



The Estonian National Risk Assessment
Report in the field of financing
the proliferation of weapons
of mass destruction for the years
2020–2024

Contents

SUMMARY	3
RECOMMENDATIONS FOR MARKET PARTICIPANTS	5
INTRODUCTION	6
1. THE RISK ASSESSMENT PROCESS	7
1.1. Definitions and Terms	7
1.2. Methodology	8
1.3. Data Collection	9
2. LEGAL AND REGULATORY FRAMEWORK	10
2.1. International Framework	10
2.2. National Framework	11
3. THREATS	14
3.1. North Korea	14
3.2. Iran	15
3.3. Russia: A Significant Evasion Channel	15
3.4. Threats Related to WMD High-Risk Countries and Russia	16
4. VULNERABILITIES	19
4.1. Vulnerabilities Related to the Economic and Trade Environment	19
4.2. Vulnerabilities Related to Technology and Sectors	20
4.3. Legislative and Administrative Vulnerabilities	21
5. MITIGATING MEASURES AND RESIDUAL RISK	23
5.1. Economic and Trade Environment-Related Vulnerabilities, Mitigating Measures and Residual Risk	23
5.2. Measures to Mitigate Technology and Sector-Related Vulnerabilities and Residual Risk	27
5.3. Legislative and Administrative Vulnerabilities and Residual Risk	33

Summary

The Estonian National Risk Assessment on Financing the Proliferation of Weapons of Mass Destruction: Threats, Vulnerabilities, Risk Mitigation Measures, and Risks

The risk assessment highlights that Estonia's direct connection with North Korea is almost non-existent and limited with Iran. However, the level of vulnerability related to the financing of the proliferation of weapons of mass destruction (WMD) is increased by Russia's geographical proximity and historical trade ties. The working group considers the greatest threat to be the possibility that Estonia's obligated entities (credit institutions, virtual currency service providers, corporate service providers) could be used for transactions or asset movements related to the financing of WMD proliferation. Estonia's territory could be used for the transit of goods to Russia and from there to North Korea or Iran (WMD risk countries), and a significant risk is the use of third jurisdictions to conceal the connections of parties involved in the financing of WMD proliferation with WMD risk countries.

The main vulnerabilities are divided into three categories: economic and trade environment, technological and sector-specific, and legislative and administrative vulnerabilities. Although Estonia's exports and financial flows towards Russia have significantly decreased in recent years, the risk of transactions supporting WMD proliferation through Russia has increased. This is primarily due to Russia's closer cooperation with North Korea and Iran, raising the threat level that Russia may act as an intermediary in WMD financing schemes. The risks in the virtual currency service providers (VASP) sector stem, among other things, from the threat of cyber-attacks, offshore clients, and transactions with high-risk jurisdictions. In recent years, the number of participants in the VASP sector has significantly decreased due to supervisory activities, and the ability of VASPs to apply due diligence measures has increased, consequently reducing the risk of WMD financing. The corporate service providers (CSP) sector also shows poor awareness and deficiencies in sanctions compliance procedures.

On a positive note, Estonia implements an effective legal and institutional framework for the enforcement of international sanctions, which includes both export control (strategic goods control) and supervision of the financial and non-financial sectors. In recent years, Estonia has also significantly strengthened supervision, updated laws, increased cooperation with international partners, and gained very good experience in the implementation of sanctions.

In conclusion, Estonia's exposure to WMD financing is currently low, but with the changing global security environment and the emergence of new risks associated with technological development, it is necessary to be prepared to update the current assessment. It is particularly important to increase the awareness of smaller and new market participants and to recognize and mitigate the risks associated with transactions through third countries. The higher risk level does not directly result from individuals on the sanctions list, but from those who may act on behalf of or under the direction of sanctioned individuals. The risk assessment concludes that it is necessary to ensure sufficient resources for competent authorities to effectively implement sanctions, continue to increase the awareness of market participants, and ensure that the risks addressed in this analysis are also reflected in the risk assessments and control systems of market participants themselves.

Table 1. Assessment of the Risk of Deliberate Violation, Non-Application, and Evasion of Targeted Financial Sanctions

	Risk	Threat level	Vulnerability level	Residual risk
FATF Recommendation 1	The risk of violating or failing to apply financial sanctions	Low	Low	Low
	The risk of evading financial sanctions	Medium	Low	Low

The threat level of violating or failing to apply targeted financial sanctions is low.

- In the context of financing the proliferation of weapons of mass destruction, the working group did not identify any instances of failing to apply financial sanctions measures. The threat may primarily arise from market participants who could be exploited to violate financial sanctions. Additionally, the threat may stem from changes in international sanctions rules: the threat that the rules change rapidly and the organization cannot keep up.

The threat level of evading targeted financial sanctions is medium.

- Most of the threat typologies addressed by the working group have previously been used to evade sanctions imposed on Iran, North Korea, or Russia. Some of these typologies are still used for evading sanctions, while measures have been taken to reduce the threat for others.
- The risk of evasion is increased by Russia’s close cooperation with Iran and North Korea. In situations where the evasion scheme involves multiple jurisdictions, detecting evasion is challenging for both market participants and supervisory authorities.

The level of vulnerability related to violating or failing to apply targeted financial sanctions is low.

- A survey conducted among market participants indicated that their awareness of the risks associated with financing the proliferation of WMD and the implementation of necessary organizational solutions is at a good level. This is especially true for those who process large volumes of international payments or offer trade finance services. Awareness is clearly lower in the CSP sector.
- Estonia’s legal framework for the application of sanctions is sufficient to effectively prevent the financing of WMD proliferation. The Ministry of Foreign Affairs, the Financial Supervision Authority, the Tax and Customs Board, and the Financial Intelligence Unit are systematically working to improve the awareness of market participants.

The level of vulnerability related to evading targeted financial sanctions is low.

- As of the end of 2024, effective mitigation measures have been implemented for most of the vulnerabilities described in this risk assessment. For example, the vulnerability level associated with the VASP sector has decreased due to the reduction in the number of market participants and the additional supervisory measures implemented. Estonia’s full customs control at the external border with Russia has become an important measure in reducing the level of vulnerability related to transit. However, operational information exchange and cooperation with third countries’ customs, security, and law enforcement representatives should be improved.

Recommendations for market participants

- All market participants should pay additional attention to sanctions¹ related to Russia and the risks of financing the proliferation of weapons of mass destruction (WMD).
- All obligated entities should consider the conclusions of this report when preparing risk assessments. They should take into account the annexes 1 and 2² of the FIU's guidelines on the implementation of international financial sanctions, which are largely based on the results of this risk assessment.
- It is recommended that the VASP and CSP sectors focus on identifying and preventing risks related to evading sanctions and take effective risk mitigation measures.

¹ EU Sanctions Map, <https://www.sanctionsmap.eu/#/main>

² The Financial Intelligence Unit's guidelines for the implementation of international financial sanctions, [rahapesu_andmebueroo_juhend_finantssanktsiooni_kohaldamiseks_250222.pdf](#)

Introduction

Weapons of mass destruction (WMD) and their proliferators pose a significant threat to international security. Therefore, the international community has agreed to jointly prevent the spread of such dangerous weapons. The fight against WMD includes preventing the financing of their proliferation. This risk assessment addresses possible ways in which the proliferation of WMD might be financed through the Estonian financial system or business environment. It should also be considered that Estonian territory might be used for moving goods intended to support the proliferation of WMD.

According to Recommendation 1 of the Financial Action Task Force (FATF³), countries must identify, assess, and understand the risks of financing the proliferation of WMD, which are associated with the actual or potential violation, non-application, or evasion of financial sanctions referred to in FATF Recommendation 7. FATF Recommendation 7 currently applies only to the targeted financial sanctions (TFS) imposed on the Democratic People's Republic of Korea (North Korea) by UN Security Council Resolution 1718⁴.

This analysis takes a somewhat broader view of the risks of financing the proliferation of WMD and goes beyond the requirements of FATF Recommendation 1, which focuses on compliance with TFS obligations related to North Korea. The analysis includes Estonia's exposure to indirect risks of financing the proliferation of WMD. This approach is in line with common practice⁵, where several countries have decided to analyze the risks of financing the proliferation of WMD more broadly than just compliance with TFS obligations. Considering that sanctions⁶ under UN Security Council Resolution 1718 are directly imposed on only 80 individuals and 75 entities⁷ (hereinafter also referred to as designated persons), it is clear that most activities related to financing the proliferation of WMD are not directly related to these designated individuals and entities. Instead, most of the fundraising and technology acquisition is carried out by individuals who are not on the sanctions list. This is clearly indicated by the PoE⁸ reports, which have identified over 5000⁹ additional entities that are in various ways connected to North Korea. The aim of broadening the focus is to make the risk assessment as practical as possible for all market participants and institutions. Although the risk assessment addresses risks related to sanctions more broadly (including trade sanctions), it provides a specific assessment only of the risks related to targeted financial sanctions.

The data used in the risk assessment covers the period from 2020 to 2024 (hereinafter referred to as the "observed period").

³ The FATF Recommendations <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
⁴ S/RES/1718 (2006) [S/RES/1718 \(2006\)](https://www.un.org/pressdocs/2006/sres1718.html) | Security Council

⁵ Crafting Robust Proliferation Financing National Risk Assessments <https://rusi.org/explore-our-research/publications/policy-briefs/crafting-robust-proliferation-financing-national-risk-assessments>

⁶ Primarily the freezing of assets and the prohibition of making financial resources available.

⁷ Sanctions List Materials <https://main.un.org/securitycouncil/en/sanctions/1718/materials?utm>

⁸ The UN Security Council DPRK Sanctions Regime Expert Committee.

⁹ DPRK Reports Database <https://www.rusi.org/explore-our-research/projects/dprk-reports-database>

1. The Risk Assessment Process

To assess the risks in the field of WMD, a separate working group was established. The working group was led by the Ministry of Foreign Affairs and included representatives from the Financial Intelligence Unit (FIU), the Financial Supervision Authority (FSA), the Tax and Customs Board (TCB), the Internal Security Service (ISS), the Prosecutor's Office, the Ministry of Justice, the Ministry of Economic Affairs and Communications, and the Ministry of the Interior¹⁰. Additionally, the Information System Authority was involved. The risk assessment took place from September 2024 to June 2025.

In the first phase of the process, initial consultations were conducted between institutions, necessary statistics were collected, typologies were mapped, and additional training was carried out to implement the chosen methodology. The private sector was involved through surveys and an information day, as well as during the review of the initial version of the WMD risk assessment report.

1.1. Definitions and Terms

According to the FATF definition¹¹, the financing of the proliferation of WMD involves the use of financial resources or the provision of financial services that are used wholly or partly for the production, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their delivery systems and related materials (including technologies and dual-use goods used for illicit purposes), in violation of national laws or international obligations.

According to the FATF methodology, the risk¹² of financing the proliferation of WMD may arise from the following activities:

- Violating or failing to apply financial sanctions: this occurs when designated persons or entities have access to financial services, funds, or assets due to inadequate communication, lack of clear obligations, or the implementation of inadequate procedures by financial institutions and designated non-financial businesses and professions (DNFBPs). Examples include weak background checks when establishing business relationships, insufficient monitoring of business relationships, inadequate employee awareness, improper risk management, insufficient systems for monitoring sanctioned persons lists, or generally poor risk management systems.
- Evading financial sanctions or enabling their avoidance: this occurs when designated persons or entities make efforts to escape the application of financial sanctions. Examples include using shell or front companies, straw men, or intermediaries/advisors who help avoid the application of laws.

