## 12. Analysis of proliferation financing risks

### 12.1. Proliferation and proliferation financing

Weapons of Mass Destruction (WMD) and parties enabling proliferation thereof pose a significant threat to international security. The international community has agreed to combat the proliferation of such dangerous weapons worldwide. The fight against WMD is also connected to proliferation financing. Within the framework of this Risk Assessment, possible ways of proliferation financing that could be utilised by taking advantage of the Estonian financial system or business environment are examined in greater detail.

Proliferation financing is defined by FATF as the provision of funds or financial services used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.[1]

Within the framework of this Risk Assessment, the focus by reference to FATF Recommendation 1 is on proliferation financing which constitutes an actual or potential breach, non-implementation, or evasion of financial sanctions referred to in FATF Recommendation 7. In the European Union (EU), which constitutes international jurisdiction under FATF Recommendation 7, the assets of designated persons and entities are frozen in accordance with EU regulations and amendments thereto[2]. The EU also publishes a list of sanctioned natural and legal persons, entities, and bodies (hereinafter "designated persons and entities") in consolidated and machine-readable form[3]. According to Estonian law, the term "strategic goods" includes both military goods and dual-use goods.[4]

FATF Recommendation 7 refers to two sanctions regimes: measures against the Democratic People's Republic of Korea (DPRK) [5] and Iran[6] which require states to immediately freeze funds and other assets belonging to a person or entity identified by or under the authority of the United Nations Security Council in accordance with Chapter VII of the Charter of the United Nations, and also to ensure that no funds or other assets will be made directly or indirectly available to any such person or entity.

Pursuant to the FATF methodology, there may therefore emerge a proliferation financing risk:

A) as caused by breach or non-implementation of financial sanctions: when designated persons or entities have access to financial services, funds, or assets due to, for example, inadequate communication, lack of clear responsibilities, or implementation of inadequate procedures by financial institutions and designated non-financial businesses and professions (e.g. insufficient background check in establishing or monitoring business relationships, insufficient staff awareness, inadequate risk management, inadequate systems for monitoring lists of sanctioned persons, or an overall insufficient conformity check level/culture).
B) as caused by evasion or enabling evasion of financial sanctions: when designated persons or entities avoid imposition of financial sanctions on them (for example, by using shell or shelf companies, figureheads, or intermediaries/advisors that provide assistance in evading implementation of the law).

[1] Combating Proliferation Financing: A Status Report on Policy Development and Consultation
[2] Hereinafter the relevant FATF Guidance Paper constitutes the methodical base
[3] https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions
[4] See § 2 (1) of the Republic of Estonia Strategic Goods Act
[5] Resolution 1718 (2006) and, in the case of subsequent resolutions, Annexes to the relevant resolutions by the Security Council or by the 1718 Security Council Sanctions Committee
[6] Resolution 1737 (2006) and, in the case of subsequent resolutions, Annexes to the relevant resolutions by the Security Council or by the 1737 Security Council Sanctions Committee when these committees operate under Chapter VII of the Charter of the United Nations

The UN Security Council has established specific obligations connected to the financing of activities related to WMD programmes in order to implement the aforementioned sanctions regimes.

1. Member States must take the required measures to prevent the provision of financial services or assistance to the DPRK or Iran in connection with the offering, supply, sale, transfer, manufacture, maintenance, or use of such prohibited articles, materials, equipment, goods, and technology, which have been banned by the relevant resolutions[7].
2. Application of financial sanctions to persons and associations[8] that support DPRK or Iranian WMD-related activities and programmes.
3. Member States are called upon to prevent the provision of any financial services or the transfer of financial or other assets or resources that could contribute to the DPRK and Iranian proliferation-sensitive activities or the development of weapon delivery systems[9].
4. Member States are called upon not to enter into new commitments or to provide grants, financial assistance, or loans to the DPRK or Iran, except for humanitarian and development aid purposes.[10]
5. Member States are called upon not to provide financial support for trade with the DPRK or, in the case of Iran, to exercise vigilance in performing relevant obligations when providing public financial support in order to avoid financial support that contributes to nuclear activities or the proliferation or development of nuclear weapons.[11]

At the same time, in the case of the Iranian regime, it is important to note that Resolution 1737 (2006) was repealed by Resolution 2231 (2015).[12] Resolution 2231 lifted previously imposed sanctions related to nuclear weapons and imposed specific restrictions on:
• arms related transfers to and from Iran that were due to end in 2020;
• ballistic missiles related transfers and freezing of related activities and assets that are due to expire in 2023; and
• nuclear weapons related transfers and activities that are due to expire in 2025.

Pursuant to Resolution 2231, the lifting of these restrictions is conditional on Iran's compliance with its obligations under the Joint Comprehensive Plan of Action (JCPOA). Repeated violations were found during 2020, but the UN Security Council did not agree to extend the measures.[13] Therefore, in Iran's case, one must foremost follow the existing restrictions related to ballistic missiles as well as restrictions on transfers and activities related to nuclear weapons, legally relying on restrictive measures imposed by the EU[14]. In addition, it should be borne in mind that additional restrictive measures imposed by the EU in relation to the human rights situation in Iran, support for terrorism, and other reasons (such as the war in Syria) are not part of the JCPOA and will remain in force. At the same time, the latter does not fall within the scope of this Risk Assessment, as it does not constitute an Iranian sanctions regime for the purposes of FATF Recommendation 7.

### 12.2. Assessment of risks

In order to limit the proliferation of WMD and refrain from collecting, holding, moving, and using the related funds, it is necessary to assess the risks of such activities. The risk of proliferation financing is a

[7] S/RES/1874(2009); S/RES/1718(2006); S/RES/1737(2006); S/RES/1747(2007); S/RES/1929(2010)
[8] S/RES/1718(2006); S/RES/1737(2006); S/RES/1747(2007); S/RES/1929(2010)
[9] S/RES/1874(2009); S/RES/1929(2010)
[10] S/RES/1874(2009); S/RES/1747(2007)
[11] S/RES/1874(2009); S/RES/1803(2008)
[12] http://www.undocs.org/S/RES/2231(2015)
[13] See Estonia's explanation of its vote: https://un.mfa.ee/estonian-explanation-of-vote-in-connection-with-agenda-item-non-proliferation/
[14] For an overview of valid sanctions, refer to this convenient application: https://www.sanctionsmap.eu/#/main

combination of the relevant threat, vulnerability, and consequences of its realisation. In order to assess the relevant risks, both the inherent risk and residual risk must be identified.

a. Inherent risk refers to the natural risk level that exists before risk management measures are implemented. An inherent risk for a country is, for example, geographical proximity to a WMD country, or production of dual-use or WMD-related goods in the country and related trade, as well as gaps in the legal framework implementing the UN Security Council resolutions.
b. Residual risk refers to the risk level that remains after the application of risk management measures. Understanding the residual risk provides an indication of whether the country (or a private organisation) can manage the proliferation risks. A high level residual risk indicates that the control measures are inadequate and that the country should take additional measures to manage the relevant risk. This chapter describes the residual risk and proposals for measures to be taken.

