported by the specialization principle utilized in the PBGB – the officials of one unit solve crimes related to a very specific field, ensuring that best practices are congregated in a specific unit and thereby the officials are able to improve via specific proceedings within the unit.

[27] https://www.riigikohus.ee/et/kohtunikuamet/kohtunike-eetikakoodeks

One potential problem is the length of proceedings. As criminal schemes are complex and often also international, it takes time to collect evidence. Therefore, the time between the committed crime and the court judgment is often long. Unfortunately, complex cases have also resulted in the closure of criminal proceedings due to the expiry of a reasonable procedural deadline. Therefore, the state should review the existing processes and, if possible, economize the timing of procedural rules. However, one aspect mitigating the vulnerability is the significant change at the EU level – the establishment of the EIO (European Investigation Order), which has remarkably simplified international cooperation between EU member states (the format of international communication was simplified and deadlines were set).

In general, money laundering risks in Estonia are identified and mitigated and penalties are imposed on criminals, for which significant resources have been allocated: employment of additional investigators, additional knowledge obtained at training and a specific goal of focusing more attention on economic crimes in 2018–2019 are expected to provide visible results in the near future. Investigators, judges as well as prosecutors have an additional need for training, which would focus more on international requirements and practices in the area of money laundering and also help decrease fracturing in the procedural practices of various prefectures. For these reasons, the overall assessment on the national vulnerability related to the application of criminal penalties is low (1.7).

8. Regulation on the confiscation of assets

The existing regulation on the confiscation of assets is largely sufficient and functional, but could be applied more efficiently. By law the possibility of confiscating the instrument by which a criminal offence was committed or the direct object of a criminal offence has been established; assets acquired through offence and anything substituted by these assets; the extended confiscation institution has been created and is functional. In all cases, a confiscation decision can be made regarding assets which belong to the offender or a third party at the time of the of the judgment or ruling, and the third party has obtained the asset in full or in essential part on account of the offender, or knew that the instrument, substance, or object was transferred to them to avoid confiscation. In addition, in all cases where there are grounds for confiscation and the instrument of committing the offence or the immediate object of the offence has been transferred, used up, or the confiscation of which is impossible or imprudent for other reasons, the court may order an amount that meets the value of assets to be subjected to confiscation. Upon the petition of the Prosecutor's Office and with the ruling of the preliminary investigation judge, various protective measures can be applied to ensure the confiscation or replacement of confiscation, such as seizure of assets, court mortgage and all other measures that can be applied to protect the claim pursuant to the Code of Civil Procedure. Among others, seizure and confiscation have also been applied to cryptocurrency in Estonia[28].

Despite the option provided by § 126 (2^1) of the Code of Criminal Procedure, pursuant to which *property seized in order to secure confiscation may be transferred at the request of the Prosecutor's Office and with the consent of the owner of the property on the basis of an order of a preliminary investigation judge. Property may be transferred without the consent of its owner if the costs of keeping thereof are unreasonably high or if this is necessary for the prevention of the decrease in the value of the property,* the requirement of the statement of reasons by the law enforcement authority is vague in regards to the "significant decrease of the value of the property", which is why at present immediate transfer without the consent of the owner is not used as a replacement for confiscation of vehicles, and vehicles are realised years later, after a court judgment has entered into force. At that point, the proprietary value is lower by a third at the very least. In other words, the state loses a significant amount of criminal proceeds via confiscation and that should be discouraged. This means that the PBGB seizes approx. 50–250 vehicles per year. The value of some vehicles ranges between 100,000–300,000 euros. For example, the option of sale arises three years after the seizure upon a conviction – the value of the property has dropped to 50,000–150,000 euros. At the same time, unreasonable storage expenses have been incurred, ranging to

[28] 6.1496 BTC = 43,846.96 EUR was seized in 2019; 2.25628458 BTC= 18,524.00 EUR was seized in one matter and 2.25628458 BTC = 18,524.00 EUR in another matter in 2020, also later confiscated by the court.

several hundred thousand euros for a few years. In summary, the state is at a loss both from the decreased value of the sold vehicle and by paying the storage costs. Due to this, a proposal is made to analyse opportunities of alleviating the requirement of a statement of reasons by the law enforcement authority.

In order for the court to make decisions on confiscating property, evidence must be collected. The PBGB has a separate department of identifying criminal proceeds and also specialized investigators in prefectures. The department of identifying criminal proceeds in the Central Criminal Police investigates criminal proceeds in criminal matters processed by the Central Criminal Police and, in addition, also provides aid to other investigative authorities when necessary. An information day for criminal proceeds investigators has taken place every year, involving the PBGB officials as well as the criminal proceeds investigators at the Estonian Tax and Customs Board. The department of logistics of the PBGB is involved in asset management, whose task is to realise the confiscated assets in storage.

One systemic issue is that the grounds for confiscation listed above can be used only in the case of a conviction. There are no instruments in domestic law such as administrative confiscation and confiscation without conviction. There is also no option of confiscating assets if the proceedings are closed due to the severe illness or death of the accused. To a certain degree, these shortcomings are mitigated in practice by the right of the Financial Intelligence Unit to freeze suspicious transactions (§ 57 of the MLTFPA), including a regulation, pursuant to which in a situation, where the owner of an asset or the beneficial owner of assets on an account have not been successfully identified within one year after the restriction on the asset was established or if the possessor of the asset notifies the Financial Intelligence Unit or the Prosecutor's Office in writing of their desire to forgo the asset, then the Financial Intelligence Unit or the Prosecutor's Office may petition the administrative court for permission to transfer the asset to state property. This provision has also been successfully used in practice.

The legal norms concerning the confiscation of assets do provide various means of confiscating assets for authorities, but several confiscation methods listed in international standards and accepted as effective measures in money laundering prevention have not been introduced: confiscation without conviction, performance of confiscation resolutions without a foreign conviction and administrative confiscation – domestic law does not provide for such options. For this reason, seizure of illegal proceeds is not always ensured. It is also necessary to ensure that there is a sufficient number of officials responsible for the identification of assets, establishment of disposal limits, seizure, confiscation, and realisation, and that they have the necessary resources and training options.

The assessment of vulnerability related to the regulation of confiscation of assets is average-low for the above reasons (2).

12. Public awareness of the importance of ML/TF prevention

The Yearbook of the Financial Intelligence Unit is published annually, also covered by the media. In addition, the website of the PBGB has had a separate section for the Financial Intelligence Unit[29], disclosing all necessary information from guidelines to the FAQ. Cases of money laundering are also displayed in the media similarly to the Yearbook. The Internal Security Service also holds an annual press event introducing their Yearbook, also covering trends and topics of terrorist financing. Press releases (and also more involved articles covering cases) and Yearbooks are used to inform the public of the threats of money laundering and terrorist financing and also to send the signal that the state is committed to discovering such crimes and punishing the offenders. The department of corruption offences of the Central Criminal Police has been publishing overviews of the activities of the department for over two years, covering issues in the area, increasing awareness of corruption and the importance and opportunities of activities against related crimes, incl. money laundering.[30]

[29] Due to the Financial Intelligence Unit moving under the Ministry of Finance, the website of the FIU has moved to a new address: fiu.ee

[30] https://www.politsei.ee/et/kasulikud-materjalid

The Tax and Customs Board has also utilised public campaigns for increasing tax compliance of the society, which has had a positive effect on overall legal compliance and public awareness, incl. from the aspect of the importance of discovering and preventing economic crimes. Publications are released by the Academy of Security Sciences, including scientific literature, which also cover problematic topics related to money laundering and terrorism. The publications increase the public attention and awareness.[31] Awareness-increasing materials are added to the updated website of the FIU on an ongoing basis[32].