¹⁰ Hereinafter, the representatives of these institutions are collectively referred to as the working group.

¹¹ Combating Proliferation Financing
<https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf.coredownload.inline.pdf>, p. 11.

¹² Guidance on Proliferation Financing Risk Assessment and Mitigation
<https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html>, p. 3.

There is no universally agreed-upon international definition¹³ of the financing of the proliferation of WMD. The FATF definition serves as the basis for this risk assessment, but this assessment also considers the financing of WMD proliferation more broadly. In the context of this risk assessment, the concept of financing the proliferation of WMD includes activities that contribute to such financing methods as fundraising, providing financial services, or conducting transactions. However, the final risk assessment is based solely on the violation, non-application, or evasion of financial sanctions referred to in FATF Recommendation 7.

1.2. Methodology

The methodological basis for this risk assessment is the methodology guide¹⁴ for countering the financing of the proliferation of WMD developed by the The Royal United Services Institute (RUSI, UK).

The RUSI methodology for assessing the risks of financing the proliferation of WMD is suitable as a starting point for Estonia, as it is based on internationally recognized FATF standards, but also takes into account the specificities of small-scale and open economies. The methodology directs the analysis of both direct and indirect risks of financing the proliferation of WMD, which is important in the context of Estonia's geopolitical position and open economic environment.

Table 2. Explanation of the risk scale and levels used in the risk analysis

HIGH	MEDIUM	LOW
The risk requires immediate attention. The financing of the proliferation of weapons of mass destruction is widespread, and there are many obstacles to its detection or prevention. Violations are very likely to continue.	The risk is moderate and requires further assessment. There is evidence of some financing of the proliferation of weapons of mass destruction, and there are some obstacles to its detection or prevention. Violations may continue.	The risk is acceptable but requires monitoring. There is little evidence of financing the proliferation of weapons of mass destruction. An increase in the number of violations over the next two years is unlikely.

After the initial information gathering from public and official sources, the working group members compiled two lists: one of potential threats¹⁵ and the other of vulnerabilities¹⁶. To assess the relevance of threats and vulnerabilities, the risk assessment tool¹⁷ provided in the methodology was used. In this way, the experts reached a consensus on which threats and vulnerabilities are significant in the Estonian context. Therefore, the focus was primarily on the methodological identification of threats and vulnerabilities. Taking into account the threats and vulnerabilities, the working group analyzed the existing mitigation measures¹⁸ and thus determined the residual risk¹⁹.

¹³ Combating Proliferation Financing <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf.coredownload.inline.pdf>, p. 7.

¹⁴ Guide to Conducting a National Proliferation Financing Risk Assessment: 2024. <https://static.rusi.org/guide-to-conducting-proliferation-risk-assessment-2024.pdf>

¹⁵ Threats refer to individuals, entities, objects, or activities that may potentially cause the risk of financing weapons of mass destruction.

¹⁶ Vulnerabilities refer to factors that threats can exploit or that may support or facilitate threats.

¹⁷ Guide to Conducting a National Proliferation Financing Risk Assessment: 2019. [20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf](https://static.rusi.org/guide-to-conducting-a-national-proliferation-financing-risk-assessment-web.pdf), p. 66-68.

¹⁸ Mitigation measures are relief measures used to reduce risk. This includes the effectiveness, capacity, and capability of the state – government, law enforcement agencies, and the private sector.

¹⁹ Residual risk refers to the level of risk that remains after the implementation of compliance measures and control systems aimed at mitigating identified threats and vulnerabilities.

Regarding the potential consequences of the realization of threats, the working group held discussions, but no separate assessments were made for the consequences. This is in line with the updated FATF guidelines, which allow countries to focus primarily on identifying their national threats and vulnerabilities, considering the difficulties in assessing the consequences of financing the proliferation of WMD. Ultimately, the consequences of financing the proliferation of WMD are more severe than those of money laundering or other financial crimes, as the use of WMD can result in significant economic damage, political instability, and loss of life.

In Estonia, the same legal and supervisory framework used to ensure compliance with other sanctions primarily functions as a mitigation measure to prevent the financing of the proliferation of WMD. Therefore, this risk assessment broadly addresses the Estonian sanctions implementation system to the extent that it overlaps with the framework for preventing the financing of the proliferation of WMD.

1.3. Data Collection

For risk assessment, information from both official and public sources was relied upon. Among the official sources, the suspicious transaction reports (STR) submitted by the FIU, information from the Internal Security Service, external payment statistics from the Bank of Estonia, trade data from the Tax and Customs Board, and information available to the Strategic Goods Commission were of significant importance. The Prosecutor's Office provided additional information regarding criminal cases initiated on the grounds of sanctions violations and related crimes. Studies conducted by the FIU during the observed period were also used as input. All official data were collected during the period 2020–2024 (hereinafter referred to as the “observed period”).

In addition, data from a private sector survey, the Business Register, and the Statistics Estonia database were used. The national threats and vulnerabilities identified in the working groups for the national risk assessment of money laundering and terrorist financing conducted during the same period were also relevant in the context of financing the proliferation of WMD.

Furthermore, public sources were used to identify information and find references to potential WMD proliferation financing risks related to Estonia. As a regional background, the national risk assessments of other countries in our region were used to map regional trends and potential indirect risks that may affect Estonia. These provided a comparative framework to better understand the WMD proliferation networks and financing methods considered significant by our neighboring countries.

Among the public sources, the FATF typology study²⁰, reports from UN PoE experts, as well as studies from RUSI²¹ and King's College London on WMD proliferation financing typologies²² were used. Additionally, reports and blog posts from two leading blockchain analysis tool providers, describing threats and typologies related to North Korean hacker groups and cryptocurrencies, were analyzed.

²⁰ FATF, 'Proliferation Financing Report'

²¹ Proliferation Financing <https://www.rusi.org/explore-our-research/topics/proliferation-financing>

²² Study of Typologies of Financing of WMD Proliferation
<https://www.kcl.ac.uk/csss/assets/study-of-typologies-of-financing-of-wmd-proliferation-2017.pdf>

2. Legal and Regulatory Framework

2.1. International Framework

Estonia is fully committed to long-term nuclear disarmament goals and preventing the proliferation of weapons of mass destruction (WMD). We have joined all major disarmament and non-proliferation treaties, including the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Comprehensive Nuclear-Test-Ban Treaty (CTBT), the Chemical Weapons Convention (CWC), the Biological Weapons Convention (BWC), and the Geneva Convention on Certain Conventional Weapons (CCW).

Estonia is a member of the three most important international export control regimes: the Wassenaar Arrangement (WA), the Nuclear Suppliers Group (NSG), and the Australia Group (AG), whose lists and best practices are implemented at the national level primarily through export control. The purpose of export control is to ensure effective control over the supply of goods used for the production of WMD and conventional weapons, to ensure that such goods are used for purposes that do not threaten peace, security, and human rights.

Sanctions are also an important tool in preventing the proliferation of WMD through the implementation of export control measures. As a member state of the European Union, Estonia implements sanctions primarily through EU legislation. If the EU has not yet adopted an international sanctioning legal act, the sanction is temporarily implemented based on a UN Security Council resolution (ISA²³ § 8 (1-2)). During this period, all natural and legal persons are obliged to immediately apply the sanction according to the conditions set out in the resolution.

Currently, there are approximately 50 different sanction regimes in place in the European Union, covering both geographical (e.g., specific countries or regions) and thematic (e.g., WMD proliferation, terrorism, cyber-attacks) restrictions. The necessary legislation has been adopted in Estonia to implement sanctions, and competent authorities have been designated based on the content of the prohibition.

²³ International Sanctions Act (ISA) <https://www.riigiteataja.ee/akt/117052025003>

2.2. National Framework

National Coordination

Estonia's system for preventing the financing of the proliferation of WMD is based on the cooperation of several different state agencies, with the Ministry of Foreign Affairs playing a central role. The Ministry leads two main cooperation formats important for preventing the financing of WMD proliferation: the National Implementation Steering Group for International Sanctions (hereinafter referred to as the "Steering Group")²⁴ and the Strategic Goods Commission (hereinafter referred to as the "Commission")²⁵. The tasks of the Steering Group include coordinating inter-agency cooperation and making proposals to government agencies and the Government of the Republic or the Riigikogu committees regarding the International Sanctions Act (ISA) and its implementation practices or their amendments, as well as the risks of violating international sanctions. The Commission, in turn, discusses issues related to the restrictions on the transportation of goods, the provision of services related to goods, and the making of transactions stipulated in the sanctioning or implementing legal act, and decides on them. The Commission also has the authority to issue licenses for the cross-border supply and transit of strategic goods and for the provision of services specified²⁶ in the legal acts.

Competent Authorities

The implementation of international sanctions in Estonia is divided among various state agencies according to their competence, as stipulated in § 11 of the ISA. Each agency is responsible for implementing specific types of sanctions – for example, the Police and Border Guard Board handles entry bans, and the FIU is responsible for implementing financial sanctions and supervising market participants within its jurisdiction. The Financial Supervision Authority oversees credit institutions, insurance companies, investment firms, pension funds, payment and e-money institutions, and other financial market participants and companies. The Consumer Protection and Technical Regulatory Authority and the Tax and Customs Board handle restrictions on the import and export of services or goods. The Defence Forces and the Transport Administration implement movement restrictions at sea and in the air.

Competent authorities must prepare administrative acts and perform relevant actions, respond to inquiries from investigative bodies related to sanctions, collect and transmit relevant data to them, including information on sanctions violations. In Estonia, pre-trial investigations related to sanctions violations are conducted by either the Tax and Customs Board or the Internal Security Service, depending on the nature of the violation. The Tax and Customs Board primarily deals with violations of import or export bans, while the Internal Security Service investigates cases related to financial sanctions or the proliferation of WMD. Pre-trial investigations related to sanctions violations are led by the Prosecutor's Office. If no competent authority is designated by law for a specific restriction, the Ministry of Foreign Affairs makes a proposal to the Government of the Republic to designate the responsible authority.

²⁴ This includes the Ministry of Foreign Affairs, the Bank of Estonia, the Financial Supervision Authority, the Ministry of Education and Research, the Ministry of Justice and Digital Affairs, the Ministry of Defence, the Internal Security Service, the Defence Forces, the Ministry of Climate, the Ministry of Culture, the Ministry of Economic Affairs and Communications, the Tax and Customs Board, the Police and Border Guard Board, the Ministry of Finance, the Financial Intelligence Unit, the Government Office, the Prosecutor's Office, the Ministry of the Interior, the Consumer Protection and Technical Regulatory Authority, the Transport Administration, and the Foreign Intelligence Service.

²⁵ This includes the Ministry of Foreign Affairs, the Ministry of Defence, the Ministry of Economic Affairs and Communications, the Tax and Customs Board, the Internal Security Service, and the Police and Border Guard Board.