The specifics of assessing proliferation financing risks:

a. THREAT refers to designated persons and entities that potentially cause or have in the past caused harm by evading or breaching WMD-related or financial sanctions. This can constitute an actual or a potential threat. Not all threats pose the same level of risk to all countries and private sector companies.
b. VULNERABILITY refers to circumstances that can be exploited by the threat or that may support or facilitate the breach, non-implementation, or evasion of WMD-related or financial sanctions. For the state, these vulnerabilities may include weaknesses in laws or regulations that include the country's proliferation financing prevention regime, or the country's contextual peculiarities that may provide opportunities for designated persons and entities to raise or move funds or other assets. For example, a jurisdiction that has weak anti-money laundering / anti-terrorist financing regulations or that does not collect data on the beneficial owners of companies incorporated under its national law. For private sector companies, vulnerabilities may include characteristics of a particular sector, financial product, or type of service that make them attractive to a person or entity involved in a breach, non-implementation, or evasion of WMD funding. For example, a customer base that consists of small trading companies located in jurisdictions known to be associated with WMD constitutes vulnerability for the private sector company.
c. CONSEQUENCE refers to a result where funds or assets are made available to designated persons and entities to enable them to procure materials, items, or systems required for the development and maintenance of illegal nuclear, chemical, or biological weapons systems (or their carriers) or where frozen assets of designated persons or entities are used for proliferation financing. The consequence of proliferation financing, i.e. use of weapons of mass destruction, is more severe than in the case of money laundering or other financial crimes and is more akin to the potential loss of life associated with the consequences of terrorist financing. This is likely to vary by country, channel, or source.

### 12.3. Threat of proliferation financing

To identify the threat – given the wide range of options for perpetrating proliferation financing – it is reasonable to focus on more probable facts and circumstances and facts and circumstances that point to threats that correspond to the relevant international trends. Committees set up to monitor compliance with the UN Security Council resolutions[15] have published reports and reviews outlining the behaviours in recent years of persons and entities included on the lists of designated persons by which they have succeeded in evading or breaching the relevant sanctions regimes.

With regard to the proliferation risk, two directions can be distinguished as more important for Estonia: breach of the sanctions regime through possible WMD transit using Estonian territory or companies established here; evasion of sanctions through the sector of virtual currency service providers.

[15] Reports of the Panels of Experts (PoE) UNSCR 1718 (2006); UNSCR 1874 (2009)

### 12.3.1. Threat of financing WMD transit

To date, there have been no known cases in our territory where anyone has been able to illegally supply nuclear, biological, radioactive, or chemical material to WMD manufacturers.

The components of weapons of mass destruction – various poisons, chemical weapons precursors, or explosives – are listed in the Common Military List of the European Union. For example, ML7: Chemical agents, "biological agents", "riot control agents", radioactive materials, related equipment, components and materials, and ML8: "Energetic materials", and related substances. The list of dual-use items includes, for example, nuclear materials, facilities, and equipment. Estonia does not manufacture weapons of mass destruction or technologies/goods required therefor.

Due to the applicable EU and Estonian regulations and Estonia's geographical location slightly away from WMD transit routes, the probability of financing the transit of weapons of mass destruction through Estonia is below average. On the other hand, the geography of transit related to weapons of mass destruction does not mean that the risk of financing transit is automatically low in Estonia as financial and financial technology services provided across borders may be used for financing.

In 2017-2020, Estonia did not have any trade with North Korea.[16]

In 2017-2020, Estonia exported to Iran mainly timber / timber materials, peat, and medication, to a lesser extent machinery and equipment. Export volumes are showing a downward trend (2017: 5.32 M €; 2018: 3.58 M €; 2019: 1.44 M €).[17]

Looking at funding trends, the United Nations Security Council's Panel on Experts (PoE) on DPRK's Sanctions Regime has found that the Democratic People's Republic of Korea continues to have access to the international financial sector through various joint ventures, offshore accounts, shell companies, and virtual assets. Analysis results show that the DPRK continues to use the banking systems of East and South-East Asia, and thus wider international correspondent banking, through associated entities and persons. The PoE has also criticised Member States for insufficient efforts in establishing rules for the registration of companies, which has continued to allow the DPRK to take advantage of non-transparent company structures. Gaps in corporate registration control mechanisms make the Know Your Customer processes and procedures in financial institutions virtually impossible.[18]

With regard to Iran, the same trends and patterns have not been analysed as pertaining to Resolution 2231; UN member states have reported individual possible violations of the sanctions regime, including possible financing activities.[19] Due to limited trade as related to Iran as well as the lack of a nuclear weapons and related technology sector in Estonia, the violation of the sanctions regime is thus mainly associated with threats by persons and entities included on the sanctions lists trying to transact with or with the help of Estonian companies.

### 12.3.2. Proliferation financing threat through the sector of virtual currency service providers

In recent years, the DPRK has paid a lot of attention to taking advantage of virtual asset (cryptoasset) service providers, such as virtual currency exchange service providers, to evade UN sanctions. In its 2019[20] and 2020[21] reports, the PoE highlighted a number of tactics and techniques used by the DPRK with the aim of illegal collection of virtual currencies, mining activities, including by using sophisticated technological operations and malware. There is no clear answer to the question of how the DPRK then converts its virtual assets into fiat currency.

