FIU LATVIA

Financial Intelligence Unit of Latvia



Translation from Latvian into English

MANAGING SANCTIONS RISKS IN TRANSACTIONS INVOLVING HEIGHTENED-RISK COUNTRIES

In cooperation with:

2025

LATVIJAS BANKA
EIROSISTĒMA

State Revenue Service
Republic of Latvia

FINANCE LATVIA ASSOCIATION

LDDK
EMPLOYERS' CONFEDERATION OF LATVIA

Table of contents

1. Introduction 3
2. General Provisions 4
Who must comply with the sanctions? 4
What types of sanctions are there? 5
What is sanctions risk? 6
What are high-risk countries? 7
3. Internal Control System 7
Sanctions risk assessment 8
Risks of targeted financial sanctions in transactions involving companies from high-risk countries 11
Risks of sectoral sanctions in transactions involving companies from high-risk countries 12
Measures for mitigating and managing sanctions risks 14
Defining 'red lines' 15
Measures for mitigating and managing the risks of targeted financial sanctions 16
Measures for mitigating and managing sectoral sanctions risks 18
Review and update of the ICS measures 23
4. Closing Provisions 23
Preconditions for effective cooperation with credit institutions 23
Useful information sources and tools 25

1. INTRODUCTION

1.1. In response to Russia's unprovoked and unjustified military aggression against Ukraine, the European Union (EU) has imposed extensive and unprecedented restrictive measures (sanctions) against Russia, introducing various types of sanctions, including restrictions on cooperation with certain individuals, restrictions on the export and import of goods, restrictions on the transfer of intellectual property and trade secrets related to sanctioned goods, restrictions on the provision of certain services, etc. Similar sanctions have also been imposed against Belarus in connection with its involvement in the Russian aggression against Ukraine.

1.2. A number of countries have been identified at EU and national level that do not impose sanctions on Russia and Belarus and that, due to their geographical location or for other reasons, are used to transport sanctioned goods to Russia or Belarus, creating a heightened sanctions risk when doing business with companies in those countries. These countries can also be used to circumvent other restrictions, including targeted financial sanctions, restrictions on the import of goods, and restrictions on the provision of services. **The countries identified as posing a heightened sanctions risk include the United Arab Emirates (UAE), Armenia, Azerbaijan, Georgia, India, Kazakhstan, Kyrgyzstan, China (including Hong Kong), Mongolia, Serbia, Thailand, Tajikistan, Türkiye and Uzbekistan (hereinafter – high-risk countries).**

1.3. The EU, Japan, the United Kingdom, and the United States have jointly identified so-called **common high priority items**[1] (hereinafter – CHP items) which are important for Russia to continue its military aggression and which enter Russia by circumventing sanctions. The EU has imposed the obligation on **persons selling, supplying, transferring, or exporting CHP items** (hereinafter – the exporters of CHP items) **to take certain measures, including performance of a documented risk assessment and implementation of policies, controls, and procedures to mitigate and effectively manage sanctions evasion risks** associated with the trade and export of CHP items.[2]

1.4. This guidance document is designed to help businesses manage their sanctions risks, including understanding how to develop and implement a set of measures or the **Internal Control System (ICS)** to mitigate and manage sanctions risks when doing business with companies from high-risk countries, in particular transactions involving sanctioned goods or services. While the focus of the guidance is on sanctions risks in transactions involving companies from high-risk countries, the sanctions risk management measures described in the guidance document are also applicable to any direct or indirect transactions of economic operators with companies in Russia and Belarus.

1.5. The exporters of CHP items[3] can use this guidance to comply with their obligation to develop and implement the ICS for the purpose of mitigating and effectively managing

[1] EU and G7 list of CHP items: https://finance.ec.europa.eu/publications/list-common-high-priority-items_en
EU and G7 guidance document "Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry". Available at: https://finance.ec.europa.eu/publications/preventing-russian-export-control-and-sanctions-evasion-updated-guidance-industry_en

[2] Article 12gb of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (hereinafter – Council Regulation (EU) No 833/2014)
Article 8ga of Council Regulation (EC) No 765/2006 of 18 May 2006 concerning restrictive measures in view of the situation in Belarus and the involvement of Belarus in the Russian aggression against Ukraine (hereinafter – Council Regulation (EC) No 765/2006)

[3] The term 'exporters of CHP items' in the context of this guidance means a natural or legal person who sells, supplies, transfers, or exports CHP items. CHP items are listed in Annexes XL and XLVIII to Council Regulation (EU) No 833/2014 and Annexes XXX and XXXI to Council Regulation (EC) No 765/2006.

sanctions risks. At the same time, exporters of CHP items must implement and apply internal control measures to all transactions, including those with companies outside high-risk countries.

1.6. This guidance material has been developed in accordance with the information sources and best practices of the European Commission, the Financial Intelligence Unit of Latvia (FIU), and other countries. The material focuses on managing the risks of EU sanctions imposed against Russia and Belarus, but can also be used to manage other sanctions risks.

1.7. This guidance has been developed by the FIU in cooperation with the Finance Latvia Association, Latvijas Banka, the National Customs Board of the State Revenue Service (SRS), the Ministry of Foreign Affairs, and the Employers' Confederation of Latvia. The guidance has been developed in consultation with Latvian credit institutions.

1.8. This guidance material is of a recommendatory nature and should not be regarded as statement of one's rights or binding legal guidance from the FIU.

2. GENERAL PROVISIONS

Who must comply with the sanctions?

2.1. The Law on International Sanctions and National Sanctions of the Republic of Latvia[4] stipulates that all persons must comply with and implement international and national sanctions. All persons are required to comply with and implement sanctions on their own initiative, without any prior warning, taking into account the specific factual circumstances of each individual situation. A person may not rely on the fact that, when concluding a transaction, sanctions have been complied with where a credit institution has executed a payment or a customs authority has allowed a cargo to cross a border, as the authorities may not have complete information about the circumstances of the transaction and the parties involved.

2.2. EU sanctions must be complied with and implemented:
- 2.2.1. within the territory of the EU, including its airspace;
- 2.2.2. on board any aircraft or any vessel under the jurisdiction of a Member State;
- 2.2.3. by any individual who is a national of a Member State, either within or outside the EU;
- 2.2.4. by all legal persons, entities, or bodies registered or established in accordance with the laws and regulations of an EU Member State;
- 2.2.5. by any legal person, entity, or body in respect of any transaction concluded in whole or in part in the EU.[5]

2.3. Furthermore, an individual must also take all appropriate measures to ensure that a legal person owned or controlled by them, including a legal person established outside the EU, is not involved in actions that would result in a violation of EU sanctions. In

[4] Section 2, Paragraph two of the Law on International Sanctions and National Sanctions of the Republic of Latvia, available at: https://likumi.lv/ta/id/280278-starptautisko-un-latvijas-republikas-nacionalo-sankciju-likums; unofficial translations in English available here: https://likumi.lv/ta/en/en/id/280278-law-on-international-sanctions-and-national-sanctions-of-the-republic-of-latvia

[5] Article 13 of Council Regulation (EU) No 833/2014; Article 10 of Council Regulation (EC) No 765/2006; Article 17 of Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine (hereinafter – Council Regulation (EU) No 269/2014).

certain cases, an individual must also ensure that a non-EU legal person owned or controlled thereby complies with specific requirements of the EU sanctions framework.[6]

What types of sanctions are there?