²⁶ Application for a strategic goods license

<https://www.vm.ee/tegevus-valdkonnad/strateegiliste-kaupade-kontrollstrateegilise-kauba-eriloo-taotlemine#samm-1-kas-kaup-on>

The implementation of export control is handled by the inter-agency Strategic Goods Commission established under the Ministry of Foreign Affairs. Although the Financial Intelligence Unit is not part of the commission, the commission has the right to contact the FIU. The commission's task is to ensure effective control over the supply of goods used for the production of WMD and conventional weapons.

Estonia's legal regulation of export control is characterized by the fact that the export, transit, and related services of WMD, materials, hardware, software, and technology used for their production are prohibited by general provisions, regardless of the destination country. The use of the listed types of weapons is prohibited by international agreements, and therefore, even with a special permit, the transportation of WMD through Estonia is not possible.

Various registry keepers also perform controls. Specifically, the registry keepers of the state information system databases must refuse entries that violate international sanctions. This obligation extends to 18 specific registry keepers (see § 13¹ of the ISA), including the Business Register, the Land Register, and the Register of Beneficial Owners. If a registry keeper identifies a sanctioned entity or a transaction that violates sanctions, they must apply the sanction and report the competent authority.

Supervision

The International Sanctions Act (ISA) stipulates that obligated entities must implement a financial sanctions risk mitigation and management system to ensure compliance with financial sanctions and prevent violations. Obligated entities are defined under § 20 of the ISA and include, for example, credit institutions, notaries, lawyers, accountants, and other financial and non-financial sector service providers. Their obligations include, among other things, implementing due diligence measures, identifying clients, checking financial sanctions lists, and reporting suspicious transactions and the application of financial sanctions to the FIU. Such a system helps identify financial activities that may be related to the financing of the proliferation of WMD.

To support the supervision of obligated entities, a multi-level supervisory system has been established. The FIU, the Financial Supervision Authority, the Chamber of Notaries²⁷, and the Bar Association are all responsible for ensuring that the obligated entities under their supervision have the appropriate risk mitigation and management systems in place, enabling them to identify and apply financial sanctions.

Penalties

Estonian criminal law provides for strict measures for violations of international sanctions (including those related to the financing of the proliferation of WMD) and the illegal transportation of strategic goods and related services. Section 93¹ of the Penal Code stipulates that violating an international or Government of the Republic sanction – for example, conducting a transaction or providing a service prohibited by the sanction – is punishable by a fine or up to five years of imprisonment. Even stricter penalties are provided for activities related to WMD. For example, under § 93, the development, production, or transfer of weapons – such as chemical or biological weapons – is punishable by up to twelve years of imprisonment.

The illegal transportation of strategic goods and the provision of related services are separately regulated in §§ 421¹ and 421² of the Penal Code. The first addresses cases where the movement of goods or services occurs without the proper authorization, while the second deals with situations involving completely prohibited goods or services. All the aforementioned criminal offenses are necessary to ensure that Estonia can penalize various violations related to the proliferation of WMD when needed.

²⁷ The competent and responsible authority is the Ministry of Justice and Digital Affairs, which has delegated this task to the Chamber of Notaries (ISA §30 (5)).

Summary

In general the working group assesses Estonia's current legal framework for countering the financing of WMD as adequate and effective. This is also confirmed by the results of the latest MONEYVAL evaluation (2022), where the effectiveness of Estonia's implementation of international financial sanctions was rated as "significant"²⁸. However, the working group noted that Russia's full-scale aggression against Ukraine has significantly increased the workload related to sanctions, especially in the Financial Intelligence Unit, the Tax and Customs Board, the Prosecutor's Office, and investigative bodies. At the same time, no additional resources have been allocated to match the increased workload, which has jeopardized the effective and consistent implementation of measures.

²⁸ FATF's Immediate Outcome 11 (IO11) addresses the effectiveness of implementing international financial sanctions.

3. Threats

From the perspective of countering the financing of WMD proliferation, the working group considers it important to monitor two high-risk countries – North Korea and Iran. The primary threat to the financing of WMD proliferation is Russia, due to its geographical proximity and its increasingly close cooperation in arms development with both North Korea and Iran. Russia has also signed military cooperation agreements (*Treaty on Comprehensive Strategic Partnership*) with both countries, specifically with Iran²⁹ on January 17, 2025, and with North Korea on June 19, 2024. The agreement with North Korea includes cooperation in the fields of finance, investment, and banking.³⁰

3.1. North Korea

North Korea (hereinafter referred to as “DPRK”) has been under international sanctions since 2006, when the country conducted its first nuclear test. United Nations Security Council Resolution 1718 demanded that the DPRK cease its nuclear tests and imposed sanctions on the country. These sanctions apply to the entire DPRK, but primarily to individuals and entities associated with the DPRK’s WMD program. Although the sanctions imposed under the resolution remain in force, no new individuals have been added³¹ to the DPRK sanctions list in the past six years. The European Union has imposed separate sanctions on DPRK individuals in connection with its nuclear tests, missile program, and military support to Russia in the war in Ukraine.³²

In general, the following restrictions³³ apply to the DPRK:

- Arms embargo (prohibition on the direct or indirect supply, sale, or transfer of arms and related materials of all types, including weapons, ammunition, and military equipment, as well as the provision of technical advice, assistance, or training related to military activities);
- Travel restrictions (individuals listed on the sanctions list are prohibited from entering the territory of a member state);
- Financial restrictions (all assets and economic resources of sanctioned individuals and entities are subject to freezing, and it is prohibited to make financial resources and economic resources available to them);

²⁹ Announcement, January 17, 2025 <http://en.kremlin.ru/events/president/news/76101>

³⁰ Order on signing a Treaty on Comprehensive Strategic Partnership between Russia and North Korea • President of Russia <http://en.kremlin.ru/acts/news/74321>

³¹ The last time new parties were added to the list was on March 30, 2018. Resolution 2397 (2017) added one individual and 21 entities to the sanctions list.

³² DPRK: EU sanctions nine additional individuals and entities involved in the country’s activities related to illegal weapons programmes and supporting Russia’s war of aggression against Ukraine. <https://www.consilium.europa.eu/en/press/press-releases/2024/05/31/dprk-eu-sanctions-nine-additional-individuals-and-entities-involved-in-the-country-s-activities-related-to-illegal-weapons-programmes-and-supporting-russia-s-war-of-aggression-against-ukraine/>

³³ Security Council Committee established pursuant to resolution 1718 (2006). <https://main.un.org/securitycouncil/en/sanctions/1718>

- Prohibition on the provision of services (prohibition on providing technical assistance, brokerage services, financing or financial assistance, and other services related to the arms embargo).

There are several other specific prohibitions against the DPRK, such as the prohibition on providing services to vessels related to North Korea, the prohibition on importing seafood and textiles, the ban on exporting luxury goods, and the prohibition on issuing work permits to North Korean citizens.

3.2. Iran

Initial UN sanctions were imposed on Iran under UN Security Council Resolution 1737³⁴ after Iran refused to comply with Resolution 1696, which demanded the cessation of its uranium enrichment program. This resolution was the first of several that imposed targeted financial sanctions on individuals and entities associated with Iran's nuclear program.

UN Security Council Resolution 2231 endorsed the Joint Comprehensive Plan of Action³⁵ (JCPOA), under which Iran agreed to limit its nuclear program in exchange for sanctions relief and other agreements. According to Resolution 2231, the targeted financial sanctions imposed on individuals and entities associated with Iran's nuclear program were lifted in October 2023³⁶, and the relevant FATF recommendations no longer apply to them. However, as Iran did not honor the terms of the JCPOA, the UN Security Council decided to continue applying restrictive measures against Iran. These measures primarily include additional restrictions on the trade of dual-use goods and technology, restrictions on the trade of essential equipment and technology used in the petrochemical industry, a ban on the import of Iranian crude oil, petroleum products, and petrochemical products, and a ban³⁷ on investments in the petrochemical industry.

In the following text, North Korea and Iran are also referred both as WMD risk countries.

3.3. Russia: A Significant Evasion Channel

The UN has not imposed sanctions on Russia related to the financing of WMD proliferation. At the same time, the European Union has imposed extensive sanctions on Russia, including trade restrictions, financial sector restrictions, travel bans, and obligations to freeze and make assets unavailable. The aim of the sanctions imposed on Russia is to weaken its economic capacity to continue its aggression in Ukraine and are not intended to prevent the proliferation of WMDs and their financing. In this analysis, Russia is not assessed as a separate WMD risk country, but as a significant channel that Iran and North Korea may use to evade restrictions related to the financing of WMD proliferation.

³⁴ S/RES/1737 (2006) <https://main.un.org/securitycouncil/en/s/res/1737-%282006%29>

³⁵ Resolution 2231 (2015) on Iran Nuclear Issue <https://main.un.org/securitycouncil/en/content/2231/background>

³⁶ Sanctions Map: Iran <https://www.sanctionsmap.eu/api/v1/pdf/regime?id%5B%5D=17&id%5B%5D=18&include%5B%5D=guidances&lang=en>

³⁷ Council Regulation (EU) No 267/2012, March 23, 2012. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32012R0267>

3.4. Threats Related to WMD High-Risk Countries and Russia

The working group identified threats based on three main categories of activities³⁸ related to the financing of WMD proliferation. These three categories essentially reflect the main activities of WMD risk countries, how they acquire the resources needed for WMD financing, and how they conduct transactions for the purpose of financing WMD proliferation.

Financial products and services directly related to the trade of goods associated with WMD proliferation.

This category is the narrowest and includes the provision of financial products and services related to the trade of goods that can be directly used in WMD development. It also includes financial products and services related to the import or export of these goods and their transportation – for example, trade finance, maritime or cargo insurance, and export guarantees.

Revenue-generating activities

This category includes any economic activity that can generate revenue for participants from WMD risk countries. Countries most affected by this area of activity often have historical and cultural ties with WMD risk countries. For example, various restrictions have been imposed on participants associated with North Korea to conduct economic activities abroad, and they use the following measures, among others, to generate funds:

- Legitimate economic activities that may support the development of nuclear and missile programs (e.g., IT services, restaurants, and textile exports);
- Illegal economic activities, such as labor exploitation, cybercrime, counterfeiting of goods, smuggling, coal and arms sales, and providing maintenance for weaponry.

Business and Financial Infrastructure Enabling Transactions for WMD Financing

This category encompasses both the trade of goods and services sensitive to WMD proliferation and revenue-generating activities, including necessary financial services. Participants from WMD risk countries use various business and financial structures to ensure access to the international financial system and to conduct transactions necessary for WMD proliferation financing. Common methods for evading sanctions include providing false information or otherwise concealing their true identity. Additionally, jurisdictions with weaker controls on anti-money laundering, counter-terrorism financing, and international sanctions compliance are often used.

An additional threat can be considered the increasing transaction volumes with the UAE, which Russia³⁹ and Iran⁴⁰ have previously used to evade sanctions.