[16] https://valiskaubandus.stat.ee/profile/country/ee/
[17] https://valiskaubandus.stat.ee/visualize/tree_map/export/ir/all/2019/?locale=et
[18] https://undocs.org/S/2020/840
[19] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_531.pdf
[20] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf
[21] https://undocs.org/S/2020/840

Since May 2019, the DPRK has increased its Monero mining activity at least tenfold (compared to bitcoin mining in the same period). Monero is a virtual currency similar to bitcoin, but offers additional anonymity and does not necessarily require mining computers with the same high capacity.[22]

By 2019, at least 35 cases had been reported to the PoE where persons of DPRK origin had committed cyber-attacks against financial institutions, virtual currency exchangers, and miners in order to steal virtual currencies for profit. So as to limit the traceability of transactions, the DPRK, like money launderers, uses various digital asset stratification methods, such as creating thousands of virtual currency wallets with different service providers. During 2019, attacks by the DPRK became even more acute against virtual currency exchange platforms; some virtual currency exchange platforms have been victims of such attacks repeatedly and have had to terminate their activities.[23]

### 12.4. Proliferation financing vulnerability

#### 12.4.1. General vulnerability of proliferation financing

Estonia has established a legal system that complies with international requirements and appointed responsible authorities. The task of the Estonian Internal Security Service is to detect and prevent illegal handling of weapons of mass destruction and their components. Export controls on military and dual-use goods are carried out in co-operation with the Strategic Goods Commission of the Ministry of Foreign Affairs and the Tax and Customs Board. It is important to prioritise the active cooperation of the Strategic Goods Commission and its members with the FIU and banks operating in Estonia in order to enhance, in case of suspected WMD financing, the exchange of information on financial transactions of persons/companies applying for licenses or potentially carrying out illegal transport.

Internationally, Estonia is involved in various organisations fighting against weapons of mass destruction: NATO and EU respective formats, IAEA (International Atomic Energy Agency), OPCW (Organisation for the Prohibition of Chemical Weapons), the Australia Group, NSG (Nuclear Supplies Group), the Wassenaar Agreement, etc. Estonia is an elected member of the UN Security Council in 2020-2021, chairing the Security Council twice during that time: in 2020 (spring) and in 2021 (summer).

In Estonia, international sanctions are applied through European Union legislation. The Council of the European Union is one of the European Union's main decision-making bodies that adopts legislation, contracts agreements, and shapes the EU's common foreign and security policy. Participants in the Council meetings include such Ministers of EU Member that have the right to assume obligations and, if necessary, vote on behalf of their country.

As part of the EU common foreign and security policy, the Council also imposes sanctions or restrictive measures. The Council of the European Union adopts decisions based on Article 29 of the Treaty on European Union in order to implement the common foreign and security policy. These decisions impose obligations, prohibitions, and restrictions on either EU Member States or natural and legal persons in the EU. For example, Member States apply such common types of sanctions as prohibition to enter and arms embargoes – in Estonia, based on the Obligation to Leave and Prohibition on Entry Act and the Weapons Act, respectively.

The prohibitions and restrictions imposed by the above decisions, which are binding on EU natural and legal persons, are applied directly by EU Council regulations the effects of which are the same as the national legislation of the Member States. Thus, EU sanctions regimes adopt two CFSP instruments – a decision containing all the measures imposed and a regulation governing the obligations of natural and legal persons.

[22] For example, Bitcoin ransom payments made by WannaCry victims were transferred to Bitcoin wallets and eventually converted to Monero using the Swiss virtual currency exchange platform ShapeShift

[23] Youbit (formerly Yapizon) fell under repeated cyber-attacks in April 2017, losing $4.8 M, and an additional 17% of total assets in December 2017, forcing it to terminate its activities.

As indicated above, the obligations, prohibitions, and restrictions set out in the directly applicable EU Council regulations have an effect similar to national legislation. The application of international sanctions in Estonia is regulated by the International Sanctions Act (hereinafter ISA) and breach of sanctions is regulated in § 93[1] of the Penal Code, pursuant to which failure to comply with the sanction obligation or violation of a prohibition is punishable by a pecuniary punishment or up to five years' imprisonment.

An overview of the current sanctions with links to the relevant legislation is available on the EU sanctions website developed within the framework of the Estonian Presidency of the Council of the European Union.[24]

Pursuant to the International Sanctions Act, the Financial Intelligence Unit monitors compliance with the requirements of the Act and is the competent authority whose home page[25] provides an overview of sanctions as well as means to search for sanctioned persons. As from 1 January 2021, the Financial Supervision Authority supervises the application of financial sanctions by credit institutions and financial institutions that are subject to its supervision.

Within the EU, the DPRK is the subject of Council Decision (CFSP) 2016/849[26] and Council Regulation (EU) 2017/1509[27]. As from 2016, the EU has decided to take additional measures against the DPRK in addition to those stemming from the UN Security Council resolutions as activities of the DPRK pose a serious threat to international peace and security in the region and elsewhere. Further restrictive measures were considered necessary to increase the pressure on the DPRK to fulfil its international obligations. The EU is determined to combat the proliferation of weapons of mass destruction and is committed to the nuclear disarmament of the Korean Peninsula, including by considering new restrictive measures.

On 16 January 2016, the EU lifted all economic and financial restrictive measures imposed in relation to Iran's nuclear programme. Therefore, the following activities are re-authorised from that date, including the related services: financial, banking, and insurance measures; trade in the oil, gas, and petrochemical sectors; activities in the shipping, shipbuilding, and transport sectors. In addition, persons, entities, and bodies were removed from the sanctions lists and therefore the freezing of their assets, the ban on making funds available, and the visa ban no longer need to be applied.[28] A number of measures and restrictions related to the proliferation of weapons of mass destruction remained in place. These among other things pertain to the arms embargo, restrictive measures related to missile technology, restrictions on transfers and activities related to certain nuclear weapons, and provisions on certain metals and software subject to the authorisation regime.
The legal basis for the measures in force is Council Decision 2010/413/CFSP[29] and Council Regulation (EU) No 267/2012[30].

It has been established that designated persons and entities use networks of shell companies to implement their schemes. Failure to apply due diligence measures (e.g. the obligation to understand the business relationship and the obligation to identify the beneficial owners of companies) may lead to the undetected involvement of above entities or persons in transactions, which leads to a breach of the sanctions regime. The use of shell companies and intermediaries acting on behalf of designated persons and entities makes it difficult to monitor transactions. The vulnerabilities of Estonian legal entities[31] are also relevant from

[24] https://vm.ee/et/rahvusvahelised-sanktsioonid
[25] https://www.fiu.ee/rahvusvahelised-sanktsioonid/rahvusvahelised-finantssanktsioonid
[26] Council Decision (CFSP) 2016/849 of 27 May 2016 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Decision 2013/183 / CFSP, OJ L 141; 28 May 2016, p. 79
[27] Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007, OJ L 224; 31 August 2017, p. 1
[28] https://eeas.europa.eu/delegations/iran/32286/nuclear-agreement_en#JCPOA+Information+Note
[29] Council Decision 2010/413/CFSP of 26 July 2010 concerning restrictive measures against Iran and repealing Common Position 2007/140/CFSP, OJ L 195; 27 July 2010, p. 39
[30] Council Regulation (EU) No 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010, OJ L 088; 24 March 2012, p. 1
[31] see Section 2 „Analysis of Exploitation of Legal Entities" in the chapter on National Vulnerabilities in this NRA

the aspect of proliferation financing, especially the fact that control over the beneficial owners of legal entities is insufficient in practice.