2.4. Sanctions can be divided into two basic types:
  2.4.1. **targeted financial sanctions**;
  2.4.2. **sectoral sanctions.**

2.5. Targeted financial sanctions:
  2.5.1. provide for the obligation to freeze all funds and economic resources belonging to, owned, held, or controlled by persons included in the EU targeted financial sanctions lists ~~or persons, entities, or bodies associated with them~~; and also
  2.5.2. prohibit making funds or economic resources available, either directly or indirectly, to or for the benefit of persons included in the EU targeted financial sanctions lists or persons, entities, ~~or bodies associated with them~~.[7]

2.6. In essence, **this means that it is prohibited to engage, directly or indirectly, in any transactions with natural or legal persons included on EU targeted financial sanctions lists, or with legal persons that are directly or indirectly owned 50% or more or controlled by EU-listed persons** (hereinafter – sanctioned persons). Control means, for example, the right of a person included in the EU targeted financial sanctions lists to exercise a controlling influence over a company, to unanimously decide on the appointment or removal of employees or officials of the company, to take other decisions related to the company, as well as other criteria and indications through which it is possible to detect that the company is controlled by a sanctioned person. Further information on the control measures and their criteria is available in the guidance material "EU Best Practices for the effective implementation of restrictive measures" issued by the Council of the European Union[8] (hereinafter – the Sanctions Best Practices).

2.7. **Sectoral sanctions are generally sanctions imposed against specific goods or services, prohibiting the provision of services and import, export, or transit of goods.** They may target specific sectors that are essential to the economy of a particular country or region and include, for example, measures such as restrictions on trade, investment, financing, or technology transfer in certain sectors, prohibitions or restrictions on the export or import of certain goods and technology, as well as prohibitions on the provision of financial services or investment, and other measures. It should be noted that in response to Russia's full-scale military invasion of Ukraine, the **EU has imposed sectoral sanctions against Russia and Belarus, covering a very wide range of goods and sectors, as well as unprecedented types of sectoral sanctions.** It is therefore important to understand that an increasing range of sectors, goods, and services are now subject to sectoral sanctions and it is important to be aware of the different types of sectoral sanctions in order to ensure compliance with sanctions and prevent persons from becoming involved in sanctions violations or circumvention.

2.8. EU sanctions provide for certain narrowly defined derogations to sanctions, where a prohibited activity may be carried out if authorised by the competent authority (in

[6] Article 12gb, Paragraph 3, of Council Regulation (EU) No 833/2014; Article 8ga, Paragraph 3 of Council Regulation (EC) No 765/2006.
[7] Article 2 of Council Regulation (EU) No 269/2014; Article 2 of Council Regulation (EC) No 765/2006.
[8] Paragraphs 64 to 67 of the guidance material "EU Best Practices for the effective implementation of restrictive measures" issued by the Council of the European Union, available at: https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/en/pdf

Latvia – the FIU).[9] EU sanctions also provide for certain narrowly defined exemptions under which sanctions do not apply in specific circumstances, for example where a pre-existing contract (i.e., one concluded before the relevant sanctions were imposed) is performed within the time limits specified in the sanction's regulations.

What is sanctions risk?

2.9. Sanctions risk refers to the potential **threats** and **vulnerabilities** that could lead to a **violation of sanctions**.

2.10. When implementing sanctions, it is required to ensure that all restrictions imposed by international and national laws and regulations governing sanctions are complied with immediately and without any prior warning.[10] It is prohibited to engage in actions aimed at violating sanctions. A person **may be held administratively**[11] **or criminally liable**[12] for violating sanctions.

2.11. It is **prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent prohibitions imposed with the sanctions regulations, including by participating in such activities without deliberately seeking that object or effect but being aware that the participation may have that object or effect and accepting that possibility**.[13] This means that liability for a sanctions violation may also arise where a person enters into a transaction knowing that their involvement may result in sanctions being circumvented, but fails to take measures to prevent such circumvention.

Table 1: Examples of sanctions violations and circumvention

Examples of sanctions violations and circumvention
▪ An economic operator concludes a transaction with a legal person that is at least 50% owned by a person included on the EU targeted financial sanctions list or is controlled by this person. ▪ An economic operator, when exporting or importing sanctioned goods, indicates an incorrect Combined Nomenclature[14] (CN) code for the goods, claiming that the goods are not subject to sanctions.

[9] According to Section 10, Paragraph one of the Sanctions Law, if international or national sanctions provide for specific exceptional cases in the implementation of sanctions, the FIU may, upon a reasoned written submission submitted by the sanctioned person or the person who wishes to perform activities covered by the international or national sanctions, take the decision to apply such exemptions, except for the cases referred to in Paragraphs $1.^1$, $1.^2$, and $1.^3$ of this Section. The submitter of the written submission has the obligation to indicate in the submission the need for the application of the exemption and the legal basis thereof, and the submission shall be accompanied by the documents and information justifying the application of the exemption. For more information see: https://sankcijas.fid.gov.lv/en/noderigi/iesniegums-atlaujas-sanemsanai

[10] Paragraph 15 of Cabinet Regulation No. 184 of 26 March 2024, Procedures for the Proposition and Implementation of International and National Sanctions, unofficial translations in English available at: https://likumi.lv/ta/id/350812-starptautisko-un-nacionalo-sankciju-ierosinasanas-un-izpildes-kartiba

[11] See Section 18 of the Sanctions Law in force from 10.06.2025.

[12] Section 84 of the Criminal Law, unofficial translation in English available at: https://likumi.lv/ta/en/en/id/88966-criminal-law

[13] Article 12 of Council Regulation (EU) No 833/2014; Article 1m of Council Regulation (EC) No 765/2006; Article 9 of Council Regulation (EU) No 269/2014.

[14] The Combined Nomenclature is the EU customs tariff nomenclature for goods, implemented based on the World Customs Organization's Harmonized System (HS) Convention. The HS Convention nomenclature is the (first) six-digit level of goods nomenclature used as the basis for the national (or regional) customs tariff nomenclature for goods of more than 200 countries, i.e. the national (or regional) customs tariff nomenclature for goods of the HS Convention Contracting Parties are identical at the level of the first six digits. The HS nomenclature is also the basis for the customs tariff nomenclature for goods of the Eurasian Economic Union, including Russia and Belarus among its member countries. The EU Combined Nomenclature was introduced by Council Regulation (EEC) No 2658/87 of 23 July 1987 on the tariff and statistical nomenclature and on the Common Customs Tariff, available at: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A01987R2658-20250101&qid=1749037014371

- A company exports goods subject to sanctions to a third country neighbouring Russia or Belarus without verifying the end-user, and the recipient subsequently supplies the goods to an end-user in Russia or Belarus.
- An exporter of CHP items has failed to take appropriate measures to prevent the risks of sanctions being circumvented, resulting in CHP items being exported to Russia or Belarus.
- An economic operator provides business management software to its subsidiary in Russia without obtaining prior authorisation from the FIU.
- An economic operator provides consultancy and training or technical assistance related to the manufacture of sanctioned goods to its subsidiary in Russia or Belarus.

What are high-risk countries?

2.12. Countries posing a heightened sanctions risk are those identified as being used to circumvent sanctions imposed against Russia, based, among other sources, on suspicious transaction reports received by FIU Latvia, information provided by the Customs Board of the SRS on transactions showing indicators of sanctions circumvention, and information compiled by competent authorities of the EU, its Member States and other countries. The countries identified as high-risk countries include:

2.12.1. member countries of the Eurasian Economic Union – **Armenia, Kazakhstan**, and **Kyrgyzstan**;[15]

2.12.2. countries of the Commonwealth of Independent States – **Azerbaijan, Tajikistan, Uzbekistan**;

2.12.3. other countries not imposing sanctions on Russia – **China (including Hong Kong), Georgia, India, Mongolia, Serbia, Thailand, Türkiye, and the UAE.**

2.13. It is important to note that the list of high-risk countries mentioned above is not exhaustive and may change over time. Economic operators should keep track of the latest information on routes and countries used for circumventing sanctions (especially in the **Southeast Asia**).