The relatively high awareness level of the society decreases national vulnerability to money laundering; therefore, the vulnerability has been assessed as low (1.5).

13. Efficiency of border and customs control

It was concluded from the analysis conducted to prepare this Report that sufficient legal regulation has been established in Estonia, ensuring the efficiency of border and customs control. Efficiency is ensured first and foremost by suspending or detaining cash and goods upon suspicion of money laundering or incorrect declaration or that false information has been submitted. There are also sufficient control procedures and equipment as well as human resources for carrying out inspections and random or risk-based physical searches in order to identify unauthorized/unlawful transport of cash in vehicles and shipping containers entering or exiting the country, and such inspections and searches are done efficiently. There are also additional protective measures to ensure the integrity of border and customs control officials.

The geographic conditions and border control mechanisms protect the country against attempts of transporting cash, precious stones etc. into and out of the country as illicit goods, therefore the vulnerability assessment is low (0.75)

14. Ensuring the payment of taxes

The working group concluded from the analysis that Estonia has an effective comprehensive legal framework, including sufficient opportunities for collecting tax debt, authorisations for collecting information, and adequate penalties for the prevention of violation of tax-related legislation and for punishing violators. Tax officials can perform their tasks without improper influence and with sufficient independence and autonomy.

The compliance with taxation legislation is ensured, the ETCB is operating fairly and consistently, therefore vulnerability is assessed as low (0.3).

15. Anonymity of financial transactions

The primary instrument allowing for anonymity of financial transactions is cash. The Euro zone contains 1.29 trillion euros' worth of bank notes and this has grown by approx. 5% per year. Eesti Pank has issued over 2 billion euros' worth of cash into circulation since joining the euro (2011). Even though the amount of cash circulating in Estonia cannot be measured precisely, based on various statistical indicators we can see that the amount of circulating cash has been growing by the year to a small extent. For example, the annual growth of cash issued from ATMs has ranged between 1–2.5%.

The MLTFPA establishes an obligation of reporting cash transactions when cash used in a transaction exceeds a limit of 32,000 euros (or an equivalent amount in another currency) or is suspicious regardless of the limit, in order to mitigate cash-related risks. Meaning that obliged entities report each transaction exceeding this amount to the Financial Intelligence Unit[33].

[31] https://digiriiul.sisekaitse.ee/discover
[32] https://www.fiu.ee/
[33] An exception is the credit institutions that only report currency exchange transaction outside of a business relationship, which exceed this limit.

A cash declaration must be submitted by a person entering the European Union when they bring 10,000 euros or more or another currency or freely exchanged assets in the same value (e.g., bonds, shares, travel cheques, or similar payment instruments). Based on the declarations of persons entering the European Union through Estonia, the following statistics can be presented regarding large-denomination euros entering and exiting the country:

Table 11. Movement of large-denomination euros in 2017-2019

Value of €200 and €500 brought into Estonia, declared to the ETCB		
	€ 200	**€ 500**
2017	992,000	2,963,600
2018	1,103,200	28,473,400
2019	3,125,000	700,000

Value of €200 and €500 brought out from Estonia, declared to the ETCB		
	€ 200	**€ 500**
2017	115 400	1 304 600
2018	190 600	1 842 600
2019	4 215 200	2 878 600

In recent years, Eesti Pank has issued large-denomination bank notes as follows:

Table 12. Issue of large denomination bank notes in 2017–2020

Value of bank notes issued by Eesti Pank as net issue			
	€500	**€200**	**€100**
2017	-24,658,500	40,952,400	-48,805,300
2018	21,450,500	351,200	-72,862,000
2019	-88,543,000	19,691,400	-59,685,000
2020	-48,894,000	31,054,200	-4,571,200

The net issue of €500 and €100 bills issued by Eesti Pank has been negative, i.e., these denominations return from circulation to the central bank more than they are issued, which has essentially not changed in recent years. The council of the European Central Bank decided to stop issuing the €500 bills in 2019[34], but it has not significantly increased the demand for €200 bank notes. The demand for large denominations has not changed much according to information available to us. At the same time, these statistics do not allow for conclusions about the actual use of cash in Estonia, as no statistics are collected about the movement of cash within the EU. For this reason, measures and restrictions established across the EU would be effective to mitigate vulnerabilities arising from the use of cash.

The Estonian MLTFPA did not use the so-called e-money exception in the previous years, i.e., did not use the exception allowed in the AMLD for establishing thresholds, therefore general rules for due diligence measures as well as reporting suspicions had to be used for e-money as well. The use of e-money is also not very common in Estonia, as people can comfortably use other alternatives and means of payment which are not anonymous and are less risky. A more detailed analysis of other virtual currencies and means of payment is in chapter 7.

[34] The Council decided to permanently stop the production of the 500-euro bill and leave this denomination out of the second series of euro notes, because the use of the 500-euro bill may ease illegal activities, https://www.eestipank.ee/press/ekp-lopetab-500-eurose-pangatahe-tootmise-ja-ringlusse-laskmise-04052016

It is difficult to assess the share of virtual currencies in the Estonian economy: the providers of virtual currency services are often connected to Estonia to a minimal extent, limited only to applying for an activity licence. This in turn does not prevent the holder of Estonian activity licence to also apply for an activity licence in another EU or third country jurisdiction. Nearly 40% of companies who have an activity licence for virtual currency had an account in Lithuania at the time of responding to the survey of the FIU, 25% in United Kingdom and only 10% in Estonia. According to the survey, the share of Estonians in all consumers of virtual currency services is only 0.15%[35]. For these reasons, it is incorrect to relate the approximate turnovers of providers of virtual currency services to Estonia. When looking at the volumes of cash transactions and the approximate cryptocurrency transactions and comparing them to the financial transaction volumes that take place via credit institutions[36], the conclusion is that the share of potential anonymous financial transactions is still very small in the Estonian economy.

Due to the small proportion of anonymous financial transactions, the vulnerability is considered low (1).

16. Economic and geopolitical factors

When taking a closer look at the impact of economic and geopolitical factors on money laundering and terrorist financing prevention and their potential impact on Estonia's vulnerability, it was found that:

- the share of shadow economy of the GDP of the state is decreasing (2017: 18.2%, 2018: 16.7%; in comparison, the European average in the years 2010-2015 according to the IMF report[37] was 20.2%)[38];
- the country is considered relatively attractive by foreign financial institutions, even though the small size of our market does not provide for many opportunities to generate profit;
- the number of immigrants and petitioners for refuge is not increasing in the country; at the same time, here we can see a trend where the immigration quota has remained the same in recent years but filled up earlier every year (July 2017, June 2018, and March 2019);
- According to the annual corruption perception survey organized by Transparency International, Estonia has continued to achieve positive results in 2017–2019, reaching the top 20 of world countries where corruption is perceived less[39]);
- Foreign geopolitical risks that may undermine financial stability (such as connection with international conflicts) are not foreseen in the near future.

The influence of economic and geopolitical factors on national vulnerability is low (1.6).

17. Remedying findings of previous assessments

In the previous NRA (2015), the weakest aspect of state vulnerability in terms of preventive mechanisms (in this NRA methodology also referred to as "control measure") was the quality of identifying beneficial owners and the data of the commercial register. In 2018, provisions entered into force, creating a mechanism for disclosing beneficial owners to the Commercial Register, which is available for free for everyone, including obliged entities (and obviously for competent authorities).