³⁸ Guide to Conducting a National Proliferation Financing Risk Assessment
https://static.rusi.org/20190513_guide_to_conducting_a_national_proliferation_financing_risk_assessment_web.pdf p. 12-15

³⁹ Fortune Hunting: Russia and Sanctions Evasion <https://hir.harvard.edu/fortune-hunting-russia-and-sanctions-evasion/>

⁴⁰ Busted Sanctions: Explaining Why Economic Sanctions Fail
<https://www.sup.org/books/politics/busted-sanctions/excerpt/introduction>

The working group assessed the following threats from the three categories mentioned above as significant (1-5). Each threat is illustrated with 1-2 case examples.

1. The use of obligated entities (credit institutions, virtual currency service providers, financial institutions, and other obligated entities) for transactions or services aimed at financing the proliferation of WMDs.

CASE EXAMPLE 1

A citizen of an EU member state, who, according to public data (such as UN expert committee reports), has connections with the mediation of technology required for virtual currency mining to North Korea, opened an account with a virtual currency service provider licensed in Estonia. The individual had been a client of the Estonian service provider for a few months when they were declared wanted by a third country. Based on this information, the Estonian service provider identified the individual's connection to North Korea. The service provider took due diligence measures, terminated the client relationship, and reported it to the Financial Intelligence Unit. The Financial Intelligence Unit analyzed the individual's transactions and shared information with the third country that had declared the individual wanted, and with the EU member state where the individual was located according to the Financial Intelligence Unit's analysis. Reportedly, the individual was arrested in the same EU member state a few months later based on the third country's request for legal assistance.

2. The use of Estonian companies for transactions aimed at financing the proliferation of WMDs, including the use of virtual currency service providers or other intermediaries to create shell companies for transactions related to WMD proliferation financing.

CASE EXAMPLE 2

In March 2023, the Estonian Internal Security Service detained an Estonian citizen suspected of illegally procuring high-tech electronics of U.S. origin for the benefit of the Russian military. According to the investigation, the individual was involved in a complex scheme to acquire embargoed electronic components that could be used for military purposes. They operated through several companies registered in Estonia, using aliases and third parties to conceal the end user and evade U.S. and EU export controls. The U.S. requested their extradition, citing export crimes and violations of the international sanctions regime.

3. Organizing a cyberattack against virtual currency service providers licensed in Estonia with the aim of obtaining funds to be used for financing the proliferation of WMDs.

CASE EXAMPLE 3

In 2023, a virtual asset service provider (VASP) registered in Estonia fell victim to a cyberattack, during which approximately 35 million euros worth of virtual currencies were stolen. According to the UN and cybersecurity experts, the attack was carried out by a state-sponsored hacker group from North Korea, known for committing cybercrimes to fund North Korea's weapons programs. Similar attack attempts have also been made against other virtual currency service providers associated with Estonia.

4. The exploitation of individuals residing in Estonia or having connections to Estonia (e.g., through e-residency) for transactions related to the financing of WMD proliferation.

CASE EXAMPLE 4

An Estonian-registered company and its e-resident founder were suspected of potentially supporting North Korea's WMD program. The individual (a Chinese national) offered web design and software development services through the company, possibly with the aim of raising funds for the WMD program. The company had no substantial connection to Estonia beyond its registration – it operated entirely outside Estonia, did not have accounts in Estonia, and has since been liquidated, with the founder's e-residency revoked. The investigation revealed that all of the company's financial transactions were conducted through a payment intermediary, and most counterparties were located outside the EU. Most of the funds collected through the provision of services were transferred to accounts of a credit institution operating in Liaoning Province, China. It was not proven that the company operated with the aim of financing the WMD program, but there were several indirect indications, and the above aligns with common typologies associated with North Korea.

CASE EXAMPLE 5

A Russian citizen e-resident (whose e-residency status has now been revoked) established a limited liability company in Estonia in 2021, which was used to mediate aircraft parts to Central Asian countries. The actual beneficiary and the authorized representative of the company were both Russian citizens. These individuals were also connected to a logistics company registered in Bahrain, from which payments were made to the Estonian limited liability company, whose bank accounts were located in Lithuania. The analysis of transactions showed that payments were made through the Estonian limited liability company to suppliers mainly based in the USA. Transactions were also identified with a company registered in Kyrgyzstan, which was added to the sanctions list by OFAC in 2023 for cooperating with the Russian aviation sector. The Estonian company was likely used as a channel to order goods under export restrictions, including dual-use items, from the USA and other countries, which were then mediated through Bahrain to Kyrgyzstan and further to Russia.

5. The use of Estonian territory for the transit of goods necessary for WMD development to Russia and from there to WMD risk countries.

CASE EXAMPLE 6

In December 2022, the Estonian Internal Security Service detained a Russian citizen in Tallinn, suspected of extensive violations of international sanctions and export controls. The individual allegedly acted on behalf of Russian security services and was part of an international procurement network that supplied high-tech components and ammunition from U.S. companies to the Russian defense industry. One of the main transit points for the suspect was Estonia, through which export-controlled electronic devices and semiconductors were transported across the border to Russia. The suspect's activities were linked to sanctioned Moscow-based companies that operated under the directives of the Russian armed forces. In the summer of 2023, the suspect was extradited to the U.S., where they were charged with conspiracy, illegal trade, and money laundering. U.S. authorities described the network in which the suspect operated as a "tool of the Russian Federation's war machine" and imposed sanctions on several associated individuals and companies. According to the indictment, the network sought to procure high-tech components that could be used in both the military industry and research and development. Additionally, export-restricted goods were found in the suspect's possession, which they attempted to transport to Russia.

4. Vulnerabilities

The working group has identified six main vulnerabilities and divided them into three main categories. The first category includes vulnerabilities related to the economic and trade environment, including export and import flows and vulnerabilities associated with being in a transit corridor. The second category includes vulnerabilities related to new technologies and sector-specific vulnerabilities. The third category highlights legislative and administrative bottlenecks that may hinder the enforcement of sanctions, supervision, and information exchange. The description of all six main vulnerabilities is provided below, and the measures to mitigate them are presented in Chapter 5.

4.1. Vulnerabilities Related to the Economic and Trade Environment

Estonia's vulnerability lies in its geographical proximity to Russia and the interconnected economic and community relations.

Due to its geographical location and cross-border community ties, Estonia has historically engaged in economic cooperation with Russia. Until the full-scale war in Ukraine began in 2022, Russia was one of Estonia's main export destinations. In addition to Estonia's own exports, transit from other countries, mainly EU member states, to Russia also passes through Estonia, which constitutes the majority of the trade volume directed towards Russia.⁴¹ This allows participants from WMD risk countries, primarily Russia, to use Estonia to evade sanctions, including those related to WMD financing. This is evidenced by the fact that the prosecutor's office initiated 191 criminal proceedings on suspicion of sanctions violations⁴² during the period under review, most of which are related to trade with Russia. The exploitation of Estonia to evade sanctions can take various forms, such as using Estonian territory for the transport of goods to Russia or using legal entities established in Estonia for transactions whose ultimate goal is to pay for goods related to WMDs.⁴³ Additionally, goods or assets that have already reached Russia may be used for the benefit of Iran and North Korea's WMD programs.

Estonia is significantly less vulnerable to participants originating directly from Iran and North Korea due to its geographical distance, the small size of the community, and the lack or scarcity of financial and economic ties. Furthermore, neither of the WMD risk countries has an embassy in Estonia that could be used for activities necessary for WMD proliferation financing. The Iranian community in Estonia is also small⁴⁴, and there is no North Korean community in Estonia.

⁴¹ What does Estonia import from the Democratic People's Republic of Korea (DPRK)? (2022)
https://valiskaubandus.stat.ee/visualize/tree_map/import/kp/all/2022/?locale=et

⁴² Penal Code § 931 *Karistusseadustik–Riigi Teataja*

⁴³ See case examples.

⁴⁴ As of 2024, there were 88 Iranian citizens with valid residence permits in Estonia.

4.2. Vulnerabilities Related to Technology and Sectors

Virtual Asset Service Providers (VASPs) are becoming an increasingly important part of the international financial system, but they are also a target for cybercrime.

Compared to credit institutions, Estonian licensed VASPs are often more vulnerable because their IT systems and information security solutions are not on the same level as those of credit institutions. Additionally, several characteristics of blockchain technology make them more vulnerable, for example, transactions made with cryptocurrencies generally cannot be reversed.⁴⁵ The PoE expert group's report highlights that the number and extent of cyberattacks organized by North Korea have increased at least since 2017. Public sources have reported a 2024 incident involving an Estonian licensed VASP, where North Korean hackers allegedly stole virtual currencies worth more than 4 million euros from the service provider.

The client base of VASPs is global and diverse, including representatives from various countries. According to the RAB, as of the end of 2024, Estonian licensed VASPs had over 1.6 million clients, of which slightly more than 0.7 million were active (service users). The sector's turnover across different services was 32 billion euros.⁴⁶ Only an average of 5% of transaction volumes across different crypto services are related to Estonian resident clients. Transactions are also conducted with high-risk jurisdictions, such as Iran. The pseudonymity of virtual currencies makes it difficult to identify and monitor suspicious transactions. Most VASPs rely on external service provider solutions to detect sanctions violations, which mostly identify only contacts with sanctions imposed by the USA and Israel.⁴⁷ It is known that funds have likely been moved through a previously licensed Estonian VASP for the benefit of North Korea⁴⁸. It is known that parties acting on behalf of North Korea use offshore casinos to move funds related to the proliferation of weapons of mass destruction, and Estonian VASPs also have several clients from offshore casinos⁴⁹.

Awareness of the risks associated with the financing of the proliferation of WMD is low in some sectors, and there are deficiencies in their procedures and control mechanisms for preventing WMD proliferation financing.

Approximately 12% of financial institutions, 20% of CSPs, and 10% of gambling operators reported in a survey that they lack a risk management system for preventing WMD proliferation financing. This is a legal requirement, and without it, market participants cannot effectively identify transactions or client relationships suspected of financing WMD proliferation.

The CSP sector also stood out for its low awareness. According to the FIU, the sector of CSPs the activity in reporting sanctions evasion is lower than expected.⁵⁰ Reports indicate that sanctions violations are detected randomly and with significant delays, rather than through transaction monitoring. Among CSPs, only about

⁴⁵ Some things you need to know <https://bitcoin.org/en/you-need-to-know>

⁴⁶ Summarization across services may result in double counting.

⁴⁷ FIU Yearbook 2024 https://fiu.ee/sites/default/files/documents/2025-04/Rahapesu%20Andmeh%C3%BCroo%20aastaraamat%202024_0.pdf p. 58.

⁴⁸ North Korea uses sanctioned Russian exchange to launder 100M in stolen crypto <https://www.nknews.org/pro/north-korea-uses-sanctioned-russian-exchange-to-launder-100m-in-stolen-crypto/>

⁴⁹ North Korean Activity in the Casino and Gaming Sector: How Do Jurisdictions Respond? https://static.rusi.org/north-korean-activity-in-casino-gaming-industry_0.pdf

⁵⁰ FIU Yearbook 2024 https://fiu.ee/sites/default/files/documents/2025-04/Rahapesu%20Andmeh%C3%BCroo%20aastaraamat%202024_0.pdf, p. 59.

64% screen clients against sanctions lists, and only 50% apply enhanced due diligence measures to clients from countries problematic from a WMD proliferation standpoint. Less than 40% apply these measures to clients dealing with dual-use goods or military goods.