2.14. It should be noted that, among other factors, as a result of diplomatic efforts by the EU and other countries, a number of high-risk countries are taking certain measures to reduce the circumvention of sanctions through their jurisdictions.

2.15. Cooperation between economic operators and companies from high-risk countries can only take place if the cooperation does not result in sanctions violations, which can be ensured through appropriate measures aimed at ensuring compliance with sanctions requirements and managing sanctions risks.

3. INTERNAL CONTROL SYSTEM

3.1. The ICS is a set of measures that includes actions aimed at ensuring compliance with sanctions requirements. These actions should be seen as a process whereby:

3.1.1. sanctions risk assessment identifies those aspects of the business activity of an economic operator where sanctions risks exist;

3.1.2. risk management and mitigation measures are designed, implemented, and applied, including introduction and performance of transaction due-diligence;

3.1.3. the ICS is subject to periodic review and updating.

[15] Notice to economic operators, importers and exporters (2022/C 145 I/01), available at: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=oj%3AJOC_2022_145_I_0001

3.2. The purpose of implementing the ICS is to mitigate and manage sanctions risks. Sanctions risk assessment helps an economic operator to identify the specific ICS measures that need to be put in place. There is no one-size-fits-all model for the ICS. Thus, when implementing the ICS, a company must take into account the sanctions risks identified during the sanctions risk assessment and also other factors, such as the size of the company, the scope of its activities, the number of transactions, and the number of employees.

3.3. The primary responsibility for managing sanctions risks and implementing the ICS lies with the management body of a company. The management body must designate the person responsible for implementing and updating the ICS and ensure that the person responsible for the ICS has the knowledge necessary for the job. Necessary resources (financial, IT, and human resources) should be provided to ensure effective sanctions risk management. Additionally, steps should be taken to provide training activities aimed at increasing employee awareness of the ICS.

Sanctions risk assessment

3.4. The purpose of the sanctions risk assessment is to:
- 3.4.1. identify and assess the sanctions risks associated with the business activity, transactions, and counterparties of an economic operator;
- 3.4.2. determine which measures need to be implemented, ensured, or improved within a company to mitigate and manage sanctions risks.

3.5. The sanctions risk assessment should involve employees who are familiar with the processes, transactions, and counterparties relating to the specific areas of business activity.

3.6. The sanctions risk assessment requires obtaining and examining information on the actual transactions, counterparties, goods, and services of the particular economic operator. The sanctions risk assessment can be organised, for example, by formulating questions to which the sanctions risk assessment should provide answers based on both internal data of the economic operator and external information. The questions should be formulated in such a way that they help to identify those transactions which are exposed to sanctions risks (see paragraphs 3.11 to 3.24 below) and identify specific measures to be put in place to mitigate and manage these risks (see paragraphs 3.25 to 3.54 below).

3.7. Examples of questions that an economic operator may ask as part of the sanctions risk assessment are given in Table 2. The list of questions provided in the table is not exhaustive and not all listed questions will be relevant to the specific type of business activity of the economic operator, thus, the economic operator should consider only those questions that are relevant to its business activity.

3.8. The economic operator must define the period for which the sanctions risk assessment is carried out, for example, the previous year or the last two years up to the moment of conducting the risk assessment. Accordingly, when answering the questions in the sanctions risk assessment, the economic operator shall take into account the actual data on the business activity of the economic operator for the relevant period.

Table 2: Examples of questions for the sanctions risk assessment

What transactions are concluded by an economic operator?
▪ What kind of services are provided and received, and to what extent? ▪ Do the services relate to any particular goods? If so, please specify which goods.

▪ To what extent and what types of goods and technologies are sold and purchased? What are the CN codes of these goods and technologies?
What type and how many companies (counterparties and other interested parties) are identifiable in the concluded transactions?
▪ Buyers and sellers? ▪ Counterparty credit institutions? ▪ Payment recipients or payers? ▪ Brokering service providers? ▪ Service end-users? ▪ Importers and exporters of goods? ▪ Manufacturers, distributors, or end-users of goods? ▪ Transport, forwarding, and logistics service providers? ▪ Insurance service providers? ▪ Other companies?
Are companies from high-risk countries, Russia, or Belarus directly or indirectly involved in any transactions?
▪ What kinds and how many/what volume of transactions involved companies from high-risk countries, Russia, or Belarus during the assessment period (for example, how many and what volume of transactions in 2024 and in the first half of 2025)? ▪ In what types and volumes of transactions might companies from high-risk countries, Russia, or Belarus be involved in the future, considering the planned operational changes of the economic operator?
What information is available on companies from high-risk countries, Russia, or Belarus?
▪ Business registration details in commercial registers, tax registers? ▪ Information on the ownership structure and officials of the company? ▪ Information on the business activities of the company? ▪ Information on the cooperation partners of the company? ▪ Information on the business activity results of the company in previous periods? ▪ Information on the presence of company, their owners, officials, and cooperation partners on sanctions lists or their links to sanctioned persons, the Russian or Belarusian defence industry, or high-ranking Russian or Belarusian officials?
Are general measures in place to mitigate and manage sanctions risks?
▪ Are "red lines" defined, i.e., transactions or circumstances that pose such a high risk to the economic operator becoming involved in sanctions violations that it cannot manage the risk and therefore refrains from entering into such transactions? ▪ Has an employee or employees been designated with direct responsibility to take measures or carry out checks to mitigate and manage sanctions risks? ▪ Are sufficient human, IT, and other resources allocated to mitigate and manage sanctions risks, taking into account the type and scale of business activity and clients of the economic operator?
Are sufficient measures in place to mitigate and manage the risks of targeted financial sanctions in transactions involving companies from high-risk countries, Russia, or Belarus?
▪ Are the main companies directly and indirectly involved in the transaction identified, including sellers, buyers, end-users, distributors, manufacturers, logistics, storage, transport, and forwarding service providers, payers or payment recipients, credit institutions? ▪ Are companies, their owners, management body, and cooperation partners verified against sanctions lists of the EU, UN, and other countries or organisations and is such verification process documented?

- Are other risks of targeted financial sanctions relating to companies analysed and documented (for example, are the sanctions risk indicators listed in Table 4 of this guidance material assessed)?
- Is sufficient information on the ownership structure, management body, and counterparties (including end-users and manufacturers) of companies obtained and maintained to ensure that they are not included in the EU, UN, or other sanctions lists, and that the operations of the company do not meet the risk indicators of targeted financial sanctions?
- Are companies involved in transactions subject to periodic verification measures?

What information is available on goods and services in transactions involving companies from high-risk countries, Russia, or Belarus?