The International Sanctions Act stipulates that financial sanctions are, among others, imposed also by the following registers:

- Register of European Patents Valid in Estonia [32];
- Register of Utility Models [33];
- Register of Trademarks and Service Marks [34];
- Land Register [35];
- Ship's Registration Book [36];
- Register of Non-profit Organisations and Foundations [37];
- Patent Register [38];
- National Traffic Register [39];
- Register of Industrial Designs [40];
- Estonian Central Register of Securities [41];
- Aircraft Register [42];
- Commercial Register [43].

The registrar refuses to make an entry in breach of a financial sanction and appoints a person who, within the limits of their competence, organises the application of the financial sanction, and forwards their contact details to the Financial Intelligence Unit. Considering that as of 10 May 2021 the register of beneficial owners is not a part of the commercial register and becomes a separate database, the controller of which is the Ministry of Finance and the processors of which are Tartu County Court's Registry Department and the state's Centre of Information Systems, the International Sanctions Act should be supplemented so that the registrar of the beneficial owner as well would be obligated to check financial sanctions and, in the event of entries violating them, to ensure that the Financial Intelligence Unit is immediately notified. Entry of a beneficial owner does not automatically create rights or obligations but the inclusion of designated persons and entities as beneficial owners (including beneficial controllers) in the data of Estonian legal persons indicates a breach of the sanction regime.

In accordance with the relevant UN Security Council resolutions, the collection, movement, and use of funds at the national level by persons and entities involved in the proliferation of weapons of mass destruction is prevented. Although coordination efforts in this area have been assessed as insufficient in recent years, a working group at the Ministry of Foreign Affairs was set up as at the end of 2020 to facilitate national implementation of UN resolutions related to both sanctions and financing of weapons of mass destruction. On the other hand, potential exploitation of legal persons by sanctioned persons is an aspect that increases vulnerability as the beneficial owners of legal persons are not checked against the lists of sanctioned persons. If a legal person is not in a customer relationship with an obliged entity who is also obliged to independently verify the beneficial owners of the customer (including as pertaining to sanctions) when applying due diligence measures, a legal person with a beneficial owner included on the list of sanctioned persons may not be identified in time. The overall vulnerability assessment is therefore **low-average**.

[32] https://www.epa.ee/et/patendid/eestis-kehtivate-euroopa-patentide-register
[33] https://www.epa.ee/et/kasulikud-mudelid/registreerimine
[34] https://www.epa.ee/et/kaubamargid/kaubamargi-registreerimine
[35] https://www.rik.ee/et/e-kinnistusraamat
[36] https://laevakinnistusraamat.rik.ee/
[37] https://www.just.ee/et/eesmargid-tegevused/ari-ja-uhinguregister
[38] https://www.epa.ee/et/patendid/toimingud-eesti-patendiregistris
[39] https://eteenindus.mnt.ee/main.jsf?lang=et
[40] https://www.epa.ee/et/toostusdisainilahendused/toimingud-toostusdisainilahenduste-registris
[41] https://nasdaqcsd.com/et/teenused/teenused-emitendile/vaartpaberiomanike-nimekiri/
[42] https://www.ecaa.ee/et/lennundustehnika-ja-lennutegevus/ohusoidukite-register
[43] https://www.just.ee/et/eesmargid-tegevused/ari-ja-uhinguregister

### 12.4.2 Sectoral vulnerabilities

#### 12.4.2.1. Financial sector

The main sources of threat are market participants who are financed and/or settled through the financial sector and may be used to finance transit of weapons of mass destruction without their knowledge due to their relatively low awareness. The financial sector specific risk occurs primarily in intermediation transactions where goods may not move through Estonia but financing is provided by credit institutions or payments are made using Estonian financial institutions.

In the recent past, the focus of awareness-raising has been on money laundering and terrorist financing. As a result, the issue of weapons of mass destruction and dual-use goods has received significantly less public attention and outreach to the financial sector has been moderate. At the same time, the probability of proliferation financing through Estonia can be considered very low, as our financial sector is mainly focused on serving Estonian customers and weapons of mass destruction or technologies/goods required therefor are not manufactured in Estonia.

Through the financial sector, it is possible to carry out the purchase and sale transactions of strategic (military, dual-use) goods through transactions related to trade financing.[44] This risk exists; however, international standards do not require financial institutions to identify dual-use goods independently due to the complexity of this issue. The main activity of financial institutions in preventing proliferation financing is to ensure that they freeze and not make funds available and not provide financial services to designated persons and entities and not finance proliferation of weapons of mass destruction by giving customers funds for such transactions. If, in the course of applying due diligence measures, a financial institution establishes or suspects that a transaction is related to prohibited goods, it will not execute the transaction and will notify the Financial Intelligence Unit of the suspicious transaction.

Awareness in this area is moderate and it is not possible to obtain much practical information from public sources. On the Estonian Internal Security Service's home page one can read about the prevention of proliferation of weapons of mass destruction[45], and the website of the Ministry of Foreign Affairs provides an overview of legislation related to strategic goods, with no separate attention paid to weapons of mass destruction. The Strategic Goods Act in force in Estonia considers weapons of mass destruction and their targeting systems to be military goods. All activities related to strategic goods require a special permit. Guidelines and threat indicators are also available on the website of the Ministry of Foreign Affairs, providing a general picture in relation to "strategic goods", yet not separately highlighting the topic of weapons of mass destruction.

It is possible to check on the website of the Tax and Customs Board[46] whether trade in goods with a specific commodity code has been restricted.

Financial institutions use a risk-based approach in their monitoring systems and application of due diligence measures. The enactment by financial institutions of financial sanctions and other due diligence measures concerning proliferation financing was supervised until 1 January 2021 by the Financial Intelligence Unit that has not been able to deal with this topic in any depth due to a lack of resources. As from 1 January 2021, the Financial Supervision Authority supervises (targeted) financial sanctions, including financial sanctions related to proliferation financing, in the financial sector.