The above suggests, according to the working group, that a significant portion of the DNFBP sector may not fully understand the role they could potentially play in managing companies created to evade sanctions established to prevent the financing of the proliferation of weapons of mass destruction (WMD).

The risk awareness among gambling operators appears to be generally satisfactory based on surveys. According to the survey, 30% of gambling operators are not concerned at all about the risks of WMD proliferation financing, which may indicate that at least some sector participants may underestimate the risks.

VASPs have average due diligence measures from the perspective of WMD proliferation financing (as discussed in the previous section), but their overall awareness of these risks is significantly higher. The awareness and ability of credit institutions and larger financial institutions to identify risks and situations related to sanctions, including those related to WMD proliferation financing, are at a good level. This is confirmed by the screening system checks⁵¹ conducted by the Financial Supervision Authority and the number and quality of reports submitted to the FIU.⁵²

4.3. Legislative and Administrative Vulnerabilities

In Estonia, the establishment of private limited companies, general partnerships, limited partnerships, and non-profit associations is simple and inexpensive for both citizens and foreigners.

The establishment of a private limited company, general partnership, limited partnership, and non-profit association in Estonia is convenient for both Estonian citizens and non-residents and can be done either through the e-Business Register or via a notary. If a person does not have a digital ID, they must contact a notary – it is also possible to use powers of attorney and company service providers. The establishment of a public limited company, foundation, cooperative, apartment association, European company (SE), European economic interest grouping (EEIG), and European cooperative society (SCE) is always done through a notary. According to the Business Register, 87% of companies are established through the e-Business Register. As of 01.02.2023, the residency requirement for board members of all legal entities has been abolished. Additionally, the residency of shareholders, members, or participants is not regulated by corporate law. From the same date, the minimum share capital requirement for private limited companies was also abolished – it is possible to establish private limited companies with a share capital of just 1 cent.

A private limited company is a classic limited liability company where shareholders generally do not bear responsibility for the company's obligations. However, the ease of establishment can lead to a situation where new private limited companies are continuously created, and problematic ones are simply abandoned. For example, a quarter of companies associated with foreign countries showed no signs of active operation between 2020 and 2022 (they did not submit annual reports or VAT declarations in Estonia). These are warning signs of possible misuse of companies for evading sanctions, money laundering, or other crimes.⁵³

⁵¹ See the next chapter for more details.

⁵² The FIU has thoroughly addressed issues related to the substantive and formal quality of reports in the feedback provided to credit institutions titled "FIU Feedback to Credit Institutions", p. 9.
https://fiu.ee/sites/default/files/documents/2025-04/Tagasiside_krediidiasutustele_2024.pdf

⁵³ Foreigners in Estonian companies <https://fiu.ee/valismaalased-est-ettevotetes> p. 7.

The establishment and management of companies in Estonia is simplified for non-residents thanks to the e-residency program, which allows foreigners – including, for example, Iranian citizens – to register a company in Estonia and perform other official activities. Companies associated with e-residents from third countries may be more vulnerable to criminal exploitation, as they have lower activity indicators – approximately 1/3 of companies in this group are inactive for extended periods. Russia stands out in particular, with over 20,300 companies associated with its citizens – this accounts for 26% of all companies associated with foreign countries and nearly 6% of all companies registered in the Estonian Business Register. Additionally, there are over 350 companies⁵⁴, registered in Estonia that are associated with individuals of Iranian origin. As of the end of 2024, there are no companies associated with North Korean citizens in the Estonian Business Register.

Customs, security, or law enforcement cooperation with high-risk countries and jurisdictions used to evade sanctions (including those related to WMD proliferation) is limited or non-existent.

The obstacles lie, for example, in the collection of evidence during the investigation of sanctions violations. This is especially the case when evidence related to the violation can only be collected from a third country. Due to Estonia's geographical location, sanctions-related proceedings are often associated with Russia, with which substantial judicial, security, or law enforcement cooperation has ceased. In practice, it is also challenging to gather information from third countries far from Estonia for the verification of violations or the conduct of proceedings, which high-risk countries for WMD proliferation have exploited to evade sanctions. For example, the FIU has had difficulties obtaining responses to inquiries from certain countries, particularly those related to sanctions violations. Similarly, the Tax and Customs Board has faced difficulties in obtaining responses to inquiries, especially from Central Asian countries, and in verifying the authenticity of documents submitted during customs procedures. Furthermore, investigative authorities and the prosecutor's office encounter obstacles in investigating cases where data is needed as evidence in criminal proceedings, but the person or asset is located in a foreign country where the investigation and cooperation on sanctions crimes are inadequate.

⁵⁴ Foreigners in Estonian companies <https://fiu.ee/valismaalased-est-ettevotetes> p. 24 and 27.

5. Mitigating Measures and Residual Risk

5.1. Economic and Trade Environment-Related Vulnerabilities, Mitigating Measures and Residual Risk

Iran and North Korea

As of May 2025, no cases have been discovered in Estonia, nor has any international information been exchanged indicating that manufacturers of WMDs have succeeded in illegally supplying nuclear, biological, radioactive, or chemical materials from or through Estonia.

From 2020 to 2024, Estonia had no trade with North Korea.⁵⁵ During this period, Estonia primarily exported wood and wood products, peat, medicines, clothing, and to a lesser extent, machinery and equipment to Iran. The export volumes during the observed period were small and clearly in a downward trend⁵⁶. Iran, in turn, imported mainly mineral products, gypsum, nuts, and fruits to Estonia. The Estonian Tax and Customs Board (TCB) controls⁵⁷ all import and export shipments to and from Iran. The total export volume to Iran during the observed period ranged from 400,000 to 3.7 million euros per year. The import volume during the observed period ranged from 110,000 to 500,000 euros per year.⁵⁸

Strict country-specific control criteria have been established for North Korea and Iran, meaning all shipments are checked. According to the TCB, most individuals organizing imports from Iran are residents living in Estonia. The number of companies engaged in trade with Iran is small – there are 15 importing and exporting companies. Therefore, Estonia's direct trade contact with Iran is limited, and with North Korea, it is non-existent and under additional supervision by the TCB.

During the observed period, no payment transactions were made with North Korea through Estonian credit and financial institutions, and only one payment was made with Iran, valued at less than 150 euros.⁵⁹ This is significant because credit institutions account for 99%⁶⁰ of the total volume of cross-border payment transactions. The working group has also separately analyzed the main target countries for payments made through Estonian payment agents during the observed period. The working group concluded that payments are primarily made within the European Union to jurisdictions^{61,62} with a low risk of WMD proliferation financing (excluding Russia). Therefore, the direct exposure of Estonian credit institutions, financial institutions, and payment institutions to Iran is minimal, and to North Korea, it is non-existent.

⁵⁵ Implementation of sanctions: <https://www.emta.ee/maksu-ja-tolliameti-aastaraamat/sanktsioonide-rakendamine>

⁵⁶ Export volumes are also in a downward trend compared to the previous NRA assessment period. 2017: €5.32M; 2018: €3.58M; 2019: €1.44M.

⁵⁷ This also applies to potential trade with North Korea.

⁵⁸ What does Estonia export to Iran(2024) https://valiskaubandus.stat.ee/visualize/tree_map/import/ir/all/2024/?locale=et

⁵⁹ Transactions with Iran made by VASPs are separately addressed, see p. 25.

⁶⁰ The total volume of cross-border transactions by payment agents is 0.02%.

⁶¹ Top 10 destination countries for domestic payment agents during the period 2020–2024: LT, EE, DE, UK, SC, HR, BE, AT, CH, MA.

⁶² Top 10 destination countries for Estonian payment agents during the period 2020–2024: EE, UA, FI, RU, MD, LT, GE, UZ, LT, BY.

Russia

Before Russia's full-scale military action in Ukraine, Russia was one of Estonia's main export destinations. However, by 2024, Russia had fallen to 12th place⁶³ among Estonia's trading partners. From 2020 to 2024, Estonia primarily exported machinery and technical equipment, prepared foodstuffs, and to a lesser extent, chemical products and medical devices to Russia.

Since 2022, the value of goods exported from Estonia to Russia has significantly decreased – in 2024, it was 52% lower than in 2022.

Similarly, Estonia's imports from Russia have also significantly decreased. In 2020, goods worth approximately 1.21 billion euros were imported from Russia, but by 2024, this had shrunk to only 108 million euros⁶⁴ – a 90% decrease. The main import items in 2024 were metals and metal products, rare earth metals, and various mineral products.

Payments from Russia have been in a clear downward trend since the start of the full-scale war in February 2022.⁶⁵ Compared to 2020, the volume of incoming payments in 2024 was 93% smaller. Payments to Russia have decreased even more.⁶⁶ The decline between 2020 and 2024 was 98%. The risks associated with payments to Russia are also mitigated by the fact that most Estonian credit institutions have practically stopped payment services to Russia and Belarus.

Export Control Measures

The Estonian Tax and Customs Board has been enforcing import and export bans on goods related to Russia since 2014 and sanctions against Belarus since 2006. Since 2022, additional sanctions have been imposed on Russia and Belarus, covering both goods and individuals. Therefore, the TCB has long-standing experience in implementing import and export bans at the border. Most of the measures used to enforce restrictions related to the financing of WMD proliferation are the same as those used for other sanctions, such as those imposed on Russia.

As of August 17, 2024, border control has been further tightened, and the Government of the Republic decided to impose 100% customs control to prevent the export of sanctioned goods to Russia. Strict export control has increased the number of detections of sanctioned goods and the number of detections of strategic goods. The tenfold increase in inspections has had a deterrent effect on parties who might want to use Estonian territory to evade sanctions.

Enhanced control is carried out in relation to strategic goods, including materials, equipment, and other dual-use items necessary for the production of WMDs, in connection with Russia. An export license (special permit) is required for the export of these goods. Since February 2022, no export or import licenses have been issued in this category. Customs control criteria have been established for Russia. Transit is also checked, as the transit of strategic goods through Russia is prohibited. This measure also reduces the risk that goods from a third country, which could be used in the development of WMDs, might reach Russia through Estonia. Enhanced control has been applied since 2022 to goods considered to be of higher risk under Article 3k

⁶³ Implementation of sanctions: <https://www.emta.ee/maksu-ja-tolliameti-aastaraamat/sanktsioonide-rakendamine>

⁶⁴ What does Estonia import from Russia? (2024) https://valiskaubandus.stat.ee/visualize/tree_map/import/ru/all/2024/?locale=et

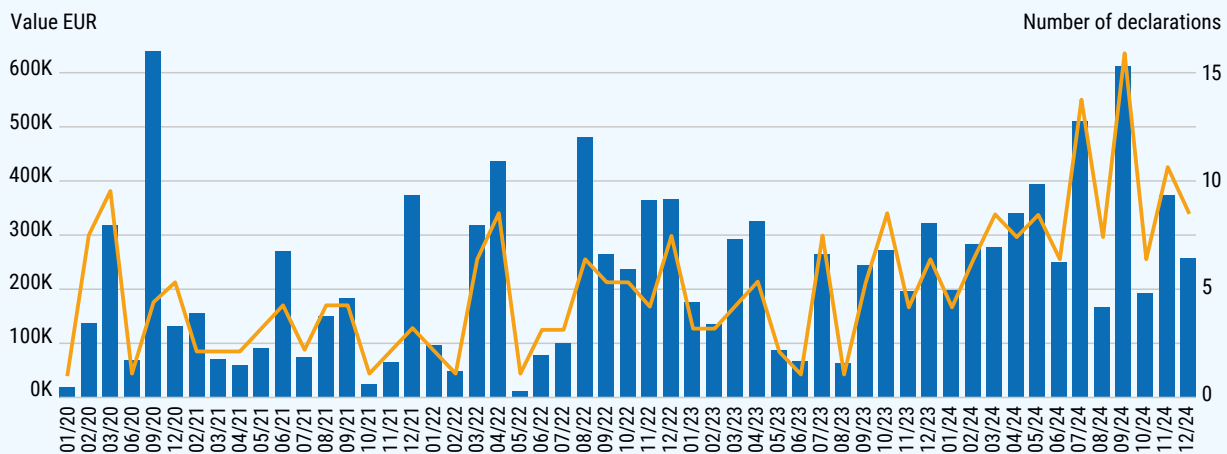
⁶⁵ In 2020, the volume of incoming payments was 1.32 billion euros, in 2021 it was 1.55 billion euros, in 2022 it was 1.01 billion euros, in 2023 it was 388 million euros, and in 2024 it was 87 million euros.