- Has the CN classification of the goods been carried out and is it known?
- Are the goods, according to their CN classification, subject to prohibitions or restrictions of sectoral sanctions, for example, listed in an Annex to Regulation (EU) No 833/2014 or Regulation (EC) No 765/2006?
- Are the goods listed in Annex VII to Regulation (EU) No 833/2014 or Annex Va to Regulation No 765/2006?
- Are the goods included in the list of CHP items?
- Are the goods or technologies included in the list of dual-use items?
- Are the goods included in the list of economically critical goods?
- Are the goods or technologies included in the Common Military List of the EU or the National List of Goods and Services of Strategic Significance of the Republic of Latvia?
- Is the country of origin of goods subjected to import restrictions known in import-related transactions?
- Is there a prohibition on the transit of goods through Russia or Belarus?
- Are the services subject to sectoral sanctions prohibitions, for example, under Article 5n of Regulation (EU) No 833/2014[16] or any other articles of Regulation No 833/2014?
- Is technical assistance, brokering services, or other services related to sanctioned goods or to the provision, manufacture, maintenance, and use of sanctioned goods provided?
- Is there any financing or financial assistance related to sanctioned goods?
- Are intellectual property rights or trade secrets sold, licensed, or otherwise transferred in relation to sanctioned goods?

Are sufficient measures in place to mitigate and manage the risks of sectoral sanctions in transactions involving companies from high-risk countries, Russia, or Belarus?

- Are checks carried out to verify the accuracy of goods classification?
- Are the end users of goods identified and are documents confirming the end-use obtained in export transactions?
- Are documents supporting the origin of the goods obtained and kept in import transactions?
- Is information on the transport route obtained?
- Are transport documents and documents confirming the import of the goods (import declarations) in the country of destination obtained and kept?
- Are transactions verified to ensure that sanctioned goods are not being diverted to Russia?
- Are transactions verified to ensure that sanctioned goods are not acquired or imported?

[16] Currently, Article 5n of Regulation (EU) No 833/2014 prohibits legal persons established in Russia and the Russian government from providing, either directly or indirectly, a range of services, such as construction, architectural and engineering services, legal advisory services and IT consultancy services, accounting, auditing, including statutory audit, bookkeeping or tax consulting services, or business and management consulting or public relations services, etc.

- Are other sectoral sanctions risks relating to the transaction analysed and documented (for example, are the sanctions risk indicators listed in Table 6 of this guidance material assessed)?
- Are users of the services and software provided identified and checks carried out to ensure that sanctioned services or software are not indirectly made available to Russian companies?
- Do the distributors of goods manufactured by the economic operator take measures intended for mitigating and managing the sanctions risks?

3.9. When identifying and assessing sanctions risks inherent to the operations of an economic operator, the economic operator should take into account the following:

3.9.1. sanctions risks described in this guidance material relating to transactions involving companies from high-risk countries (see paragraphs 3.11 to 3.24 below);

3.9.2. the risk indicators of targeted financial sanctions listed in this guidance material (see Table 4);

3.9.3. the risk indicators of sectoral sanctions listed in this guidance material (see Table 6);

3.9.4. the indicators of sectoral and targeted financial sanctions developed by the FIU;[17]

3.9.5. the national assessment of sanctions violation risks included in FIU Latvia's National Money Laundering, Terrorism Financing and Proliferation Financing Risk Assessment Report;[18]

3.9.6. information published by international organisations, the European Commission, the FIU, other national competent authorities, and non-governmental organisations on the indicators of sanctions risks, types and routes of circumvention, and examples;

3.9.7. information in the media about cases of sanctions circumvention;

3.9.8. other information available to the economic operator.

3.10. Transactions with sanctioned goods or services involving companies from high-risk countries or a territory or a jurisdiction of a high-risk country are to be regarded as transactions with a **heightened sanctions risk**. Any transactions involving companies, territory, or jurisdiction of Russia or Belarus are transactions exposed to a heightened sanctions risk. In order to ensure that the economic operator is not involved in sanctions violations, the economic operator must take appropriate measures to manage the risks associated with transactions exposed to a heightened sanctions risk.

Risks of targeted financial sanctions in transactions involving companies from high-risk countries

3.11. The EU targeted financial sanctions lists include, among others, leading businesspersons operating in Russia and Belarus, as well as legal persons that materially or financially support the Russian or Belarusian governments.

3.12. Targeted financial sanctions can, *inter alia*, be violated or circumvented by:

[17] FIU guidance material "Indicators of Sectoral and Targeted Financial Sanction Evasion", available at: https://sankcijas.fid.gov.lv/documents/file/vadlinijas%20en/Sanctions%20evasion%20risk%20indicators_2024_ENG%20(002).pdf

[18] National ML/TF/PF Risk Assessment Reports available at: https://www.fid.gov.lv/lv/darbibas-jomas/nilltfpf-risku-novertejumi-nra

3.12.1. doing business with a company that is a sanctioned person (directly included in the targeted financial sanctions list or owned or controlled by a sanctioned person);
3.12.2. doing business with a credit institution that is subject to targeted financial sanctions (for example, holding an account in a sanctioned credit institution, making payments from a credit institution established in a third country to a sanctioned credit institution, etc.);
3.12.3. supplying goods to a company without verifying the end-user of the goods, who then supplies them to a sanctioned person;
3.12.4. by entering into a transaction that indirectly provides an economic benefit to a sanctioned person (for example, renting goods from a company in a high-risk country where the goods are owned by another company that is subject to sanctions);
3.12.5. buying goods from a company in a high-risk country and the manufacturer of goods is a sanctioned person.

Risks of sectoral sanctions in transactions involving companies from high-risk countries

Trade and export of sanctioned goods to high-risk countries

3.13. Sectoral sanctions[19] impose prohibitions on a wide range of sanctioned goods intended for the **direct or indirect sale, supply, transfer, or export** to or for use in Russia and Belarus.

3.14. Such prohibitions also apply to the provision of technical assistance, brokering services, financing, financial assistance, and other services related to sanctioned goods and technology and to the provision, manufacture, maintenance, and use of such goods and technology, as well as to the sale, licensing, or transfer in any other form of intellectual property rights and trade secrets[20] related to sanctioned goods. The transit of certain sanctioned goods through Russia and Belarus is also prohibited.

3.15. The 'transfer' of goods is a broad concept covering a wide range of activities, i.e. not only the entry or exit of goods into or from the EU, but also the transportation of goods, including (but not exhaustively) their loading and transhipment. The prohibition on 'transfer' of goods applies not only to actual exports or imports (for example, goods entering or leaving the EU customs territory), but also when these products are not imported into the EU but are transported between Russia and a third country (and vice versa). Accordingly, prohibitions related to the export of goods must be complied with regardless of whether the export of goods is initiated in the EU and regardless of whether the goods cross the EU territory.[21]

3.16. Sectoral sanctions related to the trade and export of goods to high-risk countries can, inter alia, be violated or circumvented by:

[19] Council Regulation (EU) No 833/2014; Council Regulation (EC) No 765/2006.
[20] The definition of 'trade secret' is explained in Article 2(1) of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Available at: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32016L0943&qid=1745311842994
[21] European Commission Explanatory Notes "Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014." Issued 22.06.2022, last updated 28.04.2025, see Section A, Subsection 1, General Questions, Question 16, available at: https://finance.ec.europa.eu/publications/consolidated-version_en

3.16.1. selling, exporting, or transporting sanctioned goods from the EU or third countries to high-risk countries, without verifying the end-user of the goods, to companies who redirect the goods to an end-user in Russia;
3.16.2. transporting sanctioned goods from the EU or from third countries in transit through Russia, if those goods are subject to a prohibition on transit through Russia;
3.16.3. providing brokering services, technical assistance, or financial assistance in the trade of sanctioned goods from the EU or from third countries to high-risk countries, if the goods are diverted to Russia;
3.16.4. transferring, directly or indirectly, intellectual property rights or trade secrets relating to sanctioned goods to companies in Russia.