In addition, amendments have already been adopted to clarify the definition of a beneficial owner, developments to create a database of beneficial owners and a mechanism for increasing its quality are being prepared.

The assessment of the following preventive mechanisms also reached the average level according to the

[35] See the survey of providers of virtual currency services, FIU 2020, available at https://www.politsei.ee/files/Rahapesu/virtuaalvaeaeringu-teenuse-pakkujate-uuring.pdf?9fd7e5611b
[36] https://statistika.eestipank.ee/#/et/p/147/r/3610/3359
[37]https://www.imf.org/~/media/Files/Publications/WP/2018/wp1817.ashx#:~:text=The%20average%20size%20of%20the,and%20Switzerland%20with%207.2%20percent.
[38] SSE (Stockholm School of Economics) Shadow Economy Index for the Baltic Countries
[39] https://www.transparency.org/en/cpi/2019/index/nzl

NRA (2015):

- Insufficient resource of investigators of ML crimes;
- Impossibility of confiscating assets from third parties.

The increase in the investigation capabilities of economic crimes has already been discussed in this chapter (see section 7).

On 10 January 2017, amendments to the Penal Code entered into force, which regulate confiscation of assets from third parties, including the principle that in order to avoid confiscation, the party must prove that the assets are not criminal proceeds. In addition, a so-called substitutive confiscation was established, allowing also to confiscate an amount equivalent to the assets directly obtained from the crime instead of such assets.[40]

The shortcomings identified in the NRA 2015 have been addressed in Estonia in recent years and significant legal amendments have entered into force and also applied in practice by now. However, not all recommendations of the NRA 2015 could be entered into force by the due date (by 2016–2017), indicating a lack of mechanisms needed to ensure the execution of the action plan. By the time of preparation of this Report, however, the organisational side of the NRA is also regulated with more clarity – this is a statutory obligation, a specific responsible entity has been established (the AML/CFT committee[41]), and, pursuant to the action plan of the NRA 2015, new methodology for carrying out the NRA has also been created.

Additionally, execution of the recommendations and improvement proposals of the assessment report carried out on Estonia by MONEYVAL was analysed. The 2014 MONEYVAL report was relatively positive, but shortcomings were still identified in Estonia's system at the time, the remedying of which was reported to MONEYVAL regularly by Estonia's representatives. In summer 2019, MONEYVAL decided[42] that Estonia has achieved enough, having previously executed significant legal amendments: in relation to establishing the obligation to identify and disclose beneficial owners, in relation to increasing the efficiency of the confiscation system, specifying the definitions of money laundering and terrorist financing and a clearer organisation of the application of international sanctions.
For the above reasons, the practice of remedying shortcomings identified during previous assessments does not have an impact that would increase Estonia's vulnerability and it is low (1.8).

4.1.2. Additional vulnerabilities that can be derived from Estonia's international ratings

At the time of preparing this Report, various indicators, analyses and international comparisons with other countries were analysed.

Based on the Basel money laundering index[43], Estonia takes first place globally in terms of efficiency of its money laundering system (in 2017, we took 3rd place; in 2018, 2nd place, and in 2019, 1st place). The Basel index is based on indicators of the country and most recent available data on international assessments.

Based on the corruption perception index, Estonia takes 18th place globally (among 180 countries).

Based on the Fragile States Index, Estonia is a stable country, improving its ranking every year (Finland is at the top).

The share of shadow economy is decreasing in Estonia, as well as the tax gap as a general trend (the tax

[40] Also see subchapter 8
[41] MLTFPA § 11 and § 12.
[42] https://rm.coe.int/moneyval-2019-13-ee-4thfollowuprep/16809805e3
[43] https://baselgovernance.org/publications/basel-aml-index-2020

gap was assessed at 362 million euros in 2017, at 321 million euros in 2018, at 351 million euros in 2019).

The demographic scene and national economy indicators of Estonia show a positive trend (the Covid crisis of 2020 and the impact thereof have not been taken into account here).

Therefore, international rating institutions have given Estonia a positive assessment and no additional vulnerabilities are related to it that would require in-depth analysis.

4.1.3. Conclusions

State vulnerabilities were assessed pursuant to the risk assessment methodology on the basis of FATF efficiency indicators (or Immediate Outcomes). FATF had described eleven immediate outcomes (provided in the table below) which constitute the topical objectives of a money laundering and terrorist financing prevention system that efficiently protects the integrity of the financial sector and supports safety and security. The assessment of national vulnerability of Estonia is structured based on their direct results, also considering additional indicators/aspects.

The analysis in this chapter was based on the following sources and documents:

a) the legal framework effective in 2017–2019 (acts and regulations governing the field);
b) the planned and executed legal amendments (drafts and explanatory memorandums of 2019–2020);
c) court decisions on money laundering (2017—2019);
d) instructions, guidelines, internal rules of procedure, and regulations of competent authorities;
e) materials and information concerning the resources of competent authorities (budget, statistics, number of employees, etc.);
f) risk analyses of competent authorities, incl. SNRA 2017 and 2019 and the Estonian NRA 2015;
g) materials, assessments, and reports of international organizations and rating agencies concerning Estonia;
h) reports, reviews, and statistics of competent authorities concerning money laundering and terrorist financing prevention related activities;
i) meeting discussions of the national vulnerability working group and the opinions and positions of the experts involved.

Based on these materials and the methodology used, assessment was conducted across the IOs of FATF for the eleven efficiency indicators and four additional aspects regarding the control measures at national level, control measures at the stakeholder level and overall IT control measures both in terms of efficiency of setup and efficiency of functioning.

The result was the following assessments on national vulnerability concerning money laundering[44]:

Table 13. Assessments of national vulnerability across IOs

IO / additional aspect	**Short description**	**Assessment (on a scale of 0—4[45])**
IO 1	Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.	1.42

[44] This subchapter does not focus on the assessments of efficiency indicators directed at terrorist financing in particular, these can be studied in part 4.1.4 of the next subchapter.
[45] „0“= no vulnerability; „4“= the state is completely vulnerable due to lacking control mechanisms

IO 2	International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.	0.6
IO 3	Supervisors appropriately supervise, monitor and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks.	1.5
IO 4	Financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.	2
IO 5	Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments.	2.75
IO 6	Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.	1.21
IO 7 a	Money laundering offences and activities are investigated.	1.31
IO 7 b	Offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.	1.15
IO 8	Proceeds and instrumentalities of crime are confiscated.	2
Additional 1	Attitude of the society	1.5
Additional 2	Border and customs control	0.75
Additional 3	Ensuring the payment of taxes	0.33
Additional 4	Opportunities of control of financial transactions	1
Additional 5	Economic and geopolitical factors	1.6
Additional 6	Efficiency of addressing systemic shortcomings	1.87

	identified by previous assessments	

In summary, the level of national vulnerability to money laundering is **average low (2.57)**.

Table 14. Level of vulnerability to money laundering at the national level

	Level of vulnerability to money laundering	
national level	2.73	**average**

Summary

The national vulnerability to money laundering is **average**, i.e., **2.73**, which in turn arises from the fact that the national vulnerability to money laundering is rated 2.57 and the aggregated vulnerability of sectors involved is 2.97.