Based on survey results, the efficiency of market participants' conformity check systems can be assessed as follows:

[44] For example: letters of credit, factoring, escrow, various guarantees, loans, credit insurance, etc.
[45] https://www.kapo.ee/et/content/massihävitusrelvade-leviku-tõkestamine.html
[46] https://apps.emta.ee/arctictariff-public-web/#!/taric/nomenclature/sbn?sd=11.01.2021&d=I&cc=&l=et&ql=et&ea=false

- The adequacy of conformity check systems is assessed on a regular basis[47];
- The monitoring systems of market participants with the greatest impact are automated[48]; as a rule, automation of other market participants' monitoring systems also corresponds to the service volumes;
- Sanction lists are updated regularly and automatically[49];
- The selection and calibration of transaction monitoring scenarios is generally in line with the relevant entity's profile and risks arising therefrom[50], while some market participants have room for improvement to further enhance their capabilities by allowing real-time monitoring and suspension of transactions and being more risk sensitive[51];
- Transaction monitoring systems for the most influential market participants allow the detection of certain complex or unusual transactions, yet should nevertheless be more risk sensitive[52];
- Most market participants have a system in place that allows for a risk-based calculation of the client's risk level[53];
- Most market participants invest in technical solutions of risk management and mainly invest in programs and software[54].

Based on the international sanction notifications sent to the FIU, it can be stated that the conformity check systems of financial institutions are efficient and able to identify persons and entities designated by the relevant sanctions lists.

The following vulnerabilities were identified in a survey on the quality of the customer check framework:

- Information on beneficial owners in national registers is not always reliable;
- It is difficult to access information required to identify beneficial owners;
- It is difficult to access information required to identify and check other high-risk customers (e.g. embassies, virtual currency service providers, undertakings that provide financial services, non-profit associations, etc.).

The quality of the due diligence measures framework is generally high. From the point of view of customer checks, major problems include the complexity of the process of identifying the beneficial owner and lack of a reliable source for verifying the beneficial owner's information. In addition, it is difficult to identify all parties to trade financing transactions, as financial institutions may not see the entire transaction chain.

As a rule, the quality of identifying international sanctions is high. Although the topic of dual-use goods is very specific and requires highly extensive knowledge from the financial sector, it is not expected that financial institutions identify dual-use goods independently, as this is a complex issue for financial institutions. The financial sector should foremost pay attention to transactions related to high-risk countries in which goods are brokered and/or the transaction is financed, yet where the goods may not cross the Estonian customs border at all.

[47] Based on the results of surveys of credit institutions, payment institutions, investment firms, life insurance undertakings

[48] Based on the results of surveys of credit institutions, payment institutions, investment firms

[49] Based on the results of surveys of credit institutions, payment institutions, life insurance undertakings

[50] Based on the results of surveys of credit institutions

[51] Based on the results of surveys of management companies, payment institutions, investment firms

[52] Based on the results of surveys of credit institutions, payment institutions, life insurance undertakings

[53] Based on the results of surveys of credit institutions, management companies, payment institutions, investment firms, life insurance undertakings

[54] Based on the results of surveys of credit institutions, payment institutions, investment firms, life insurance undertakings

On a scale of 0-4, the financial sector's vulnerability rating for proliferation financing is 1.75 or **average-low**.

The following mitigation measures are envisaged to manage the residual risks of proliferation financing in the financial sector:

1) establishing, in cooperation with the competent authorities, model scenarios to help market participants identify and analyse risks associated with their activities;
2) raising awareness and adding to the available instructions a chapter "About Weapons of Mass Destruction" that would include clear descriptions of practical measures and potential threats;
3) it is certainly also important to inform economic agents outside the financial sector about the relevant topic;
4) encouraging obliged entities to also inform the FIU of transactions where it is identified or suspected that proliferation financing is involved.

### 12.4.2.2. Fintech sector

According to information obtained from special literature, WMD distributors use official financial service providers for two main purposes:

1) to pay for the acquisition of goods related to weapons of mass destruction;
2) for the collection, laundering, and movement of money related to the proliferation of nuclear (or biological or chemical) weapons (e.g. money ultimately paid for weapons of mass destruction or profits from the proliferation of weapons of mass destruction) [55]. In doing so, they would make the financial technology sector part of their distribution plan.

The vulnerability of the Fintech sector may foremost be magnified by insufficient awareness as related to the application of international sanctions, weapons of mass destruction, and dual-use goods. Knowledge gaps can also occur among regulators which in turn may lead to regulations not always meeting the real needs or lacking sector-specific guidelines for tackling risks.

The topic of weapons of mass destruction and dual-use goods has received significantly less public attention than, for example, the field of money laundering and terrorist financing and outreach to the financial technology sector has been moderate.

Threats posed by virtual currencies mainly lie in their characteristics: technology that allows relative anonymity, the ease of use of which and insufficient implementation of Know Your Customer (KYC) rules by service providers allow abuse of the virtual currency sector for criminal purposes. In recent years, the DPRK has put a lot of effort in abusing virtual asset (cryptoasset) providers, such as virtual currency exchange service providers, to evade the UN Security Council's sanctions. In its 2019[56] and 2020[57] reports, the PoE highlighted a number of tactics and techniques used by the DPRK with the aim of illegal collection of virtual currencies and mining activities, including by way of using sophisticated technological operations and malware. There is no clear answer to the question of how the DPRK then converts its virtual assets into fiat currency.

Since May 2019, the DPRK has increased its Monero mining activity at least tenfold (compared to Bitcoin mining in the same period). Monero is a virtual currency similar to Bitcoin that offers additional anonymity and does not necessarily require computers with the same performance capacity for mining.[58]

[55] Kassenova, T., The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation, https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221

[56] https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf

[57] https://undocs.org/S/2020/840

[58] For example, Bitcoin ransom payments made by WannaCry victims were transferred to Bitcoin wallets and were finally converted to Monero using the Swiss virtual currency exchange platform ShapeShift.

By 2019, at least 35 cases were reported to the PoE where persons of DPRK origin had committed cyber-attacks against financial institutions, virtual currency exchangers, and miners with the objective of stealing virtual currencies for profit. So as to limit the traceability of transactions, the DPRK, like money launderers, uses various digital asset stratification methods, such as creating thousands of virtual currency wallets with different service providers. During 2019, the DPRK attacks became even more acute against virtual currency exchange platforms; some virtual currency exchange platforms have been victims of such attacks repeatedly and for that reason have terminated their activities.[59]

In the case of crowdfinancing, the main threats include under-regulation of the relevant sector and a lack of sector-specific guidance materials on the prevention of the proliferation or financing of weapons of mass destruction.

Sources of threat also include market participants financed and/or settled through the financial technology sector that may be exploited without their own knowledge due to their relatively low awareness. The threat may, similarly to the financial sector, occur in various intermediation transactions, where the goods may not move through Estonia, but financing is provided by an Estonian financial technology service provider. Uneven application of checks of beneficial owners internationally can also pose a threat.