Additional risks for the exporters of sanctioned CHP items

3.17. The list of CHP items[22] includes such sanctioned goods that are necessary for Russia in the development, manufacture, and use of military goods, or which have been found in Russian weapons on the battlefield. Russian companies are trying to obtain these goods by circumventing sanctions.

3.18. A person selling, supplying, transferring, or exporting CHP items or technology has the obligation to take appropriate measures to identify and assess the risks associated with the export of CHP to or for use in Russia or Belarus and to ensure that such risk assessments are documented and kept up to date. A person shall have in place appropriate policies, controls, and procedures to mitigate and effectively manage the risks associated with the export of such goods or technology to or for use in Russia or Belarus. The person must also ensure that these requirements are implemented by legal persons owned or controlled thereby in third countries, unless this is not possible for reasons beyond the person's control.[23]

3.19. The aforementioned means that a person has the obligation to implement the ICS in order to mitigate and manage sanctions risks. According to the European Commission Explanatory Notes if a CHP item exported from the EU to a third country are then found to have reached Russia, then the EU exporter's failure to conduct adequate due diligence can be considered as a violation of EU sanctions law.[24]

3.20. Persons selling, supplying, transferring, or exporting CHP items or technology to a third country must be contractually prohibited from re-exporting the goods to Russia and Belarus and from re-exporting them for use in Russia and Belarus. In addition, the contract must prohibit third-country cooperation partners from using intellectual property rights, trade secrets, or other information protected by intellectual property rights or constituting trade secrets transferred thereto in connection with CHP items to be sold, supplied, transferred, or exported directly or indirectly to or for use in Russia.[25]

Purchase and import of sanctioned goods from high-risk countries

[22] Annexes XL and XLVIII to Council Regulation (EU) No 833/2014; Annexes XXX and XXXI to Council Regulation (EC) No 765/2006.
[23] Article 12gb of Council Regulation (EU) No 833/2014, Article 8ga of Council Regulation (EC) No 765/2006.
[24] EU Commission Explanatory Notes "Enhanced due diligence for operators manufacturing and/or trading with CHP items" Question 12, available at: https://finance.ec.europa.eu/document/download/6d765a17-b609-4282-9b99-9afef38bb545_en?filename=faqs-sanctions-russia-chp-due-diligence_en.pdf
[25] Articles 12g and 12ga of Council Regulation (EU) No 833/2014; Article 8g of Council Regulation (EC) No 765/2006

3.21. Sectoral sanctions impose a prohibition on the direct or indirect purchase, import, or transfer of a wide range of sanctioned goods, whether originating in or exported from Russia or Belarus. The prohibitions also apply to the provision of technical assistance, brokering services, financing, financial assistance, and other services related to sanctioned goods and technology, and to the provision, manufacture, maintenance, and use of such goods and technology. Hence, the prohibition to 'transfer' goods should be interpreted broadly and, according to the European Commission Explanatory Notes[26], the aforementioned restrictions should also apply in cases where the goods are not imported into the EU or do not cross the EU territory.

3.22. In transactions involving the purchase or import of goods from high-risk countries, sectoral sanctions can, *inter alia*, be violated by:
- 3.22.1. purchasing or importing EU-sanctioned goods acquired from a company in a high-risk country or exported from a high-risk country but the actual country of origin whereof is Russia or Belarus;
- 3.22.2. providing brokering services in the trade of sanctioned goods originating in Russia or Belarus or exported from Russia or Belarus to third countries;
- 3.22.3. transporting sanctioned goods originating in Russia or Belarus or exported from Russia or Belarus to the EU or third countries.

Provision of sanctioned services to high-risk countries

3.23. It is prohibited to provide, directly or indirectly, certain services and certain software to the Russian government or to any legal person established in Russia (including Russian subsidiaries owned or controlled by EU persons). This includes accounting, legal advisory, IT services, as well as business management system software and analytical software. The provision of certain aforementioned services to the Belarusian government and Belarusian public authorities, corporations, and agencies is also prohibited.[27]

3.24. In the provision of sanctioned services or software to a company from a high-risk country, sectoral sanctions can, *inter alia*, be violated or circumvented in cases where:
- 3.24.1. the service is provided directly to a parent company, subsidiary, or sister company of a Russian legal person in a high-risk country, but the Russian company also receives the service indirectly, for example, the service is provided to a group of companies that includes the Russian company;
- 3.24.2. the software is provided directly to a parent company, subsidiary, or sister company of a Russian company in a high-risk country, but the software is also used by the Russian company, for example, the business management system is used by the entire group of companies.

Measures for mitigating and managing sanctions risks

3.25. Measures for mitigating and managing sanctions risks identified during the sanctions risk assessment shall be implemented and documented in the form of procedures clearly specifying how the measures are to be taken and how decisions are to be made. Economic operators concluding transactions with sanctioned goods involving companies from high-risk countries are required to implement and apply, depending on the nature of the transaction, appropriate ICS measures, such as **enhanced due**

[26] EU Commission Explanatory Notes "Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014." Issued 22.06.2022, last updated 28.04.2025, see Section D, Subsection 5, paragraph 2, available at: https://finance.ec.europa.eu/document/download/66e8fd7d-8057-4b9b-96c2-5e54bf573cd1_en?filename=faqs-sanctions-russia-consolidated_en.pdf
[27] Article 5n of Council Regulation (EU) No 833/2014; Article 1jc of Regulation (EC) No 765/2006.

diligence of counterparties and transactions, **verification of the classification of goods and services**, **end-user verification**, and **verification of the origin of goods**.

3.26. When implementing measures for managing sanctions risks, employees with appropriate knowledge must be designated as responsible for taking specific actions and decision-making. The economic operator must ensure that the responsible persons have opportunities to regularly improve their knowledge in the field of sanctions, particularly, to attend training sessions and seminars, to obtain appropriate certifications.

3.27. Large companies exposed to high sanctions risks may establish formal sanctions committees to coordinate various departmental activities, alongside introducing an audit function. It is helpful if the person responsible for the ICS reports to the management body of the company, which in turn regularly assesses whether the sanctions risks are acceptable.

3.28. For the purpose of conducting counterparty verification, it is necessary to consider the possibility of acquiring commercial tools and databases which contain lists of legal persons identified as owned or controlled by, or otherwise linked to, sanctioned persons. Depending on the number of transactions, consideration should be given to automating the verification of counterparties against these lists.

Defining 'red lines'

3.29. When implementing measures for managing sanctions risks, it is advisable to define 'red lines' or transactions (or circumstances) which pose such a high risk to the economic operator of being involved in a sanctions violation that the economic operator cannot manage, and in which the economic operator therefore does not engage. When defining 'red lines', the economic operator is additionally advised to consult the credit institution, given that the credit institution may refuse to execute payments related to the transaction if the transaction violates or has violated the 'red lines' defined by the credit institution.

Table 3: Examples of 'red lines'

Examples of 'red lines' in transactions involving companies from high-risk countries
▪ The economic operator refrains from transactions involving such companies whose ownership structure includes sanctioned natural or legal persons. ▪ The economic operator refrains from transactions involving companies that refuse to provide information on their ownership structure or officials. ▪ The economic operator refrains from export transactions involving companies that refuse to provide information on the end-user or end-use of the goods. ▪ The economic operator refrains from transactions involving companies related to the Russian military sector. ▪ The economic operator is only engaged in export transactions with sanctioned goods if it arranges the transportation of the sanctioned goods to the end-user itself. ▪ The economic operator refrains from exporting certain sanctioned goods to a high-risk country which, according to the information available to the economic operator, have no market in the country of destination. ▪ The economic operator refrains from export or import transactions with sanctioned goods involving companies in third countries whose ownership

structure includes a legal person established in Russia that is engaged in the same economic activity as the company in third country.
- The economic operator refrains from export transactions with sanctioned goods involving companies that are wholesalers and are engaged in the trade of goods to Russia as part of their business activities.
- The economic operator refrains from import transactions with sanctioned goods involving companies that refuse to provide information and documents substantiating the origin of the goods.