4.1.4. The assessment of compliance with SNRA 2017 and 2019 recommendations in Estonia at the national level

The SNRA 2017 report identified that business operations utilising cash and payments in cash, as well as the non-profit sector and e-money products are areas to which member states should pay due attention in national risk assessments and establish relevant mitigating measures. The Commission repeated this recommendation in the 2019 report. Estonia has followed this recommendation in the 2020 NRA, taking a closer look at the sector of cash traders (chapter 9), the non-profit sector (chapter 8), and the sector of financial technology, including the sector of providers of virtual currency services (chapter 7). E-money as a service has been regulated in the Estonian context in such a manner that its use does not require a separate risk assessment and measures: a significant restriction was in force in the Payment Institutions and E-money Institutions Act until 13 January 2018: up to 1000 euros of e-money could be stored on an e-money device if the e-money device does not allow repeated storage of e-money (hereinafter recharging). If the e-money device allowed recharging, up to 2500 euros of e-money could be stored or recharged on the e-money device during a calendar year. Estonia's first (and so far, the only) e-money institution started operating only in 2019. E-money institutions fall under financial service providers in Estonia and for this reason, they were discussed in detail in chapter 5.

The 2017 SNRA report suggested that member states adopt measures regarding information collected on beneficial owners that would ensure that the information is correct, precise, and up to date. First and foremost, measures had to be adopted in order for the beneficial owner to be identified as due diligence is exercised. The SNRA 2019 report repeats this recommendation. Estonia has been applying a mechanism of notifying of beneficial owners as a solution integral to the Commercial Register since 2018. In summer 2020, the Parliament (*Riigikogu*) adopted additional amendments in the regulation of beneficial owners – the definition was clarified and a legal basis was founded to establish a database of beneficial owners. However, additional steps are needed to improve the quality of data on beneficial owners, which is also indicated in this chapter of the Risk Assessment (see 4.1. subclause 5). Identifying the beneficial owner is specified in the Estonian law as a mandatory due diligence measure (MLTFPA § 20 (1) 3)).

The SNRA reports have held that member states should exercise additional effort so that supervisory authorities responsible for money laundering and terrorist financing prevention are able to perform their tasks. Estonia agrees with that recommendation and has directed additional resources to supervisory authorities. In 2019, all supervisory authorities received additional resources, the Financial Intelligence Unit and the department of economic crimes of the PBGB was enhanced – a separate unit for investigating financial crimes was formed, the budget of the Financial Supervision Authority has grown steadily, the

position of a supervisory official on money laundering / terrorist financing was created at the Chamber of Notaries in 2019. Also see more in clause 3 in this chapter.

Both the reports of 2017 and 2019 indicate the need to carry out thematic and risk-based supervisory activities in the financial sector. Specifically, it is recommended that supervisory authorities focus attention on the practices of identifying the beneficial owner (in the context of payment mediators). The Financial Supervision Authority has increased thematic and risk-based supervisory activities in the financial sector, more can be read about the supervisory activities in the financial sector in chapter 5 of this NRA.

The SNRA report of 2017 and 2019 also urge supervisors of the non-financial sector to direct their attention to traders with high-value goods, real estate, and antiques. The Financial Intelligence Unit has performed supervision in these sectors during this time, more about supervisory activities in these sectors can be read in chapters 9 and 6.

The MLTFPA, adopted in 2017, established that all traders using cash (starting from a cash payment of 10,000 euros as required by the AMLD) and providers of virtual currency service are obliged entities. Therefore, Estonia already complied with the Committee's recommendation to increase attention on the new sectors of obliged entities in 2017 (real estate mediators, art and antique traders, and providers of virtual currency services[46]).

Both the SNRA report of 2017 and 2019 urge member states to clarify due diligence measures to be applied to transactions carried out occasionally and to ensure that currency exchangers and money transferors do not avoid the obligation to apply due diligence in situations of occasional transactions. In Estonia, the law has uniformly specified that an obliged entity shall apply due diligence measures 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.[47] The provider of a payment service to the payer as well as the recipient identifies the client for each money transfer which complies with Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (ELT L 141, 05.06.2015, pp 1–18), article 3 clause 9, and the amount of financial obligation of which exceeds 1000 euros 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 month. Providers of currency exchange services are considered financial institutions in the context of the MLTFPA (see MLTFPA § 6 (2) 1)) and therefore its obligations to apply due diligence measures outside of a business relationship are uniformly specified in the law. The definition of a business relationship is also in the law: pursuant to § 3 (4) of the MLTFPA, a "business relationship" means a relationship that is established upon conclusion of a long-term contract by an obliged entity in economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the obliged entity repeatedly makes separate transactions in the course of economic, professional or official activities while providing a service or official service, performing official operations or offering goods. Therefore, a lack of a business relationship and the situation of an occasional transaction cannot be relied on as justification, for the absence of a long-term contract would not constitute an absence of a business relationship as long as a certain duration of the relationship and repetition of service provision could reasonably be expected at the time of providing the service. Therefore, both currency exchangers and money transferors are obliged to apply due diligence in situations clearly defined by the law.

[46] The MLTFPA that was valid in 2008–2017 involved providers of virtual currency services under a different name: providers of alternative means of payment services (see resolution no. 3-3-1-75-15 of the Supreme Court).
[47] MLTFPA § 19 (1) 2).

The report of 2017 recommends that member states regulate safe custody services from the perspective of money laundering and terrorist financing prevention, regardless of who is providing such services. The Credit Institutions Act § 6 (1) 14) establishes "safe custody services" as a financial service and in clause 15) also all other "transactions and acts" which are essentially similar to the financial transactions specified in clauses 1)-14) of this section. Estonia has also met this recommendation, as in general, the duty of applying due diligence extends to all services provided by credit and financing institutions, incl. for instance the rent of safe deposit boxes, etc. Additionally, credit and financing institutions are not allowed at all to provide services, the clients of which may remain anonymous – which is based on the text of the MLTFPA adopted as early as 2007[48].

As a horizontal recommendation, SNRA 2019 also indicates a report that discusses the cooperation and framework of financial intelligence units in the European Union and highlights the shortcoming of lacking feedback of financial intelligence units to obliged entities. Cooperation between the Financial Intelligence Unit and obliged entities must be improved. This NRA 2020 has also touched upon this topic and first and foremost found it necessary for the Financial Intelligence Unit to also give feedback on reports regarding suspicious transactions even in a generalized manner. This feedback, particularly for sector-based reports, has a large practical value for stakeholders and market participants. In Estonia, sector-based feedback has been given since 2020. Read more in subchapter 6 of this chapter.

Estonia has also addressed the need of training for obliged entities (see sector chapters 5 to 11) and the role of the Chamber of Notaries and the Bar Association in exercising supervision in their sectors, which is listed as issues requiring additional attention in SNRA 2017 and SNRA 2019. Inter alia, the MLTFPA regulates that by April 15 of every year, other supervisory authorities report to the Financial Intelligence Unit about their supervisory activities (MLTFPA § 67 (2)) and all supervisory authorities cooperate (MLTFPA § 64 (5)).

The topic of cash has also gained attention in the risk assessments of the Commission. Member states are recommended to analyse the matter in national risk assessments and allow reacting also in situations where amounts remain below 10,000 euros if there is suspicion of criminal activity.

- Estonia analysed the risks of using cash in the NRA of 2015. Available at: https://www.rahandusministeerium.ee/et/finants-ja-ettevotluspoliitika/rahapesu-ja-terrorismi-rahastamise-tokestamine , see Annex 2, *Sularaha analüüs*.
- The right of the Estonian customs to seize cash is not limited to violations of the declaration obligation – if the customs have reason to believe that the cash is criminal proceeds or is related to money laundering or terrorist financing, the customs have the right to seize the cash for up to 48 hours for carrying out customs control and ascertain facts (Customs Act § 29 (4)).
- The activities of law enforcement and supervisory authorities is also not limited to any amounts upon suspicion of money laundering or terrorist financing crimes.