⁶⁶ In 2020, the volume of outgoing payments was 1.03 billion euros, in 2021 it was 1.47 billion euros, in 2022 it was 599 million euros, in 2023 it was 31 million euros, and in 2024 it was 12 million euros.

of Regulation (EU) No 833/2014⁶⁷, which could help increase Russia’s industrial capacity. For example, in 2022–2023, customs conducted 75,530 inspections, detecting 6233 violations.⁶⁸ The proportion of violations is practically equal in terms of imports and exports. The main violators are individuals, and the violations mainly involved cash, consumer electronics, luxury goods, and cars.

When transporting cash from the EU to third countries, a declaration requirement of 10,000 euros applies. The number of declarations on the incoming route is one-third higher than on the outgoing route. The main countries to which cash is taken from Estonia are the United Kingdom, Russia, Switzerland, Norway, and Turkey. Cash is mainly brought to Estonia from the United Kingdom, Russia, Norway, the United States, and Ukraine. The working group has also analyzed the volumes of cash taken to Russia⁶⁹. The amount of cash taken to Russia has significantly increased since 2022, which can be partly explained by the increase in the number of people using Estonia for travel⁷⁰ to Russia. According to the working group, the number of declarants and the total amount of exported funds are largely correlated (see Figure 1). This suggests that the increase in volumes is related to the increase in the number of people traveling through Estonia. In 2024, an average of about 330,000 euros worth of cash was taken across the border to Russia per month, compared to about 150,000 euros in 2020.

Figure 1. Cash outflow from Estonia to Russia



⁶⁷ Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia’s actions destabilizing the situation in Ukraine. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:02014R0833-20240224>

⁶⁸ Most of them were related to the obligation to declare cash and so-called luxury goods.

⁶⁹ No cash imports/exports or related violations have been detected in other AML risk countries.

⁷⁰ The use of Estonian road border points for travel to Russia has increased mainly due to the sanctions imposed on the Russian aviation sector and Finland’s decision to close border points with Russia.

Border crossers are subjected to risk-based and random checks, using various customs and border crossing systems and control criteria. Customs can use modern technical equipment and cash dogs for customs control at all border points. Customs officers undergo annual training that covers various customs risks, interrogation, and inspection techniques. Customs cooperates internationally, sharing and receiving risk information and participating in joint operations.

In 2022, a working group of the Baltic States' customs was established to harmonize the implementation of sanctions and share risk information. Additionally, Estonia has signed a cooperation agreement "Regional approach to ensure uniform customs controls and information exchange for implementation of the EU Restrictive measures." The agreement has also been signed by Latvia, Lithuania, Finland, Poland, and Croatia. The task of the working group is to uniformly implement sanctions in all participating countries and at external borders. There is close operational information exchange to prevent the export of prohibited goods from one country through the border of another.

Domestically, the Tax and Customs Board cooperates closely with the Strategic Goods Commission, the Security Police Board, and the FIU in enforcing export control. In cases where the TCB identifies a situation at the border indicating that economic resources are being made available to a financial sanctions subject or a person acting on their behalf, the TCB submits a report to the FIU. The FIU helps assess whether financial sanctions measures should be applied to the respective goods. During the period under review, the TCB has reported the FIU in 80 cases of suspicion that economic resources are being made available to financial sanctions subjects. This indicates that the TCB is capable of effectively identifying situations where financial sanctions are attempted to be violated, for example, by making goods available to a financial sanctions subject.

Since 2024, credit institutions have an additional obligation to notify the TCB of suspicions or risks of violating the import and export ban on goods. To effectively implement this measure, the TCB and credit institutions have signed a cooperation agreement and implemented an information system that enables operational and bilateral information exchange. Additionally, information exchange between credit institutions and authorities involved in the implementation of sanctions takes place through the Estonian Banking Association's International Sanctions Working Group⁷¹.

As a result, both the volume of trade and payments with Russia have significantly decreased, and authorities have taken additional control measures. Therefore, the level of vulnerability related to the economic and trade environment has decreased during the period under review, especially since 2022. Although the level of vulnerability directly related to Russia has decreased during the period under review, the volume of goods and cash flows with third countries, which Russia is known to have used to circumvent sanctions, has increased⁷² in some cases.

Considering both the threats and mitigating measures, the working group assesses that the residual risk level related to the economic and trade environment is low.

⁷¹ International Sanctions Working Group <https://pangaliit.ee/uldteave/toimkonnad/rahapesu-tokestamise-toimkond/rahvusvaheliste-sanktsioonide-toogrupp>

⁷² The FIU conducted a thorough analysis of goods and cash flows related to Russia in 2024. The study by the FIU: Changes in money and goods flows and the application of financial sanctions after the start of the full-scale war between Russia and Ukraine.

5.2. Measures to Mitigate Technology and Sector-Related Vulnerabilities and Residual Risk

Individuals listed on the UN Security Council sanctions list, or parties under their control, are unlikely to be motivated to hold assets or economic resources in Estonia. This is primarily because the sanctions against North Korea, and previously also against Iran, have been in force for a long time, and market participants are generally aware of the obligations related to these regimes. Estonian authorities are not aware of any cases where market participants have failed to apply the measures prescribed in the sanctioning legal act regarding assets belonging to a person listed on the UN Security Council sanctions list or under their control.

Legal Framework

The primary measure to prevent violations of UN Security Council sanctions is the obligation arising from the ISA to ensure that a person with special obligations has an appropriate system of procedural rules and control mechanisms. This system must enable effective due diligence measures, including adherence to the “know your customer” principle, understanding the nature of business relationships, and identifying beneficial owners. These measures are central to risk mitigation and help avoid situations where services are unknowingly or unintentionally provided through sanctioned entities. The 2024 amendment to the ISA included those entities with special obligations who were already obligated entities⁷³ under the Money Laundering and Terrorist Financing Prevention Act (MLTFPA). Previously, the circle of entities with special obligations was too narrow, but the 2024 amendment to the ISA expanded it to align as closely as possible with the FATF standard⁷⁴. This ensures that both the financial sector and other sectors must have procedural rules and organizational structures that enable the identification, assessment, and implementation of risk-based measures to mitigate the risks of WMD proliferation. Failure to establish and comply with the procedural rules and internal control regulations provided for in the ISA constitutes an offense under the ISA.⁷⁵

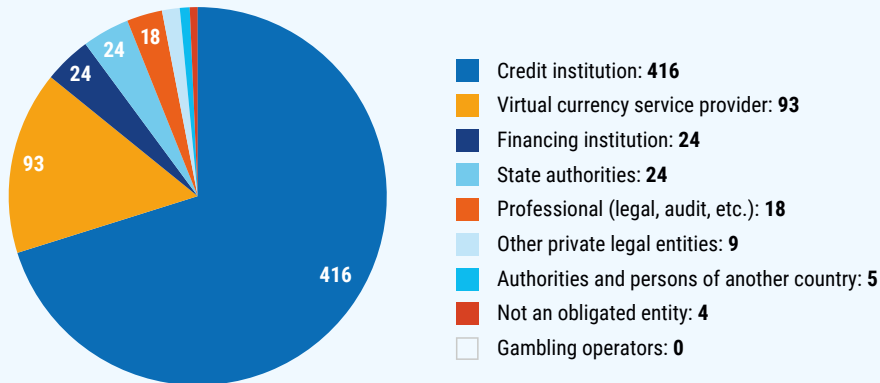
Regarding the application of sanctions, § 21 of the ISA stipulates that entities with special obligations are required to check whether a person is subject to financial sanctions. Additionally, during the due diligence process, the person with special obligations must ensure that their planned or executed transaction or operation does not violate financial sanctions. If the additional information obtained during the due diligence process does not allow for this determination, the person with special obligations must report the FIU of this and the applied financial sanction. This means that if the person with special obligations is unsure whether it is a situation of applying financial sanctions, they are obliged to apply the measure and submit a notice to the FIU. The FIU, in turn, provides feedback to the reporter on the legality of the application of the financial sanction. This two-step system mitigates risks by helping to ensure that decisions on the application of sanctions are verified and lawful. It also helps mitigate the risk of entities with special obligations making mistakes in complex situations.

⁷³ § 20(1) Clauses 6–12 of the International Sanctions Act (ISA) <https://www.riigiteataja.ee/akt/117052025003>

⁷⁴ International standards on combating money laundering and the financing of terrorism & proliferation <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> p.12

⁷⁵ §§ 35 – 36 of the ISA <https://www.riigiteataja.ee/akt/117052025003>

Figure 2. Submission of international sanction reports in 2024



Source: FIU Annual Report

Awareness and Reporting Among Market Participants

Survey results further revealed that credit institutions demonstrated the highest level of awareness regarding the financing of the proliferation of WMD. All of them had a compliance function in place to counter WMD proliferation financing, integrated within a broader risk management system (e.g., anti-money laundering, counter-terrorism financing, and sanctions compliance). Credit institutions assessed the risks associated with WMD proliferation financing as significant and considered themselves well-informed about the threats and risks involved. All interviewed representatives of credit institutions stated that they had read the latest FATF guidelines on WMD proliferation financing (2018) and felt up to date with the most recent recommendations and guidance, particularly those related to sanctions against North Korea and Iran.

Similar to credit institutions, most financial institutions, VASPs, CSPs, and gambling operators also have systems in place for managing the risks of financing the proliferation of WMDs, but not all. Approximately 10% of financial institutions, 20% of CSPs, and 10% of gambling operators reported in the survey that they lack a system for managing the risks of financing the proliferation of WMDs. All representatives of gambling operators and financial institutions considered themselves aware of the risks and threats of financing the proliferation of WMDs. The CSP sector stands out, with 42% responding that they are not concerned about the risks of financing the proliferation of WMDs at all. Additionally, 39% of CSPs assessed that they are not aware of the risks associated with financing the proliferation of WMDs. Regarding the activities carried out within the framework of the risk management system for financing the proliferation of WMDs, CSPs have the most problems, with only about 64% conducting customer screening or checking against sanctions lists. In contrast, 80-100% of market participants in other sectors conducted checks against the sanctions list. Deficiencies in risk management systems and awareness are also reflected in reporting activity, where CSPs, considering the size of the sector and customer base, are one of the sectors with the lowest reporting activity. One of the risk mitigation measures for the CSP sector is Article 5n of Regulation (EU) No 833/2014, which prohibits the provision of services offered by market participants in the sectors to legal persons, entities, or bodies established in Russia. This reduces the risk of evasion related to Russia.