Measures for mitigating and managing the risks of targeted financial sanctions

3.30. When implementing measures for managing the risks of targeted financial sanctions, the procedures must define which particular counterparties (and other parties involved in the transactions) are subject to the application of enhanced due diligence measures. Economic operators engaging in transactions with companies from high-risk countries, Russia, or Belarus **are required to conduct enhanced due diligence on both direct counterparties and companies from high-risk countries, Russia, or Belarus engaged in transactions indirectly, including consignors, consignees, storage providers, end-users or manufacturers, end recipients of services, payers or payment recipients.** The results of such enhanced due diligence measures must be documented and retained.

Enhanced due diligence of counterparties

3.31. The enhanced due diligence measures for counterparties include obtaining and assessing information on the ownership structure of the company and the officials or other persons who own or control the company to ensure that the company is not a sanctioned person, specifically, it is not included in the targeted financial sanctions lists and is not directly or indirectly owned or controlled by persons included in the targeted financial sanctions lists.

3.32. It is considered good practice to obtain information by requesting the counterparty to complete the so-called "Know Your Customer" or "Know Your Supplier" forms (questionnaires) which typically require the counterparty to provide registration details, information on its ownership structure, beneficial owners and officials, as well as other relevant data, for example, its business activities, main cooperation partners, including end-users or manufacturers of the goods. If the accuracy of the submitted information cannot be verified in reliable public information sources (such as public registers), the counterparty must also be requested to provide its registration documents and, where necessary, other relevant documentation required for verification, for example, annual financial statements.

3.33. The information provided in the completed forms and documents submitted must be compared with, *inter alia*, information available in public registers and also other publicly available sources, such as the website of the counterparty or press articles, to ensure that the information provided in the completed forms is accurate and that the counterparty is not otherwise associated with sanctioned persons. In case of lack of information or uncertainties, the counterparty must be requested to provide additional information or clarifications.

3.34. Counterparties, their owners, legal and natural persons involved in the chain of ownership structure, officials and other associated persons shall be verified against

targeted financial sanctions lists using publicly available[28] or commercial screening tools.

3.35. Economic operators exposed to high sanctions risks may use commercial databases that allow verification of counterparties in targeted financial sanctions lists (screening) against various international and national sanctions lists, as well as lists that identify legal persons owned or controlled by sanctioned persons and persons otherwise associated with sanctioned persons. Depending on the sanctions risks of the economic operator, as well as the number of counterparties and transactions, consideration should be given to automating counterparty verification process and performing it on a regular basis, for example, once a day or before each transaction, including the possibility to block a transaction in the event of a match during verification. Selection of particular tools is at the discretion of the economic operator, based on the sanctions risk assessment and the identified sanctions risks.

3.36. The information obtained about the counterparty and the transaction during the verification process is compiled and assessed to determine whether the potential transaction displays any characteristics described under the **risk indicators of targeted financial sanctions**, suggesting an increased risk of targeted financial sanctions violations. The identification of risk indicators does not in itself imply that the cooperation with the counterparty will result in a violation of targeted financial sanctions. If the sanctions risk characteristics described under the risk indicators of targeted financial sanctions are identified, it must be assessed whether the available information provides sufficient and reasonable assurance that sanctions will not be violated. Following the verification process, a decision is made whether to establish a business relationship with the counterparty.

3.37. Enhanced due diligence of counterparties is conducted prior to the commencement of the business relationship and is repeated periodically, for example, following changes in the sanctions framework, changes in the contractual relationship and circumstances of the transaction (delivery terms, final recipient, type of goods or services, etc.), or changes in information on the counterparty. **All information gathered during the due diligence, the results of the verification, and the decisions made must be documented and retained.** Even a negative circumstance (for example, absence of a person from the sanctions lists) must be documented.

Table 4: Risk indicators of targeted financial sanctions

Risk indicators of targeted financial sanctions
Risk indicators related to ownership structure ▪ The counterparty has a legally and economically unjustifiably complex ownership structure; trusts, shell companies are used in the ownership structure. ▪ In the ownership structure, the shareholder is a sanctioned person, a relative of the sanctioned person, or a person closely linked to the sanctioned person (business partner, long-term employee) about whom public information is available. ▪ Public registers do not provide information on the ownership of the counterparty, for example, the company is a private limited company and the counterparty does not provide supporting documents such as extracts from registers.

[28] See section "Useful information sources and tools" under Chapter 4 "Closing Provisions".

- Following the entry into force of the sanctions against Russia, the ownership of the transaction partners has changed.
- There is a sanctioned person in the board or council of the counterparty.
- The current or historical owners, beneficial owners, officials, or contact persons of the counterparty are or have been related to sanctioned persons.
- The counterparty is identified in the grounds for including the sanctioned person on the EU targeted financial sanctions lists.
- The counterparty is included in sanctions of other countries and the grounds for inclusion indicate that it is related to a sanctioned person.

Risk indicators related to operations of the company

- The counterparty was established, became active, or changed the type of business after 24 February 2022.
- The counterparty is located in a country where there is not a large Russian-speaking minority, but the contact persons or officials of the counterparty are Russian citizens or residents, communicate in Russian, use email addresses registered in Russian (public) domains.
- The counterparty or its owners have no or minimal presence on the internet.
- The officials of the counterparty are never available, communication takes place only with an employee or an authorised person.
- The website of the counterparty has been created only recently, is of poor quality, or is registered in Russian or Belarusian domain registries.
- Information available on the website of the counterparty or elsewhere indicates that it is cooperating with sanctioned persons or with Russia in general.
- The address of the counterparty matches that of a person on the EU targeted financial sanctions lists.
- Several companies are registered at the address of the counterparty, or it serves as a company formation service provider.
- The address of the counterparty is not intended for the specific type of business, for example, it is a multi-apartment building.
- The counterparty uses a contact telephone number registered in Russia.
- The contact telephone number or email address provided by the counterparty is used by persons associated with or cooperating with sanctioned persons.
- The counterparty acts as an intermediary or agent and does not provide information about cooperation partners.

Measures for mitigating and managing sectoral sanctions risks

3.38. When implementing measures for managing sectoral sanctions risks, the procedures must define the types of transactions for which specific measures to manage sanctions risks are to be taken. Economic operators conducting transactions with companies from high-risk countries must verify the classification of goods and services involved in the transaction. If the goods or services involved in the transaction are subject to sanctions, the transaction is considered to be a transaction with a heightened sanctions risk and should be subject to enhanced due diligence measures.

Verification of the classification of goods and services

3.39. In order to determine whether goods purchased, imported, manufactured, traded, exported, or transported by an economic operator in transactions involving companies from high-risk countries are not sanctioned goods, verification of the classification of goods must be included in the procedures. Information on the classification of goods can initially be obtained from the counterparty from which the goods were purchased. The information obtained on the classification of goods should be independently verified to ensure that the classification is accurate. This includes checking whether

identical or similar goods have been classified differently in the past. The classification of own-manufactured goods must be carried out independently. In order to ascertain that the goods are not subject to sanctions, it is necessary, *inter alia*, to carry out the classification verifications provided in Table 5.