4.1.5. Vulnerabilities to terrorist financing identified at the national level

1. Policy development and application

In Estonia, money laundering and terrorist financing prevention is regulated centrally by the same act – the Money Laundering and Terrorist Financing Prevention Act. Therefore, a lot of obligations and measures arising from this Act are directed both against money laundering and terrorist financing. At the same time, it is not directly possible to highlight the specificity of terrorist financing prevention in regulations. Similarly, terrorist financing is not separately highlighted in policies (the coalition agreement) or strategic documents. For this reason, compared to vulnerability to money laundering, the development and application of state politics is in a weaker situation in regards to terrorist financing,

[48] MLTFPA (2008) § 15 (2): *A credit institution and a financial institution is not allowed to provide services that can be used without identifying the person participating in the transaction and without verifying the submitted information. Credit institutions and financial institutions are required to open an account and keep an account in the name of the account holder*.

which is why it is difficult to prove political desire to prevent terrorist financing based on existing evidence. At the same time, there is also no evidence to the contrary – that terrorist financing is not as important as money laundering prevention. Similar to a clear state policy and strategy on money laundering, there is also no such document in the area of terrorist financing. Pursuant to § 6 of the Security Authorities Act, the functions of the Estonian Internal Security Service include prevention and combating terrorism and terrorist financing and support and collection and processing of information necessary for such purpose. Therefore, in practice it is interpreted that the Security Authorities Act refers to terrorist financing in the meaning of the MLTFPA and more broadly, and the task of the Internal Security Service is to be responsible for all related strategies in the scope of terrorist financing prevention and combating, including with the use of its membership in the governmental committee specified in § 12 of the MLTFPA, who also has the mandate to develop terrorist financing prevention policies pursuant to (1) 4) of the same section. Even though reports on transactions with suspicion of terrorist financing are formally received by the Financial Intelligence Unit, it is important to see the desire of the legislator, particularly from the perspective of terrorist financing, to separately regulate the cooperation of the Financial Intelligence Unit and the Internal Security Service, to which a separate section is contributed in the MLTFPA, section 62: *The Financial Intelligence Unit and the Security Police Board cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information.* The state assessment of terrorism and the financing thereof via regulation under penal law also deserves a separate mention, by declaring several offences related to terrorism and the financing thereof as crimes in the Penal Code as offences against the public authority, which allow the application of more severe penalties for committing such acts.

The total assessment of the vulnerability of terrorist financing prevention policy and coordination activities is low (1.8).

2. International cooperation in criminal matters

As with money laundering, international cooperation in criminal matters of terrorist financing also takes place in cases of terrorist financing, which is why the text of subchapter 2 in this chapter 4.1 also applies in the context of terrorist financing.

A sufficient legal framework has been established for international criminal cooperation, allowing possibilities for efficient international cooperation in investigating terrorist financing. Efficient international cooperation is first and foremost possible via requests for judicial assistance and European Investigation Orders and Estonia is also actively using those opportunities. Also, the legal framework currently in force allows to coordinate actions with colleagues in other countries via the option of creating international investigation teams. International law enforcement networks such as Egmont, Interpol, Europol, Sirene, Eurojust are used actively. There is also active cooperation between law enforcement and security authorities / special services of partner states.

International cooperation and the internal coordination mechanisms of ensuring thereof are efficient and allow Estonia to offer substantial and valued cooperation to its international partners, which is why the level of international cooperation has a clear mitigating effect on the overall vulnerability of the state.

The vulnerability of international cooperation in processing crimes of terrorist financing has been assessed at 0.4, i.e., vulnerability is extremely low.

3. Capability of supervisory authorities

Supervision over market participants is exercised by supervisory authorities similarly over regulations of money laundering prevention and regulations of terrorist financing prevention, as the legal norms are the same. Therefore, the capabilities and assessments of supervisory authorities described in subchapter 3 of this chapter 4.1 also apply in the context of terrorist financing.

Certain specificities may occur only as a result of risk assessments of supervisory authorities: terrorist

financing starts from small amounts and the indicators in monitoring suspicious transactions are different than those of money laundering. But this is more about the setup of the first line of defence than an actual subject of supervision as such. At the same time, when awareness is low, the number of reports is also non-existent (e.g., the sector of NPOs, chapter 8).

According to the MLTFPA, the authorities performing supervision over the compliance with the requirements of money laundering and terrorist financing prevention are the Financial Intelligence Unit, the Board of the Estonian Bar Association, and the Ministry of Justice, who may (and has) delegate supervision to the Chamber of Notaries.

The Financial Intelligence Unit exercises supervision over subjects who they authorize (issue licences to). The Bar Association exercises supervision over the performance of requirements of professional activities and professional ethics of members of the Bar Association and foreign attorneys operating in Estonia. The Chamber of Notaries supervises the performance of the requirements of the MLTFPA and legislation established thereunder by the notaries. The Financial Supervision Authority exercises national supervision over subjects that the Financial Supervision Authority has authorised.

Statutory supervisory activities and the structure thereof are the same for money laundering and terrorist financing, meaning that it is based on risk, in order to identify abuses of the system and anomalies. For example, relevant instructions of the Financial Intelligence Unit direct to identify transactions indicating money laundering as well as terrorist financing, and help notice and report transactions indicating suspicion of terrorist financing.

The Internal Security Service carries out activities arising from the Security Authorities Act to prevent terrorist financing.

The capability of supervisory activities and the efficiency of its structure has been assessed at 1.5 in terrorist financing prevention, i.e., the vulnerability is low.

4. Use of reporting suspicious transactions and preventive measures

§§ 49 and 50 of the MLTFPA establish a reporting duty on all obliged entities in the case of suspicion of money laundering. The reporting duty can be performed electronically via an online form or the X-Road service. If the person has no such options, they can also send an e-mail to the Financial Intelligence Unit as a last measure and the information received is registered as a report. There are also instructions regarding the format and filling of a report issued to the Financial Intelligence Unit on the website of the Financial Intelligence Unit, helping an obliged entity in submitting a report.[49]

As preventive measures for money laundering, the MLTFPA specifies the management of risks related to money laundering and terrorist financing (chapter 2) and the application of due diligence measures (chapter 3).

One vulnerability is the fact that movements of money related to terrorist financing are not easily monitored by obliged entities. Reports of terrorist financing generally arrive based on connection to countries at risk, actual suspicion in relation to terrorist financing is often not found because identification is difficult or, in certain cases, impossible from the perspective of the obliged entity. Additionally, it should be considered that most of the due diligence measures, both in Estonia and internationally, are established for the purpose of money laundering prevention and there are no effective due diligence measures, the application of which would ensure a better functioning of the terrorist financing prevention system.

For these reasons, the assessment of vulnerability is average-low (2).

[49] https://www.fiu.ee/oigusaktid-ja-juhendid/juhendid#juhend-kahtlaste-teh

5. Opportunities for the misuse of legal persons

Additional specificities in comparison with clause 4.1.3 of this Report cannot be highlighted in regards to terrorist financing. However, increasing the quality of data of beneficial owners would significantly aid in terrorist financing prevention, which is why it is necessary in this aspect to apply additional measures to increase the transparency of owners and beneficial owners of legal persons. In the case of abusing Estonian companies, vulnerability to terrorist financing is assessed to be even higher than in terms of money laundering, as vulnerability is increased by lower awareness, also see section 2 of this chapter and chapter 8 on NPOs.

The assessment of vulnerability is average-high, 3.16.