To raise awareness, the FIU conducted 17 financial sanctions-related training sessions (including those related to the financing of WMDs) for various sectors from 2020 to 2024, with 4500 participants. The FIU also conducted two training sessions on typologies of financing WMDs, and the Ministry of Foreign Affairs and the Financial Supervision Authority have also conducted training on preventing the financing of WMDs. The FIU⁷⁶ and the Financial Supervision Authority⁷⁷ have issued guidelines that provide recommendations for the application of financial sanctions and the development of organizational solutions.

The risk of non-compliance with sanctions imposed by the UN Security Council is reduced by the fact that sanctions imposed or updated by the UN Security Council are applied under § 8 of the ISA until updated or adopted by the Council of the European Union. The public is informed about sanctions imposed by the UN Security Council and related changes through the Ministry of Foreign Affairs website⁷⁸. In 2024, public notifications have been made without delay.⁷⁹

The competent supervisory authorities oversee the requirements set for obligated entities, i.e., the existence and effective implementation of procedures. During the period 2020–2024, the FIU conducted 23 on-site inspections⁸⁰ focused on ISA due diligence measures, during which the FIU identified deficiencies in the compliance with ISA requirements in 11 cases and issued precepts to correct the deficiencies. According to the FIU, smaller market participants (e.g., CSPs) face more problems in establishing and following the necessary procedural rules and control mechanisms for applying financial sanctions. However, this is somewhat understandable, as these requirements have only been in effect for them since mid-2024. Nevertheless, the FIU believes that compliance with ISA due diligence measures has improved during the period under review. This is primarily indicated by the increased reporting activity. For example, specialists⁸¹ in the fields of law and audit submitted only one suspicion report to the FIU in 2021, but the same market participants submitted 37 reports in 2022. This trend has continued in subsequent years.

In the autumn of 2024, the Financial Supervision Authority conducted on-site inspections aimed at testing the functionality and effectiveness of the automated screening systems of supervised entities in identifying financial sanction subjects and transactions or actions that violate financial sanctions. The test was carried out in cooperation with an external service provider across 15 supervised entities: 12 credit institutions, 2 payment institutions, and 1 investment firm. Credit institutions, with 2.9 million customers and the largest share of activity volumes, overwhelmingly dominate the Estonian financial sector. Their market share is particularly significant in payments – 99%. The test examined 38 sanction screening systems in practice, evaluating the effectiveness and efficiency of identifying both manipulated and unmanipulated data records in customer and payment screening. The test also included checking the systems' capability to screen against UN sanctions lists established to prevent the financing of the proliferation of WMDs and the ability to identify ships named in the sanctions lists during payment screening. The test showed that the most important market participants in the Estonian financial sector use effective solutions for screening payments and customer bases.

⁷⁶ https://fiu.ee/sites/default/files/documents/2022-03/rahapesu_andmebueroo_juhend_finantsanktsiooni_kohaldamiseks_250222.pdf p. 22-23.

⁷⁷ The Financial Supervision Authority's recommended guidelines "Application of International Financial Sanctions in Credit and Financial Institutions" https://www.fi.ee/sites/default/files/2021-11/Finantsinspektsiooni%20soovituslik%20juhend%20Finants-sanktsiooni%20kohaldamine_0.pdf

⁷⁸ <https://www.vm.ee/tegevus/rahvusvahelised-sanktsioonid/muudatud-rahvusvahelistes-sanktsioonides>

⁷⁹ Although the term "without delay" is not defined by the FATF, it can be inferred from mutual evaluation reports that, in general, a period not exceeding two days is considered acceptable.

⁸⁰ Credit institution, financial institutions, payment institution, and VASP.

⁸¹ Lawyers (members of the bar), auditors, financial and tax advisors, bailiffs, other legal advisors, notaries, bankruptcy trustees, accounting service providers, trust, company, or similar service providers.

Between 2020 and 2024, market participants reported the application of financial sanctions (including those imposed by the UN) to the FIU 825 times, with 71% of the cases being legitimate applications. In the remaining 29% of cases, it was mostly a matter of so-called false positives, where the market participant applied the sanction, but the person to whom the measure was applied was not actually a sanction subject. Therefore, according to the working group, market participants mostly apply sanctions correctly. The number of financial sanction reports submitted to the FIU has increased year by year (see Table 3), but the growth is primarily related to financial sanctions imposed on Russia and sanction subjects with frozen assets in Estonia.

Table 3. Number of financial sanction reports (ISR) submitted to the FIU by year

Year	Number of ISR reports
2020	2
2021	7
2022	448
2023	166
2024	204

The largest market participants, i.e., credit institutions and VASPs, have also demonstrated their ability to identify situations where a sanction subject indirectly owns or controls a third party⁸² and to effectively freeze assets. This further indicates that market participants can detect indirect transactions related to a financial sanction subject.

Table 4. Volume of Frozen Funds in Euros by Year-End

Sanctioning authority	2020	2021	2022	2023	2024
UN	0	0	75	8,205	8,205
EU	81,689	48,696	25,708,065	33,222,212	49,111,885

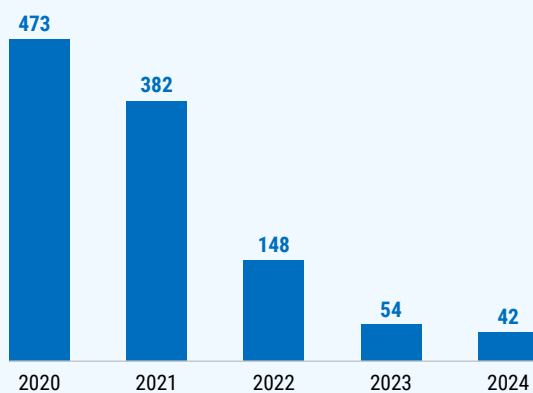
Considering the aforementioned circumstances, it can be stated that although there is a risk that market participants may fail to correctly apply UN-imposed sanctions due to ignorance or malice, the working group did not identify any situation where a sanction imposed by the UN on a sanctioned person or related person was not applied. A survey conducted among market participants indicates that larger market participants (credit institutions, VASPs, and financial institutions) generally have good awareness of the risks associated with the financing of WMDs and better-developed risk management systems compared to non-financial institutions. In the CSP sector, there appear to be deficiencies in both the risk management system and awareness of the risks associated with the financing of WMDs. However, the situation in the CSP sector has improved compared to the early years of the observed period, and the restrictions on providing certain services to Russian legal entities reduce the level of evasion risk. The working group assesses that the level of vulnerability related to awareness in the CSP sector is relatively low.

⁸² For example, in cases analyzed by the FIU, three different Estonian credit institutions immediately identified (i.e., on the day the individual was added to the list) that among their clients were companies owned or controlled by the sanction subject.

Technology-Related Vulnerabilities

In Estonia, the number of virtual asset service providers (VASPs) has significantly decreased since 2020, mainly due to regulatory changes and strengthened supervision (see NRA report 2025 in the field of ML risks, the sectoral money laundering risk assessment report for virtual asset service providers, Figure 3). Consequently, the number of VASPs with an Estonian operating license that could potentially fall victim to cyberattacks has also significantly decreased.

Figure 3. Number of VASPs by year-end for the years 2020–2024



The main measure that allows VASPs with an Estonian operating license to mitigate cyberattack threats is awareness of the risks associated with WMD risk countries (especially North Korea) and the existence of a framework for preventing and responding to cyber incidents. According to the survey, VASPs' awareness of cyber risks appears to be high. 95% of the VASPs who responded to the survey considered the level of cyberattack risk to be either high or at least medium. Three VASPs participating in the survey noted that they had themselves been victims of some type of cyberattack. On the positive side, all three sought assistance from law enforcement authorities. All VASPs who responded to the survey had at least one employee, and at least 26% had more than one employee responsible for cybersecurity. Almost all VASPs, i.e., 95%, also avoid storing data in offshore countries' servers.

The main regulatory measure directing VASPs to enhance cybersecurity is Regulation (EU) 2022/2554 (hereinafter "DORA"), adopted in 2022 and now in force. DORA is the European Union's new regulation on digital operational resilience, which brings significant changes to all companies operating in the financial sector, including VASPs. Since VASPs fall under financial supervision through the MiCA regulation, they will have to start complying with additional rules aimed at identifying, managing, and mitigating IT risks. The regulation requires⁸³ strengthening cybersecurity, establishing clear governance structures, and the direct responsibility of the board for ensuring digital security.

DORA also focuses on the rapid notification of supervisory authorities about cyber incidents and regular system testing, including simulated attacks. VASPs must also assess and control the risks of external IT service providers, such as cloud services and cryptocurrency wallet custodians. All contracts must include security clauses, audit rights, and options for secure contract termination. These measures significantly reduce

⁸³ The DORA regulation and requirements for companies operating in the Estonian financial sector. <https://www.fi.ee/et/kindlustus/kindlustusvaldkonna-regulatsioonid/dora-maarusest-ja-nouetest-est-est-finantssektoris-tegutsevatele-ettevotetele>

the possibility of hackers gaining access to market participants' systems, especially through subcontractors. According to the DORA regulation, all VASPs must have a significantly stronger framework for preventing and responding to cyber incidents.

At the end of 2024, the Markets in Crypto-Assets Regulation (EU) 2023/1114 (also known as "MiCA") came into full effect, further standardizing the activities of VASPs in providing services with various virtual assets. To properly implement the MiCA regulation at the national level, the Crypto-Asset Market Act was adopted on June 5, 2024.⁸⁴ In addition to legislative changes, according to the Minister of Finance's regulation, virtual asset service providers operating in Estonia are required to regularly (quarterly) submit data on their activities, due diligence measures, services provided, and assets and liabilities to the Bank of Estonia and the Financial Intelligence Unit from January 1, 2024. These legislative changes and reporting obligations help strengthen the supervision of VASPs and enable better assessment and identification of risks associated with the VASP sector. Several supervisory measures have also significantly contributed to mitigating the risks in the VASP sector: remote control questionnaires, on-site inspections, supervisory proceedings (22 supervisory proceedings), and awareness-raising activities regarding sanctions and WMD risks in the VASP sector.

It can be generalized that virtual asset service providers still operating in the Estonian market have significantly improved their risk management systems according to the FIU, and their awareness of WMD-related threats, especially those originating from North Korea, is high according to the conducted survey. Additionally, the supervisory authority's capabilities to conduct more effective risk-based supervision have expanded.⁸⁵

Exploitation of VASPs

An important measure to reduce the risk of financing the proliferation of WMDs from North Korea is the fact that VASPs with an Estonian operating license do not have clients with North Korean citizenship or origin. Additionally, VASPs that participated in the sector survey have excluded initiating client relationships with North Korean clients due to their risk appetite. A similar risk associated with Russian citizens⁸⁶ is mitigated by the prohibition in Article 5b, paragraph 2 of Regulation (EU) No 833/2014, which prohibits the provision of virtual asset services to Russian citizens. Article 5b, paragraph 2a of Regulation (EU) No 833/2014 also prohibits Russian citizens or residents from being part of the ownership or management of a VASP established in the EU. This restriction helped mitigate the previously realized risk where a VASP established by Russian citizens and licensed in Estonia (the Estonian license had already been revoked by that time) was used to evade⁸⁷ sanctions and finance WMDs.