Table 5: Verification of the classification of goods

Type of transactions	Verification of the classification of goods
Transactions involving the import and export of goods	Verification of the CN classification of the goods and verification that the CN code of the goods is not included in any of the Annexes to Regulation No 833/2014 or Regulation No 765/2006
Transactions related to the export of goods	Verification that the goods are not listed in one of the Annexes to Regulation No 2021/821 (not considered dual-use items)
Transactions related to the export of goods	Verification that the goods are not listed in Annex VII to Regulation No 833/2014 or Annex Va to Regulation No 765/2006

3.40. The Integrated Tariff Management System (ITMS) of the SRS may also be used to check the CN classification of goods.[29] If, during the verification of the classification of goods, doubts arise as to the correct CN classification of the goods, it is possible to consult the National Customs Board of the SRS, for example, by requesting "binding tariff information".[30]

3.41. If in doubt as to whether goods are dual-use items or items listed in Annex VII to Regulation No 833/2014 or Annex Va to Regulation No 765/2006, it is possible to consult with the Strategic Goods Export Control Division of the Ministry of Foreign Affairs.[31]

3.42. If it is established that the goods are subject to sanctions, it must be determined which sectoral sanctions prohibitions apply to the particular goods and related transactions, such as prohibition on import or export, prohibition on providing technical assistance, financing, or financial assistance related to the goods. It is important to understand which transactions would be prohibited if the counterparty was a Russian or Belarusian person or the country of origin or destination of the goods was Russia or Belarus. For the scope of the prohibitions applicable to the goods, it is possible to consult the FIU.[32]

3.43. If a transaction with a company from a high-risk country involves sanctioned goods, **enhanced due diligence for the transactions** must be carried out to obtain a sufficient level of assurance that, in export transactions, the sanctioned goods will not be diverted to Russia or Belarus, and in import transactions, that the country of origin or export is not Russia or Belarus.

3.44. When providing services to companies from high-risk countries, it is necessary to ascertain that the provided service is not subject to sanctions. Particular attention should be paid to whether the service is a service listed under Article 5n of Regulation

[29] Available at: https://www.vid.gov.lv/lv/integreta-tarifa-vadibas-sistema-taric
[30] For more information see: https://www.vid.gov.lv/lv/saistosa-izzina-par-tarifu
[31] Contact details are available at: https://www.mfa.gov.lv/lv/filiale/strategiskas-nozimes-precu-eksporta-kontroles-nodala
[32] Contact details are available at: https://sankcijas.fid.gov.lv/en/kontakti

No 833/2014 as prohibited to be provided directly or indirectly to the Russian government, natural and legal persons established in Russia.[33]

3.45. When providing software to companies in high-risk countries, it is necessary to verify whether the software falls within the scope of sanctions under Article 5n and Annex XXXIX to Regulation No 833/2014, which prohibit its direct or indirect provision to the Russian Government and legal persons established in Russia.[34]

3.46. If, in the course of a transaction with a company from a high-risk country, a service or software subject to sanctions is provided, enhanced due diligence of transactions must be conducted to obtain sufficient assurance that the service is not indirectly provided or the software is not indirectly made available to the Russian legal person, or the Russian government.

Enhanced due diligence of transactions

3.47. Enhanced due diligence of a transaction must be conducted in cases where the transaction with companies from high-risk countries involves sanctioned goods or services. The transaction documents and information relating to the transaction, including transport documents, customs declarations, information on the route and modes of transport, must be obtained as part of enhanced due diligence of a transaction. Transactions related to the import of goods are subject to the **verification of the reliability of origin of the goods** by obtaining and verifying information and documents supporting the origin of the goods. Transactions related to the export of goods are subject to **end-user verification** by obtaining and verifying information on the end-user and end-use of the goods. The information obtained is compiled and assessed to determine whether the potential transaction displays any characteristics described under the **risk indicators of sectoral sanctions**, suggesting an increased risk of sectoral sanctions violations.

Verification of the reliability of the origin of goods

3.48. In order to determine whether sanctioned goods purchased, imported, transferred, or transported from a high-risk country as part of a transaction are of Russian or Belarusian origin or exported from Russia or Belarus and are not subject to the prohibitions of sectoral sanctions, verification of the reliability of the origin of the goods must be established and conducted as part of the procedures.

3.49. The counterparty must be requested to provide a certificate of origin for the goods and other documents, such as manufacturer's certificates, quality certificates and declarations that substantiate the origin of the goods. The information obtained should be compared with information available in public sources to ascertain that the information is accurate, including by checking whether the named manufacturer produces goods of the indicated type and quality and whether there is any publicly available information on sanctions circumvention in relation to the particular goods. In addition, it is necessary to ascertain that the goods are not being exported from Russia or Belarus, for example, by requesting the counterparty to submit an export declaration.

[33] Pursuant to Article 1jc of Regulation (EC) No 765/2006, the provision of certain aforementioned services to the Belarusian government and Belarusian public authorities, corporations, and agencies is also prohibited.
[34] Pursuant to Article 1jc of Regulation (EC) No 765/2006, the provision of certain software to the Belarusian government and Belarusian public authorities, corporations, and agencies is also prohibited.

End-user verification

3.50. In order to ensure that sanctioned goods sold, supplied, transferred, or exported to a high-risk country as part of a transaction will not be diverted to an end-user or for end-use in Russia or Belarus in violation of the prohibitions of the sectoral sanctions, the procedures must include and ensure the implementation of end-user and end-use verification process.

3.51. The counterparty should be required to provide documents and information identifying the end-user of the goods and the country of end-use of the goods. This may include requiring statements signed by the end-user of the goods, stating, *inter alia*, the end-use of the goods or the purpose for which they were purchased.

3.52. The information obtained should be compared with information available in public sources to ascertain that the information is accurate, including by checking whether the named end-user of the goods (or related legal persons) is trading identical or similar goods in Russia or Belarus. If the end-user indicates that the goods will be used as components for the manufacture of other goods, it is necessary to check public information in order to verify whether the end-user manufactures goods of such type that require the exported components and also whether legal persons related to the end-user (for example, group companies) in Russia or Belarus manufacture goods that use the exported components.

Identification of sanctions violation "red flags" described under the risk indicators of sectoral sanctions

3.53. The information on the transaction obtained during enhanced due diligence of transactions, including information on the origin of the goods (for import transactions) and on the end-user of the goods (for export transactions), as well as the information obtained during enhanced due diligence of counterparties, shall be assessed to determine whether the transaction presents any "red flags" for sanctions violations described in the sectoral sanctions risk indicators. The identification of risk indicators does not in itself imply that involvement in the transaction will result in a violation of sectoral sanctions. f red flags for sanctions circumvention are identified, it is necessary to assess whether the available information provides reasonable assurance that sanctions will not be violated. Where necessary, the counterparty is requested to provide additional information or clarifications.

Table 6: Risk indicators of sectoral sanctions

Risk indicators of sectoral sanctions in transactions with sanctioned goods
<u>Risk indicators related to the classification of goods</u> ▪ A counterparty requests not to indicate the CN code in the transport documents and invoices, or requests to indicate a different CN code or an inappropriate description of the goods. ▪ The counterparty does not provide information to support the classification of the goods it manufactures or trades. <u>Risk indicators related to the origin of goods</u> ▪ Goods of the particular type and quality are not obtained or manufactured in the country of origin of the goods. ▪ The counterparty avoids providing information on the manufacturer of the goods. ▪ The counterparty avoids providing documents supporting the origin. ▪ The counterparty was established, became active, or changed the type of business after the entry into force of the sectoral sanctions.