6. Timeliness of supervisory authorities' access to information

The right of the Financial Intelligence Unit to access information and the speed thereof is ensured with laws across sectors and in the same way across money laundering and terrorist financing prevention, therefore the description of the situation in subchapter 6 of chapter 4.1. also applies in the context of terrorist financing. § 58 of the MLTFPA establishes the rights of the Financial Intelligence Unit to request information, the general principle being that to perform the duties arising from law, the Financial Intelligence Unit has the right to receive information from the competent supervisory authorities, other state authorities, and local authority agencies, and, based on a precept, from obliged entities and third parties by the deadline set by the Financial Intelligence Unit. The law ensures the Financial Intelligence Unit access to banking and business secrets and to data collected during intelligence. Pursuant to § 58 (4) of the MLTFPA, the right to receive information does not apply to an attorney unless the attorney provides the services specified in subsection 2 of § 2 of the Act or a report given by the attorney to the Financial Intelligence Unit does not meet the established requirements, is not accompanied by the required documents, or is accompanied by documents that do not meet the requirements. The overall opportunity of receiving information is good based on the legal framework, as rights are ensured and in general, responses are sent within 5–10 days. In the case of urgent information requests, the Financial Intelligence Unit can also receive information faster and in the case of large information requests, a longer deadline is granted for performing the request. The Financial Intelligence Unit has access to the primary state registers and information systems, in which the Financial Intelligence Unit can access information without delay.

The only vulnerability is the opportunity and speed of gaining access to information in a situation where persons have given incorrect contact information.

In order to supervise the field of terrorist financing, the Financial Supervision Authority collects information from market participants directly via on-site inspections, annual remote inspections as well as topical inquiries. Special acts regulating the activities of subjects operating on the basis of an activity licence from the Financial Supervision Authority have set a reporting duty on the market participants to Eesti Pank and the Financial Supervision Authority with the required frequency. The Financial Supervision Authority uses the data collected in reporting for monitoring terrorist financing risks on an ongoing basis, both quarterly and monthly (e.g., deposit data, data on foreign payments. There is a mutual cooperation and information exchange between the Financial Supervision Authority and the Financial Intelligence Unit. The cooperation agreement between the Financial Supervision Authority, the PBGB, and the Prosecutor's Office was concluded in 2009. Cooperation control is exercised via discussions, setting of priorities, and regular meetings. The Financial Intelligence Unit and the Financial Supervision Authority also cooperate with other competent authorities such as the Internal Security Service.

No direct contact with terrorist financing has been identified in notarised transactions. However, in late 2020, the Internal Security Service directed attention of supervisory authorities to potential risks in real estate transactions where the purchasers are persons from a country of risk.

Pursuant to § 24 of International Sanctions Act, notaries are obliged to identify whether a person

participating in a transaction, including the beneficial owner, is subject to international financial sanctions. The notary identifies this via the e-notary, which has interfacing to the EU and UN list of sanctions. If the notary has identified that the person has been entered in the international list of financial sanctions or has found a person with a similar name in the international list of financial sanctions, they will not carry out the transaction and will send a report of international sanctions to the Financial Intelligence Unit.

Specificities regarding terrorist financing prevention cannot be brought up from the perspective of supervision by the Bar Association. In practice, contact in the sector of attorneys is even less likely for terrorism than for money laundering.

Authorities competent to combat terrorist financing utilise financial data and all other necessary information in a relevant manner to investigate money laundering and terrorist financing, therefore the assessment of vulnerability is low, 0.9.

7. Application of criminal penalties

The framework of criminal law generally does not differ when processing crimes of money laundering or terrorist financing and here, too, the Prosecutor's Office is responsible for the proceedings; preliminary investigation is conducted by the Internal Security Service in this case.

A sufficient legal framework has been established for crimes of terrorist financing in order to ensure the efficient and independent functioning of the work of investigating authorities, courts, and the Prosecutor's Office. Protective measures are established to ensure the integrity of the judges and prosecutors. Judges are appointed for life. A three-level court system has been established for all criminal proceedings in Estonia. With prosecutors, integrity is ensured by supervision of the higher level of the Prosecutor's Office, inspections of senior prosecutors, a basis for recusing prosecutors, the option of disciplinary proceedings, and analyses of acquittals. The independence of prosecutors is ensured by the opportunity of reporting disturbances and threats via a separate channel, the unlawful influencing of a prosecutor is also criminalized.

The penalty rates provided for in the law are proportionate. The competence of the pre-trial investigation of financing and supporting terror crimes and activities directed in committing terror crimes is vested in the Internal Security Service.

Vulnerability level is assessed at 1.1, i.e., vulnerability is low.

8. The regulation on confiscation of assets

The effective regulation on confiscation of assets is largely sufficient and functional, but could be made more efficient. The law has established the possibility of confiscating the instrument by which a criminal offence was committed or the direct object of a criminal offence; assets acquired through the offence and anything acquired on account of these assets; the extended confiscation institution is established and is functional. In all cases, a confiscation decision can be made regarding assets which belong to the offender or a third party at the time of the judgment or ruling, and the latter has obtained it in full or in essential part on account of the offender, or knew that the instrument, substance or object was transferred to them to avoid confiscation. In addition, in all cases where there are grounds for confiscation and the instrument of committing the offence or the immediate object of the offence has been transferred, used up, or the confiscation of which is impossible or imprudent for other reasons, the court may order that an amount that meets the value of the assets be subjected to confiscation.

Upon the petition of the Prosecutor's Office and with the ruling of the preliminary investigation judge, various protective measures can be applied to ensure the state confiscation or replacement of confiscation, such as seizure of assets, court mortgage, and all other measures that can be applied to protect the claim pursuant to the Code of Civil Procedure.

One systemic issue is that the grounds for confiscation listed above can be used only in the case of a conviction. There are no instruments in domestic law such as administrative confiscation and confiscation without conviction. There is also no option of confiscating assets if the proceedings are closed due to the severe illness or death of the accused.

Pursuant to a regulation of investigative jurisdiction between the Police and Border Guard Board and the Internal Security Service, pre-trial investigation in offences of funding and supporting a terror crime and activities directed towards committing a terror crime is carried out by the Internal Security Service.

The working group assessed the vulnerability of confiscating assets from the perspective of terrorist financing at 2, i.e., average-low.

9. Identification of cases related to terrorist financing and use of preventive measures

The Internal Security Service investigates crimes related to terrorist financing. A sufficient and functioning legal framework and systems have been established. In order to ensure a specific definition, an amendment to the Penal Code entered into force in 2019, establishing as crimes: § 237^2 Preparation of and incitement to acts of terrorism, § 237^5 Travel for terrorist purposes, 237^6 Organisation, funding and support of travel for terrorist purposes. The court may order an imprisonment for such crimes. So far, there has been 1 conviction, in 2016.

The Internal Security Service is involved in increasing public awareness of terrorism-related crimes through various channels. For example, the Internal Security Service Yearbook is published every year, covering these topics. Many obliged entities are also reached via special training, directed towards increasing awareness in vulnerable sectors. In addition to the above, the Internal Security Service also increases awareness through data procurements.

In identifying cases of terrorist financing, the primary vulnerability is the transactions via virtual channels, as they are difficult to identify and process. Vulnerability has been assessed at 2.75, i.e., average in this risk assessment. The main sources of vulnerability are the potential problems arising from the application of international sanctions. Therefore, it is necessary to continue increasing awareness of the topic of sanctions, improve cooperation between institutions and enhance information exchange, with the use of the cooperation and coordination format executed by the Ministry of Foreign Affairs at the end of 2020, and the Governmental Committee of Money Laundering and Terrorist Financing Prevention.