In the case of the financial technology sector, threats posed by the cyber and crypto domains must be highlighted separately. For example, dark web transactions, organised cybercrime, increased reliance on information technology, and movement of critical services to the cyber environment.[60] Cyber and crypto domains can be used for illegal purposes, including for programmes related to weapons of mass destruction or to obtain funds.[61]

The risk of evasion of sanctions against the DPRK in the case of the virtual currency service providers sector is **high**.

Vulnerability is increased by the fact that information on sanctions regimes as well as on activities by the DPRK or Iran is often not available from official channels and is surfacing through the press, where the service providers may not pay attention to at the correct time. For the purposes of the International Sanctions Act, virtual currency service providers constitute "persons having specific obligations" on account of which their internal procedures must include among other things appropriate measures to act in the case of suspicion of sanctioned persons or transactions.

The implementation of financial sanctions related to the financing of weapons of mass destruction in the financial technology sector is monitored by the Financial Intelligence Unit that has not been able to address this issue in depth due to a lack of resources.

Approximately 50% of companies do not have dedicated mechanisms in place (e.g. to detect or prevent evasion of sanctions, terrorist financing (here the lack of mechanisms is lower, just 25%), radical movements, cash flows related to dual-use goods, etc.). Also, about 40% of companies answered "no" or "don't know" about documenting the asset freezing procedure.

The risk of the virtual currency sector in the field of weapons of mass destruction is the same as in other sectors. Technology that enables relative anonymity, ease of use, and insufficient implementation of the Know Your Customer (KYC) rules means the highest possible risk of criminal exploitation. The probability of the virtual currency exchangers to be exposed to the relevant threat is high in relation to the

[59] Youbit (formerly Yapizon) fell under repeated cyber-attacks in April 2017, losing $4.8 M, and an additional 17% of total assets in December 2017, forcing it to terminate its activities.

[60] Developments in the security environment on the Baltic Sea region until 2020; https://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/RIIGIKOGU_RAPORT-2.pdf, p. 35

[61] See, for example, this paper on North Korea: Kassenova, T., The Exploitation of the Global Financial Systems for Weapons of Mass Destruction (WMD) Proliferation, https://carnegieendowment.org/2020/03/04/exploitation-of-global-financial-systems-for-weapons-of-mass-destruction-wmd-proliferation-pub-81221

DPRK's activity and various tactics to use the virtual currency sector to earn illegal income. The crowdfinancing as a service is not a problem in the context of the financing of weapons of mass destruction.

Virtual currency service providers are particularly vulnerable due to the threat of breaches of sanctions against the DPRK as it is known that the DPRK has recently been using virtual currencies to generate illegal revenue and to avoid the imposed sanctions. In view of the above, vulnerability related to virtual currency service providers as pertaining to the financing of weapons of mass destruction can be considered **average-high**.

Vulnerability related to crowdfinancing service providers as pertaining to proliferation financing was assessed "low".

For the above reasons, the identified residual risks of proliferation financing have not been adequately managed in the financial technology sector and the following measures should be taken:

1) supervisory authorities should compile sector-specific guidelines and guidance materials;
2) competent authorities should provide sector-specific training as pertaining to the prevention of proliferation financing;
3) establishing, in cooperation with the competent authorities, model scenarios to help market participants identify and analyse risks associated with their activities;
4) virtual currency service providers should pay particular attention to DPRK-related activities, entities, and persons, and use efficient measures to develop indicators of DPRK origin among customers;
5) enhanced due diligence measures must be applied in situations where the customer has an interest in exchanging a common virtual currency (Bitcoin) for virtual currencies that provide additional anonymity (such as Monero), and in particular when converting the latter type of virtual currency to fiat currency;
6) Pursuant to § 25 of the Republic of Estonia Money Laundering and Terrorist Financing Prevention Act, wallet service providers must ensure the identification of all customers, and, as an additional due diligence measure, additional measures must be taken to identify persons of DPRK origin.

#### 12.4.2.3. Traders' sector

The various sectors of traders included in the sample of the survey implemented within the framework of this NRA do not constitute persons operating in areas that could be involved in the production, transit, or financing of weapons of mass destruction. Proliferation of weapons of mass destruction and the related trade is very unlikely in the traders' sector as in the case of the relevant areas of activity these proliferation related activities would be clearly distinct from the relevant companies' normal business.

Estonia checks the trade flows exported across its border, paying attention to strategic goods and risks related to weapons of mass destruction. Proliferation financing can be considered impracticable issue in the context of the Estonian traders' sector.

Management's awareness of threats related to the proliferation of weapons of mass destruction and financing thereof is low, as the sectors' exposure is very unlikely: Estonia does not produce weapons of mass destruction or the components thereof. Awareness varies across sectors. Awareness is expected to be higher in the automotive and precious metals sectors as there are more obliged entities in these sectors on account of which awareness is higher. From the point of view of supervision, the biggest problem is the inadequacy of human and technological resources or insufficient skills and awareness to use available resources. As the sector is wide, there are also large differences in the quality of supervision within the sector. There are few sub-sectors where awareness and skills are sufficient.

Identifying proliferation financing is certainly a difficult task for traders as funding may be provided by the so-called "non-sanctioned" persons, whether knowingly or not. Indicators to pay attention to have not

been made available to traders by supervisory authorities. Information on the application of sanctions as well as regulations and procedures related to dual-use goods and for military goods is available on the websites of the authorities to anyone with an interest in these matters. Traders are generally aware of the obligation to notify the supervisory authority if terrorist financing is suspected when concluding a transaction with a customer or if an unusual transaction involves areas with a high terrorist threat, i.e. a high-risk country. However, in reality, no reports have been filed due to either absence of these situations or inefficiency of detection. The information systems used to identify high-risk customers and verify customer data could not be evaluated due to scarce experience and awareness. Awareness of the existence of sanctions lists is generally low and comparison of lists/products/persons is not provided for in any detail within companies' internal work organisation.

The vulnerability of the traders' sector in relation to proliferation financing needs to be viewed as a whole along with all the strategic goods: weapons of mass destruction, all military goods, and dual-use goods. Despite the fact that the risk is small, the topic is very specific and requires exceedingly extensive knowledge.