The potential risk levels associated with Iranian citizens are somewhat higher, according to the working group. This is primarily because several VASPs with an Estonian operating license have Iranian clients and allow transactions with VASPs operating in Iran. According to the working group, VASPs with an Estonian operating license had a total of 633 Iranian clients in 2024, with approximately 2,000 transactions amounting to just over 380,000 euros during the year.⁸⁸ Based on the analysis of the information received by the FIU, the working group concluded that most of the transactions made by Iranian citizens are small-scale transactions with Iranian virtual currency platforms. In most cases, the transactions appear to involve sending small amounts

⁸⁴ Virtual asset service providers are now subject to a reporting obligation.

<https://fiu.ee/uudised/virtuaalvaaringu-teenuse-pakkujatele-kehtestati-aruandluskohustus>

⁸⁵ See the sectoral ML risk assessment for virtual asset service providers for more details (NRA 2025 report on ML risks).

⁸⁶ There is an exemption to the prohibition provided in the regulation for individuals residing in a member state of the European Economic Area or Switzerland, or for individuals who have a residence permit in a member state, a member state of the European Economic Area, or Switzerland

⁸⁷ Elliptic in Action: Uncloaking Garantex for law enforcement and sanctions complicity.

<https://www.elliptic.co/blog/elliptic-in-action-garantex>

⁸⁸ Based on VASP reporting data.

to family members in Iran or payments between accounts on different virtual currency platforms belonging to the same person.⁸⁹ The FIU has not identified any indications of financing weapons of mass destruction in these transactions, but notes that transactions with Iranian counterparts carry a higher risk level for WMD financing. In 2023 and 2024, the turnover of Estonian VASPs related to services provided towards the UAE has significantly increased. For example, in 2023, it was nearly 68 million, and in 2024, it was already over 100 million.⁹⁰ Although there are no sanctions related to the financing of WMD proliferation against the UAE, both Iran and Russia have used the UAE to circumvent various sanctions⁹¹. While the use of the UAE to evade sanctions is not a risk solely associated with the virtual currency sector, additional attention must be paid to the vulnerabilities related to increasing transaction volumes with the UAE and the financing of WMD proliferation. The risk assessment of the VASP sector has thoroughly addressed the vulnerabilities associated with offshore clients of Estonian licensed VASPs and the measures to mitigate them.

In summary, the vulnerabilities associated with the activities of Estonian VASPs are somewhat mitigated, primarily through more effective supervision, a stronger legal framework, and a decrease in the number of market participants and their increased awareness. However, the presence of Iranian clients, transactions with Iranian platforms, and increasing transaction volumes towards the UAE still leave significant vulnerabilities. Therefore, the sector requires continued attention.

Considering both the threats and mitigating measures, the working group assesses that the residual risk level related to technology and sectors is low.

5.3. Legislative and Administrative Vulnerabilities and Residual Risk

Exploitation of Legal Entities

Several factors mitigate the vulnerabilities related to the financing of WMD proliferation through the exploitation of legal entities. Firstly, there is free access to the data of the Business Register and TEKSA. Secondly, the prohibition of nominee directors and bearer shares in Estonian law increases transparency. These measures prevent the use of anonymous and concealed business structures that could be abused for the purpose of financing WMD proliferation. Although the quality of TEKSA data is not always up-to-date and accurate, access to information on beneficial owners still helps to reduce risks. Additionally, some obliged entities must notify the register if they notice that the beneficial owner data may be incorrect. Furthermore, the generally high level of due diligence measures by credit institutions strengthens control. For example, during the period under review, credit institutions reported the FIU 391 times of suspected sanctions evasion, and in 81% of cases, the report involved a legal entity registered in Estonia. Although most reports were related to sanctions imposed on Russia, this indicates that credit institutions can effectively identify situations where an Estonian legal entity, which is their client or uses the services of the credit institution, potentially violates sanctions.

The vulnerability level of Estonian companies to WMD financing risks is also reduced by the reorganization of the Business Register. On February 1, 2023, a significant amendment to the Business Register Act came into force: if the annual report is not submitted, the registrar may either fine the offender (Business Register Act § 57: fines can be imposed repeatedly until the obligation is fulfilled) or forcibly dissolve the legal entity (Business Register Act § 58). Since 2024, a significant number of legal entities that have not submitted their annual report have been automatically deleted from the register.

⁸⁹ The main reason for submitting the report appears to be the fact that Iran has been added to the list of countries with a higher risk of terrorism financing.

⁹⁰ Based on VASP reporting data and 2023 offsite data.

⁹¹ Busted Sanctions: Explaining Why Economic Sanctions Fail.

<https://www.sup.org/books/politics/busted-sanctions/excerpt/introduction>

This measure reduces the potential vulnerability level due to the large number of inactive and potentially exploitable companies, limiting the opportunities to use them as shell companies for illegal transactions. For example, in 2023, more than 121,600 companies failed to submit their annual reports on time, of which nearly 26,700 were deleted from the Business Register, and 13,100 companies were fined⁹² for failing to submit their reports. The vulnerability level of Estonian legal entities to exploitation is also reduced by the fact that, in general, the ownership structure of Estonian companies is very simple compared to companies in other EU countries.⁹³

Since many high-risk companies related to Russia and Iran are backed by e-residents, the direction taken in the e-residency continuation strategy for 2022-2025 helps to prevent the exploitation of these companies. According to this strategy, e-residency is generally not offered to citizens of countries that pose a significant security or e-resident digital ID misuse risk.⁹⁴ Additionally, since March 2022, new e-resident cards have not been issued to citizens of aggressor countries, namely Russia and Belarus.⁹⁵ Since 2022, an automatic follow-up solution has been implemented, resulting in an increase in the number of e-resident digital IDs issued to citizens (or residents) of the aforementioned countries that have been revoked, from 29 in 2020 to 227 in 2024. The information exchange between the Police and Border Guard Board and its partners has also improved, resulting in an increase in the number of e-residencies revoked⁹⁶ specifically due to suspicions of money laundering.

Although Iranian citizens or e-residents related to Iran have established over 350 companies in Estonia, the FIU has not yet received information indicating that these companies are involved in sanctions violations. The FIU has received a total of 78 reports regarding companies with connections to Iran, and the analysis of the information from these reports shows that the reason for submitting the report was mostly the person's connection to Iran, unusual cash activities, or the obliged entity's inability to fully apply due diligence measures. This suggests that market participants indeed treat transactions related to Iran as higher-risk transactions and submit reports to the FIU if there is any suspicion regarding companies with connections to Iran. Therefore, it can be stated that despite the relatively large number of companies with connections to Iran potentially posing a vulnerability, no cases have been identified so far where this has been used to evade sanctions, and the increased awareness of credit institutions and the applied appropriate due diligence measures have helped to mitigate these vulnerabilities.

Cooperation with Third Countries

During the period under review, Estonian investigative authorities have not initiated any criminal investigations related to the financing of WMD proliferation or received legal assistance requests related to sanctions imposed on North Korea or Iran. The FIU has received information from Estonian market participants twice regarding suspected financing of WMD proliferation. Additionally, foreign countries have provided Estonia with information related to the financing of WMD proliferation on two occasions. This confirms the hypothesis that Estonia's exposure to the financing of WMD proliferation is low.

⁹² The Business Register deleted over 26,000 companies that failed to submit their annual reports. <https://www.err.ee/1609361351/ariregister-kustutas-ule-26-000-majandusaasta-aruande-esitamata-jatnud-ettevotte>

⁹³ Project DATACROS: Developing a Tool to Assess Corruption Risk factors in firms' Ownership Structure. https://www.transcrime.it/wp-content/uploads/2021/09/Datacros_report.pdf

⁹⁴ E-residency strategy 2022-2025 <https://www.mkm.ee/sites/default/files/documents/2022-05/E-residentsuse%20j%C3%A4tkustrateegia%202022-2025.pdf> p. 24

⁹⁵ Restrictions on Russia and Belarus citizens <https://learn.e-resident.gov.ee/hc/en-us/articles/4575271559441-Restrictions-on-Russia-and-Belarus>

⁹⁶ See more details in the risk assessment concerning e-residents.

Estonian investigative authorities and the prosecutor’s office certainly have the capability to investigate sanctions violations (including WMD-related violations). This is evidenced by the fact that during the period under review, 191 criminal cases were initiated under § 93¹ of the Penal Code. A total of 50 criminal cases were initiated under § 421¹⁹⁷ and § 421²⁹⁸ of the Penal Code. During the same period, nine criminal cases under § 93¹ of the Penal Code resulted in a court decision, which constitutes 4% of all initiated criminal cases, and 38 proceedings were terminated, which is 20% of all criminal cases. A total of 13 criminal cases were sent to court and resulted in a court decision (see Table 5).

Table 5. Court decisions on violations of international sanctions and Government of the republic sanctions

Year of initiation of the criminal case under PenalCode § 93 ¹	Number of court decisions
2020	0
2021	1
2022	2
2023	9
2024	1

In Estonia, inter-agency cooperation related to sanctions, including the prevention of WMD financing, is conducted closely and promptly. For example, all competent authorities listed in § 11 of the International Sanctions Act have the right to exchange information with each other under § 11¹ of the ISA.

If one authority is unable to obtain the necessary information from a third country counterpart, the capabilities of another Estonian authority are used to obtain this information. This flexible and cooperative approach allows the use of all available channels of the authorities to obtain information from third countries, and this is the main way to obtain the necessary information from third countries in the absence of cooperation. It is also possible to improve the access of competent authorities to necessary data through information technology tools and databases provided by private companies. If competent authorities have access to databases that consolidate various trade data, it reduces dependence on third-country registers. This reduces, at least to some extent, the dependence of competent authorities on the willingness of third countries to cooperate. It can be concluded that although solutions based on databases and information technology tools help reduce dependence on third-country cooperation, their disadvantage is the high acquisition and/or license fees, which makes it impossible for many authorities to acquire them without additional resources. Reducing this vulnerability level is also supported by cooperation in national and international working groups. For example, the FIU actively participates in three international working groups⁹⁷ established between financial intelligence units, which are responsible for cooperation, joint analyses, and information exchange in the field of sanctions. The Tax and Customs Board also participates in a working group that mainly includes EU member states bordering Russia. The aim of the working group is to ensure operational information exchange and the consistent and uniform application of sanctions.

Considering both the threats and mitigating measures, the working group assesses that the residual risk level related to legislation and administration is medium.

⁹⁷ The working groups are Russia-Related Illicit Finance and Sanctions, Baltic Taskforce on Sanctions, and Counter Terrorist Financing Task Force.



REPUBLIC OF ESTONIA
MINISTRY OF FINANCE