10. Opportunities of abuse of the NPO sector for TF and the prevention thereof

The largest vulnerability of the NPO sector is a lack of sufficient awareness and shortcomings of the legal framework which do not obligate the NPOs to apply sufficient due diligence measures or the basis for their application does not cover the practical necessities (at present, obliged entities only include cash within one transaction exceeding 5000 euros). For example, a very small part of the sector has reported to the Financial Intelligence Unit, which, considering the activities of the sector, the potential risks and threats, including transactions with third countries and unknown origin of assets, the performance of the reporting duty is clearly disproportionate with the potential points of contact of the sector with TF. It can also be concluded that the sector is particularly vulnerable in regards to background checks of transactions carried out with foreign countries: the summary of the responses to the questionnaires sent out during the NRA 2020 clearly showed that NPOs do not exercise a lot of effort to determine the background of the transaction partner. At the same time, there are also no national special directions, guidelines and training for NPOs that would help easily identify and recognize the risk indicators characteristic to this sector, which would point to the unreliability of the transaction partner. The sector can be guided by the overall guidelines of the Financial Intelligence Unit, but it can be presumed that it would also be necessary to establish special guidelines with consideration for the vulnerability of the sector.

The overall vulnerability assessment is 2.75 both for the reasons above and also considering that so far

there has been a lack of

- definition of the nature of risks for NPOs by terrorist organizations by the state;
- information on how terrorists abuse NPOs;
- the state checking the sufficiency of measures, including legal norms, related to the part of the NPO sector that may be abused for the purpose of supporting terrorist financing, in order to adopt proportional and efficient measures to mitigate the identified risks (also read more in chapter adressing the NPO sector).

11. Following and applying the resolutions of the UN Security Council

Sufficient legal regulation and systems have been established. The resolutions of the UN Security Council are used to prevent the collection, movement, and disposal of money by persons and units related to the distribution of weapons of mass destruction. This is first and foremost achieved by cooperation and coordination mechanisms of competent authorities to prevent the financing of distribution of weapons of mass destruction. Read more in chapter 12.

In cooperation with the relevant resolutions of the UN Security Council, the collection, movement, and disposal of money by persons and units related to the distribution of weapons of mass destruction is prevented. Even though coordination activities in the few recent years assessed have been insufficient, at the end of 2020, a working group operating within the Ministry of Foreign Affairs has been founded to coordinate the internal application of UN resolutions related to sanctions and weapons of mass destruction. Due to this, the overall assessment of vulnerability is average-low (2).

12. Public awareness of the importance of ML/TF prevention

The Internal Security Service is involved in increasing public awareness of crimes related to terrorism via various channels. For instance, the Internal Security Service Yearbook is published every year, covering these topics. Many subjects of the society are also addressed via special training directed at increasing awareness in vulnerable sectors. In addition to the above, the Internal Security Service also increases awareness via a call for data. It is planned to consolidate topical information on the new FIU website regarding both money laundering and terrorist financing, and terrorist financing prevention is also covered in FIU yearbooks, publications and literature of the Estonian Academy of Security Sciences, as well as the overviews of the department of corruption crimes of the Central Criminal Police.

National vulnerability in this issue is 1.75, i.e., the grade shows vulnerability to be low.

13. Efficiency of border and customs control

Sufficient legal regulation has been established, ensuring the efficiency of border and customs control. Efficiency is ensured first and foremost by detaining cash and goods upon suspicion of terrorist financing[50] or wrongful declaration or that false information has been submitted regarding them. There are also sufficient control procedures and equipment as well as human resources for carrying out inspections and random or risk-based physical searches in order to identify unauthorised/unlawful transport of cash in vehicles and shipping containers entering or exiting the country, and such inspections and searches are done efficiently. There are also additional protective measures to ensure the integrity of border and customs control officials. The technical solutions used on the border and by the customs are constantly upgraded, there is cooperation with international partners and the option of receiving tips has been created, including for applying in situations of suspicion of terrorist financing.

Vulnerability related to the efficiency of border and customs control is low (0.75).

14. Ensuring the payment of taxes

[50] § 29 (4) of the Customs Act

An effective comprehensive legal framework has been established, including sufficient opportunities for collecting tax debt, authorizations for collecting information, relevant penalties for prevention of violation of tax-related legislation, and for punishing violators. Tax officials can perform their tasks without improper influencing and with sufficient independence and autonomy.

Vulnerability related to ensuring the payment of taxes is very low (0.3).

15. Anonymity of financial transactions

The primary instrument allowing for anonymity of financial transactions is cash. The Euro zone contains 1.29 trillion euros' worth of bank notes and this has grown by approx. 5% per year. The Bank of Estonia has issued over 2 billion euros' worth of cash into circulation since joining the euro. Even though the amount of cash circulating in Estonia cannot be measured precisely, based on various statistical indicators we can see that the amount of circulating cash has grown by the year to a small extent. For example, the annual growth of cash issued from ATMs has ranged between 1–2.5%.

The MLTFPA establishes an obligation of reporting cash transactions when the cash used in a transaction exceeds the limit of 32,000 euros (or an equivalent amount in another currency) or is suspicious regardless of the limit, in order to mitigate cash-related risks. This means that obliged entities report each transaction exceeding this amount to the Financial Intelligence Unit[51].

The Estonian MLTFPA did not use the so-called e-money exception in the previous years, i.e., did not use the exception allowed in the AMLD for establishing thresholds, therefore general rules for due diligence measures as well as reporting suspicions had to be used for e-money as well. The use of e-money is also not very common in Estonia, as people can comfortably use other alternatives and means of payment which are not anonymous and are less risky. A more detailed analysis of other cryptocurrencies and means of payment is in chapter 7.

Nowadays, virtual currencies are used increasingly in financial transactions. Virtual currencies allow criminals to store assets outside of the formal financial system, digitally, in order to conceal its origin and eventual acquirer. Several properties of virtual currencies, such as the complexity or in some cases also the impossibility of identifying the beneficiary, the ease, speed, and low cost of international transactions, and in certain cases also lack of mediators make it difficult to connect assets to the actual owner even for publicly monitored transactions, and therefore also to confiscate assets in criminal proceedings. In addition, virtual currencies are used to pay for unlawful acts as well as to trade "dirty" cash. Mixers are used to hamper the monitoring of cryptocurrency transactions, used to mix illegal and legal proceeds at different points of a chain of transactions. This in turn makes it more difficult to identify the actual owner of the assets.[52]

One problem with transactions related to virtual currencies is also exchanging it for regular currency (*fiat* money) and vice versa, with the use of ATMs, wherein the provider of mediation service has not properly exercised due diligence and thus the actual owner of the assets is not known. The volumes (turnover) of the sector of virtual currency are difficult to assess and it would be incorrect to connect the turnovers of all service providers authorised to operate in Estonia with the Estonian economy.

Due to the small share of anonymous financial transactions, vulnerability is assessed as low (1).

16. Economic and geopolitical factors

The impact of economic and geopolitical factors was also assessed in regards to terrorist financing.

[51] An exception is the credit institutions that only report currency exchange transaction outside of a business relationship, which exceed this limit.
[52] https://fiu.ee/aastaraamatud-ja-uuringud/uuringud#virtuaalvringu-tee

Out of the economic/geopolitical factors assessed more closely, the following are of relevance:

- the share of shadow economy of the GDP of the state is decreasing[53];
- the number of immigrants and petitioners for refuge is not increasing in the country; at the same time, here we can see a trend where the immigration quota has remained the same in recent years but filled up earlier every year (July 2017, June 2018, and March 2019);
- foreign geopolitical risks are unlikely to influence the country in the near future (e.g., Estonia does not have much perceivable connection with international conflicts).