The main vulnerability is the general low awareness of traders (except traders that knowingly deal in strategic goods and have obtained a relevant permit) which may lead to a situation where a trader, without being aware of it (or knowingly), intermediates products or services that may be included on the list of strategic goods or contain parts/materials/details that are on the list. The list of strategic goods exists and is freely available on the website of the Ministry of Foreign Affairs. Sanctioned (embargoed) goods may pose a higher risk as restrictions related to such goods depend on the specific country and person. Embargo restrictions also cover goods other than strategic goods. Lists of sanctions are also available on the website of the Ministry of Foreign Affairs.

There are few traders that have trade relations specifically with Iran and Estonia does not have trade relations with the DPRK, on account of which the probability of breaching these sanctions regimes in the traders' sector can be considered **very low**.

For the above reasons, the following measures can be recommended to manage the low residual risk:

1) at the national level, risks can be managed by creating model scenarios in cooperation between the competent authorities which would help market participants identify and analyse the risks associated with their activities;
2) within the sector, risks can be managed foremost by raising awareness and adding to freely available instructions a chapter "About Proliferation Financing" that would include clear descriptions of practical measures and potential threats.

#### 12.4.2.4. Real estate sector

The sector is unlikely to be exposed to proliferation financing. The implementation of the DPRK and Iran sanctions lists upon acquisition of real estate is monitored by the land registrar whose specific obligation arises from § 25 (1) 4) of the International Sanctions Act and who notifies the FIU of identification of a subject of a financial sanction or a transaction or an act that breaches a financial sanction.

#### 12.4.2.5. Non-profit sector

In preventing the proliferation of weapons of mass destruction and financing thereof, it is very difficult to identify vulnerabilities in organisations operating for charitable, religious, cultural, educational, social, or family purposes as exposure is minimal. There are no cases in Estonia in this respect. Such activities may occur that potentially breach sanctions regimes within the education sector as know-how or the movement of laboratory equipment could be made available to criminals, especially from the point of view of the threat of breaching the Iranian sanctions regime.

In terms of security authorities, a distinction can be made between dual-use goods and aspects related to weapons of mass destruction. The risk of proliferation of weapons of mass destruction is low in Estonia, and Estonia does not produce weapons of mass destruction or technologies/goods required therefor. To date, there have been no cases in our territory where attempts would have been made to use or fund nuclear, biological, radioactive, or chemical material in an attack.

The biggest threat related to weapons of mass destruction is considered to be cross-border proliferation, in the case of which Estonia could be used as a transit country.

Organisations operating for charitable, religious, cultural, educational, social, or family purposes may face certain specific threats due to their wish to support people in need in the DPRK or, in the case of Iran, to engage in educational cooperation that may in practice involve research related to the development of nuclear weapons. For humanitarian purposes, derogations from sanctions are also allowed in certain cases. This, in turn, entails additional risks. However, it is known that the Estonian non-profit sector does not currently mediate assistance or relations to these countries.

Based on expert assessment, the sector's vulnerability level in proliferation financing is **low**.

The following measures should be implemented to manage residual risks:

1) creating model scenarios in cooperation between the competent authorities which would help market participants identify and analyse risks associated with their activities;
2) within the sector, risks can be managed foremost through awareness-raising and supplementation of freely available instructions outlining practical measures and potential threats.

**12.4.2.6. Company service providers' sector**

Looking at trends in the financing of weapons of mass destruction, the UN Security Council's Panel of Experts (PoE) on the DPRK Sanctions Regime has found that the Democratic People's Republic of Korea continues to have access to the international financial sector through various joint ventures, offshore accounts, shell companies, and virtual assets. Analysis results show that the DPRK continues through related entities and persons to use the banking systems of East and South-East Asia, and, through that, wider international correspondent banking. The PoE has also criticised Member States for insufficient efforts to establish rules for the registration of companies which has continued to allow the DPRK to take advantage of non-transparent company structures. Gaps in corporate registration control mechanisms make Know Your Customer processes and procedures in financial institutions virtually impossible.

With regard to Iran, the same trends and patterns have not been analysed with regard to Resolution 2231, and UN Member States have reported individual possible violations of the sanctions regime, including possible financing activities. Due to limited trade with Iran as well as on account of a lack of a nuclear weapons and related technology sector in Estonia, violation of the sanctions regime is thus mainly associated with threats by persons and entities on the sanctions lists trying to transact with or with the help of Estonian companies.

For the purposes of the International Sanctions Act, company service providers do not constitute persons having specific obligations; on the other hand, they are obligated under the EU directly applicable regulations to freeze the assets of persons included on both the DPRK and Iranian lists of sanctioned persons.

The residual risk in the sector is **high** for the above reasons, and it may happen that company service providers are exploited by sanctioned persons for the purpose of setting up companies. As the provisions of the Money Laundering and Terrorist Financing Prevention Act are mainly applied in the sector by way of general application regime, upon implementation of which the guidelines of the FIU must be taken into account, the practice of application of due diligence measures cannot be considered appropriate in the case of risks of proliferation financing/application of international sanctions. As the service providers in

question are not financial institutions, stricter identification requirements do not apply, i.e. services may in certain cases be provided without identification. For example, in the absence of a business relationship, for transactions below the EUR 15,000 threshold and no other legislative terms or conditions apply.

To manage the risks:

- the legal provisions should be amended so that the use of services in the sector without identification would not be permitted and it would be ensured that persons on the list of sanctioned persons do not have access to the services of company service providers.

#### 12.4.2.7. Lawyers, auditors, bailiffs, other legal service providers, notaries, pawnbrokers, accountants, gambling operators

Exploitation of these sectors for proliferation financing through violations of the DPRK or Iranian sanctions regimes can be considered unlikely and it is therefore not appropriate to separately analyse the vulnerability of the sectors in this respect.

The general regulation for the application of international sanctions applies.

### 12.5. Consequences of proliferation financing

In Estonia, the consequences of proliferation financing must be assessed at the national level through the potential impact of the materialised violation of a sanctions regime on:

a) national security,
b) the economy,
c) the political situation (incl. the country's reputation), and
d) society

The consequences of proliferation financing, i.e. the use of weapons of mass destruction, are more severe than those of money laundering or other financial crimes and are more akin to the potential loss of life associated with the consequences of terrorist financing. The possibility of financing such activities through Estonia has a great impact on national security. The associated negative consequences would include loss of confidence in us by our international partners and extensive damage to international peace and security.

The impact on the country's economy would be extensive: termination of correspondent banking relationships associated with the funding of WMD would lead to reduced access to financial services which damages national economy, raises interest rates, inflation; damaged credibility and a significant drop in customer confidence have negative consequences for international business relations, leading to reduction or suspension of foreign direct investment, financial market instability, and reduction in tax revenues.