The influence of economic and geopolitical factors on state vulnerability is low (1.75).

17. Remedying findings identified during previous assessments

Recommendation no. 21 of the Financial Action Task Force, from the previous assessment highlights the need to monitor transactions carried out with countries of risk more carefully. For example, there was a lack of requirement to investigate the nature, purpose, or background of a transaction if a transaction is discovered that has no apparent economic or legal purpose and which is related to a country of higher risk. This shortcoming was resolved with amendments of the MLTFPA and has also been approved for compliance by MONEYVAL[54].

The previous assessment also indicated an issue where a technical problem existed in regards to, for example, applying due diligence to a client or person from a given (high risk) country. This shortcoming is also resolved with the new version of the MLTFPA adopted in 2017 and the amendments are confirmed to comply with the requirement.

One dedicated recommendation of the MONEYVAL assessment was about shortcomings regarding elements of the crime of terrorist financing. In order to ensure a clearer definition of the law, an amendment of the Penal Code entered into force in 2019 where the elements of the offence were defined: § 237^2 Preparation of and incitement to acts of terrorism, § 237^5 Travel for terrorist purposes, § 237^6 Organisation, funding and support of travel for terrorist purposes. Amending the Penal Code allows to prevent as well as investigate crimes more effectively. It also gives a clear warning to persons whose criminal behaviour was previously defined less clearly but the purpose of whose activity is related to terrorism.

An ongoing topic for the recommendations is also increasing the capability of supervision exercised by the Financial Intelligence Unit. During the past three years, additional finances have been allocated to the Financial Intelligence unit in order to improve the efficiency of the unit, including recruiting more officials for supervision. A separate group for financial crimes has been created with the same financial allocations to the PBGB, focusing on preventing economic crimes. The analysing capability of the Financial Intelligence Unit has also been increased.

The cooperation of various domestic authorities is of great importance. Various ministries and authorities under their jurisdiction take part in terrorist financing prevention. The Internal Security Service is involved in the prevention of terrorism and the financing thereof. The Prosecutor's Office and the Internal Security Service have investigation capability in this matter and supervision over measures adopted for terrorist financing prevention is exercised over subjects distributed with the law by the Financial Intelligence Unit and the Financial Supervision Authority. During the previous assessment, insufficient cooperation was highlighted as a shortcoming. Even though provisions regarding cooperation have been added to the MLTFPA and information exchange among supervisory authorities has become efficient, it would also be necessary to create a format of operative cooperation among these parties.

Therefore, the practice of eliminating deficiencies identified during previous assessments does not have

[53] Based on the assessments of SSE (Stockholm School of Economics) 2017, 2018.
[54] See the Exit-Follow-up Report, available at https://www.coe.int/en/web/moneyval/jurisdictions/estonia

an impact increasing Estonia's vulnerability and it is low (1.8).

4.1.6. Additional vulnerabilities that can be derived from Estonia's international rating analysis

There are no terrorist financing vulnerabilities in regards to assessments of Estonia carried out by international rating agencies. The risks of terrorist financing arising from the geographic location are relatively low[55]. The demographic distribution of the Estonian population is relatively stable, annual quotas are established for immigrants and petitioners for asylum and as at 2020, there were only 531 persons who received international protection.

Even though the share of Estonians in the general population has decreased in recent years, if the same patterns continue, the share of Estonians should increase again in the near future, due to the age proportions, immigration, and emigration.[56]

Based on international rating assessments and local indicators, no additional vulnerabilities have been identified in regards to terrorist financing. Vulnerabilities related to the providers of virtual currency services, e-residency, and founding of companies have been analysed in the corresponding chapters.

4.1.7. Conclusions

State vulnerabilities were assessed pursuant to the risk assessment methodology on the basis of the FATF efficiency indicators (or Immediate Outcome). FATF had described eleven immediate outcomes (provided in the table below) which are the topical objectives of a money laundering and terrorist financing prevention system that efficiently protects the integrity of the financial sector and supports safety and security. The assessment of vulnerability of the Estonian state is structured based on their direct results, also considering additional indicators.

The analysis in this chapter was based on the following sources and documents:

a) the legal framework valid in 2017–2019 (acts and regulations governing the field);
b) the planned and executed legal amendments (drafts and explanatory memorandums of 2019–2020);
c) court resolutions on money laundering (2017—2019);
d) instructions, guidelines, internal procedure rules and regulations of competent authorities;
e) materials and information concerning the resources of competent authorities (budget, statistics, number of employees, etc.);
f) risk analyses of competent authorities, incl. SNRA 2017 and 2019 and the Estonian NRA 2015;
g) materials, assessments, and reports of international organisations and rating agencies concerning Estonia;
h) reports, reviews and statistics of competent authorities concerning money laundering and terrorist financing prevention related activities.
i) meeting discussions of the national vulnerability working group and the opinions and positions of the experts involved.

Based on these materials and the methodology used, assessment was conducted across the IOs of FATF for the eleven efficiency indicators and four additional aspects regarding the control measures at the national level, control measures at the stakeholder level and overall IT control measures both in terms of efficiency of setup and efficiency of functioning. The same IOs were assessed in terms of terrorist financing, but in sepcific regards to the relevance of terrorist financing, which varied somewhat for different IOs. Even though all IOs were assessed and the assessments of terrorist financing could also

[55] Leaving aside some specificities arising from the varying definition of terrorism in different countries.
[56] Data from Statistics Estonia and the Ministry of the Interior.

vary somewhat, the specificities are discussed in the corresponding subsection 4.2, together with the relevant arguments, which is why the assessments below are only in summary of the IOs which have a more significant impact on the assessment of vulnerability to terrorist financing and which were assessed differently from the aspect of money laundering and the aspect of terrorist financing.

Table 15. Assessments of vulnerability to terrorist financing

IO / additional aspect	**Short description**	**Assessment (on a scale of 0—4)**
IO 1	Money laundering and **terrorist financing** risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.	1.8
IO 2	International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.	0.4
IO 5	Legal persons and arrangements are prevented from misuse for money laundering or **terrorist financing**, and information on their beneficial ownership is available to competent authorities without impediments.	3.16
IO 6	Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and **terrorist financing** investigations.	0.9
IO 9	Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.	2.75
IO 10	Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.	2.75
IO 11	Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.	1
Additional 1	Attitude of the society	1.5

Additional 2	Border and customs control	0.75
Additional 3	Ensuring the payment of taxes	0.33
Additional 4	Opportunities of control of financial transactions	1
Additional 5	Economic and geopolitical factors	1.75
Additional 6	Efficiency of addressing systemic shortcomings identified by previous assessments	1.87

In summary, the level of state vulnerability to terrorist financing is **average low** (2.55).

Table 16. Level of vulnerability to terrorist financing at the national level

	Level of vulnerability to terrorist financing	
National level	2.67	**average**

Summary

The vulnerability level of the state to terrorist financing is **average**, i.e., **2.67**, which in turn arises from the fact that the national vulnerability to terrorist financing is 2.55 and the vulnerability of sectors is 2.85.

4.1.8. Vulnerabilities to the distribution of weapons of mass destruction identified at the national level

The assessment on the vulnerability of the state particularly regarding the vulnerability to the sufficiency of UN Security Council regulations concerning weapons of mass destruction is specified in clause 4.1.7 of this Report (i.e., the assessment of IO 11) and is average-low in total (2).