The consequence for the country's political situation and reputation is considerable: the accompanying negative attention in international media and political scandals that have a long-term impact on the country's reputation; high likelihood of being classified under FATF's ICRG classification of "non-co-operative countries" in relation to inability to efficiently implement international sanctions; depending on the breached WMD proliferation regime, certain impact on political stability may be brought about due to hindrances in international relations.

The consequence for the society would be average as the target countries for the prevention of proliferation of WMD are located both geographically and culturally far from Estonia. It would certainly be accompanied by public condemnation, possible references to the weakening of ethical and democratic standards; the effects of the economic, security, and political situation would somewhat reduce the number of available jobs and general lowering of living standards.

### 12.6. Mitigation measures

In addition to relying on lists, obliged entities should apply additional due diligence measures to manage the risk of evasion of sanctions. The purpose of due diligence measures is to ensure that obliged entities understand the nature of their customers' business activity and identify and check the customers and beneficial owners to make sure that they are not directly or indirectly linked to persons and entities included on the list of sanctioned persons.

Obliged entities should apply a list of risk transaction indicators to manage the risks of funding of WMD. The relevant indicator demonstrates or refers to the likelihood of unusual or suspicious activity. The existence of a single indicator in relation to a customer or a transaction alone may not justify the suspicion of proliferation financing or necessarily indicate such activity clearly; however it may facilitate further monitoring and investigation. At the same time, the presence of several indicators may also justify the application of additional measures and gathering of information. Whether one or more indicators refer to proliferation financing also depends on the specific business, products, or services of a particular undertaking; how they interact with their customers; opportunities related to human and technological resources.

Depending on their field of activity and transaction partners, obliged entities should, in particular when operating in a cross-border manner, define in their internal rules of procedure and in accordance with their risk assessment which indicators should be subject to enhanced due diligence measures using comparisons with various additional external sources (e.g. the comparison of financial transactions, export/customs data, and open market prices).

**Indicators related to customer's risk profile**

- upon establishing a business relationship, the customer provides vague or incomplete information about their intended trading activities. The customer does not want to provide additional information about their activities if asked for additional information against the backdrop of negative information[62];
- continued application of due diligence measures reveals negative information about the customer, its owners, or senior management, such as past money laundering schemes, fraud, other criminal activities, or ongoing or past investigations or convictions, including non-compliance with lists of persons under export control regimes;
- the customer is a person associated with a country linked to proliferation of WMD or a diversion country (a country known to have been used to evade restrictions imposed on proliferation of WMD), e.g. persons with dual citizenship from such countries.
- the customer is a person who handles complex equipment for which they have no technical background or which does not correspond to their defined field of activity;
- the customer concludes complex commercial transactions involving a large number of third-party intermediaries in business areas that do not correspond to the risk profile defined upon the establishment of the business relationship;
- a customer or a party of a transaction concludes transactions that indicate that they are operating as a money remittance company or a payable through accounts. These accounts encompass rapid movement of large transactions and small end-of-day balances without any clear business reasons. In some cases, the initiators appear to be associated with entities that may be associated with a country with an WMD proliferation problem (such as shell companies operating in the country or in diversion countries in relation to the proliferation of weapons of mass destruction) and beneficial owners appear to be associated manufacturers or logistics companies subject to export control regimes;
- a customer related to a university or a research institution handles potentially WMD-sensitive goods or goods subject to export control.

**Indicators related to account or transaction risks**

[62] For example, asking for more information on the scope of their activities in countries subject to international sanctions

- the initiator or beneficiary of the transaction is a person or entity domiciled in a country with problems related to the proliferation of WMD or diversion of sanctions;
- account holders conclude transactions involving items controlled under multilateral export control regimes or national control regimes related to weapons of mass destruction;
- accounts or transactions encompass potential shell companies, e.g. companies do not have sufficient capital or publish (online) only the company's key figures;
- there are visible links between the representatives of the companies owned by different parties to the transaction, i.e. between the owners or the management, the same physical address, IP address or telephone number, or their activities; indications that their activities may be coordinated;
- the account holder makes "circular transactions" – the amount moves from account to account and returns to the original account in a similar manner;
- account activities or transactions where the associated financial institution's initiator or the recipient is located in a country with a weak export control regime (this is also important for correspondent banking services);
- the customer of a manufacturing or trading company wishes to use cash to pay for transactions in the case of industrial goods or commercial transactions. For financial institutions, transactions are visible through cash inflows to company accounts, followed by cash withdrawals;
- transactions are carried out on the basis of the so-called general ledger procedure (incl., for example, mirror transactions) which eliminates the need for frequent international financial transactions. The general ledger system is characterised by related companies that visibly keep records of transactions made on behalf of each other and transfers appear to pursue balancing objectives;
- the customer uses a personal account to purchase industrial goods that are subject to export control or that are otherwise unrelated to the company's activities or common business areas.

**Maritime sector risk indicators**

- the trader is registered at an address that is likely to be a mass registration address, e.g. dwellings, post office addresses, commercial buildings, or industrial complexes with a large population, especially if there is no reference to the operations of the relevant specific entity at that address;
- the person or entity preparing the shipment indicates a forwarding company as the final destination of the product;
- the destination of the consignment differs from the location of the importer;
- inconsistencies in contracts, invoices, or other business documents, e.g. discrepancies between the name of the exporting entity and the name of the beneficiary; various invoices and their underlying contracts; or discrepancies in the actual quantity, quality, volume, or value of the goods and descriptions thereof;
- the dispatch of the goods does not comply with the technical level of the country to which they are sent, e.g. semiconductor manufacturing equipment is shipped to a country where there is no electronics industry;
- the transport of goods takes place "in a circle" (if freight information is available), including several destinations without a visible commercial purpose;
- the transport of goods is not in line with traditional geographical trade patterns, e.g. the country of destination does not normally export or import the goods listed in the relevant trade transactions' documents;
- the consignee does not pay for the imported goods without clear economic reasons, e.g. instead, a non-commercial shelf or shell company makes the payment.

**Trade financing risk indicators**

- the shipment is routed through a country where export control laws are weak or enforcement of export control laws is feeble;
- before completing the establishment of the business relationship, the customer applies for a letter of credit for a transaction related to special regulations or dual-use goods;
- inconsistencies in trade documents and financial flows, such as names, companies, addresses, final destination, etc.;

- transactions involve instructions or payment details from or by parties not specified in the original letter of credit or another document.[63]

[63] Source: 2018 FATF Guidance on Counter Proliferation Financing and UNSC PoE reports