- The exporter repackages goods purchased from the manufacturer.

Risk indicators related to the end-use of goods

- The counterparty avoids providing information on the end-user of the goods.
- The counterparty required to carry out the import (release for free circulation) of the sanctioned goods is not registered in the relevant national registers (for example, value added tax register) in the recipient country or has not obtained the necessary authorisations to import the goods.
- The counterparty or its affiliated companies are or have been engaged in the business of selling or providing sanctioned goods or services in Russia or Belarus (for example, through an online shop or by offering goods or services via a website).
- The counterparty is newly established or has not been in business for a long time.
- The counterparty wishes to conclude the transaction on prepayment basis and is ready to purchase the goods at a disproportionately high price or in large quantities.
- The counterparty undertakes to transport the goods itself and avoids providing information on the place of delivery, or the information provided on the place of delivery does not match the information requested to be indicated in the transport documents.
- The counterparty makes last-minute changes to the place of delivery in the transport documents and instructions.
- The counterparty avoids providing an import declaration of the goods.
- The transaction involves an intermediary that uses letters of credit (back-to-back letters of credit) to guarantee payments.
- The contact person of the counterparty lacks knowledge about the goods.
- The counterparty is included in sanctions of other countries and the grounds for inclusion indicate that the counterparty is engaged in activities related to sanctions circumvention.
- The counterparty supplied goods to Russia before the entry into force of the sectoral sanctions.
- It is not possible to accept the goods at the delivery address of the goods.
- The end-user of the goods does not have the technical capacity, knowledge, or ability to use the goods.
- The end-user of the goods is the provider of logistics, transport, or forwarding services.
- The end-user of the goods is a natural person, but purchases goods in large quantities or goods not intended for household use (for example, industrial goods).
- The place of delivery of the goods in the country of destination is a free trade zone, warehouse, port, or airport.
- The place of delivery of the goods in the country of destination is at a location where land, sea, or air transport routes to Russia or Belarus are available, for example, by ship.
- The place of delivery of the goods is close to the Russian or Belarusian border.
- The route for transporting the goods is unclear or economically unreasonable.
- There is no market for the goods in the country of destination.

3.54. Enhanced due diligence measures are implemented both prior to the transaction and, where necessary, after completion of the transaction, by obtaining documents confirming the delivery of the goods, such as an import declaration in the country of end-use of the goods. **All information gathered during the due diligence, the results of the verification, and the decisions made must be documented and retained.**

Review and update of the ICS measures

3.55. The ICS needs to be reviewed and updated periodically (preferably not less than every three years), including by conducting a repeated sanctions risk assessment, to ensure timely identification of new sanctions risks that may arise over a longer period of time as a result of changes in external or internal circumstances or processes.

3.56. If significant changes in sanctions legislation or the company's business activities could cause existing sanctions risks to increase significantly or new risks to emerge, an *ad hoc* sanctions risk assessment must be conducted and ICS reviewed.

4. CLOSING PROVISIONS

Preconditions for effective cooperation with credit institutions

4.1. It is important for credit institutions to make sure that the economic operator is fully aware of its sanctions risks and can explain what measures are being taken to manage these risks. The economic operator must be able to demonstrate to the credit institution that the ICS developed is not a formal or standardised document but is appropriate to the risk profile of the economic operator.

4.2. For better understanding of the approach of the economic operator to sanctions risks, the credit institution may request an interview with the responsible persons of the company. Credit institutions expect that the persons responsible for managing sanctions risks are competent in the field of sanctions and are familiar with the business specifics of the company (for example, the details of customs and logistics processes).

4.3. It is important for credit institutions to obtain assurance that the economic operator has:
- 4.3.1. defined and implemented clear measures to manage sanctions risks;
- 4.3.2. identified specific persons responsible for managing sanctions risks and their responsibilities;
- 4.3.3. clearly defined processes, criteria, and sources of information for the verification of counterparties and transactions;
- 4.3.4. clearly defined "red lines", i.e. certain transactions and circumstances in which the economic operator should not engage in the transaction;
- 4.3.5. put in place processes to keep up to date with developments in the field of sanctions, including what steps to take when new sanctions are introduced.

4.4. Credit institutions expect that when verifying counterparties and transactions, the economic operator does not rely solely on formal confirmations from counterparties or client questionnaires. A "wilful blindness" approach is not acceptable.

4.5. The economic operator must be able to demonstrate to the credit institution that it has a clear procedure in place for the verification of counterparties and transactions, which includes targeted actions to obtain, using defined information sources and tools, certain information necessary to check the transaction. For example, the procedure provides that, as part of the end-user verification, street view photos of the end user's address are examined in certain defined online sources.

4.6. Credit institutions expect economic operators to have clearly defined "red lines". For example, if the minimum amount of counterparty information specified in the procedure cannot be obtained, the economic operator refrains from the transaction.

4.7. If the credit institution assesses the quality of counterparty and transaction due diligence documentation as high and obtains assurance that the economic operator itself properly understands and manages the sanctions risks inherent in its business activity, it may adjust its measures accordingly. For example, to carry out random checks instead of implementing enhanced due diligence measures for each transaction, thus ensuring faster execution of the transaction.

4.8. The ability of the economic operator to quickly submit transaction documents to the credit institution will also speed up the settlement process. For example, when a certain transaction requires the authorisation of the competent authority, the economic operator must obtain it in a timely manner and submit it to the credit institution before the transaction takes place.

4.9. Credit institutions can also be bound by and comply with sanctions of the United States (US), the United Kingdom, and other countries. The credit institution may therefore also require its client to comply with the respective sanctions of other countries. The client should be aware that transactions with the goods of US origin or containing components or inputs of US origin may be subject to US export and re-export restrictions on goods and technology for which the client may be liable under US law.[35]

4.10. The economic operator whose business activities involve, in whole or in part, trade in CHP items, military, or dual-use items should note that the availability of settlements may depend directly on whether the economic operator has carried out a sanctions risk assessment and established an effective ICS. However, even in this case, it should be considered that settlements for the supply of such goods may not be authorised if, in the opinion of the credit institution, they would create high and unmanageable sanctions risks.

4.11. Credit institutions assess the payment traceability of economic operators. The use of different, unduly complex settlement arrangements may give rise to suspicions of sanctions circumvention. In such cases, credit institutions may refuse the transaction or terminate the business relationship with the economic operator.

4.12. Finally, the economic operator should be aware that credit institutions have different business models. Credit institutions whose business model does not involve transactions with high-risk countries may be reluctant to service transactions and economic operators with a high risk of sanctions. Credit institutions specialising in servicing transactions with high-risk countries may also impose restrictions and specific requirements on certain payments. A high risk of sanctions also means a risk price that the credit institution may add to the service fee. Economic operators must therefore assess which credit institution best suits their business profile. Information on the types of clients and transactions serviced by credit institutions is available on their websites or by contacting them.

[35] Export Administration Regulation or the EAR of the Bureau of Industry and Security of the US Department of Commerce, available at: https://www.bis.gov/regulations/ear

Useful information sources and tools

4.13. Search on sanctions lists:[36]

Tool	Sanctions lists
FID Sanctions Search Tool	Targeted financial sanctions lists binding on the Republic of Latvia, comprising the United Nations (UN), the EU, and Latvian national sanctions lists.
EU Sanctions Map	EU targeted financial sanctions lists and information on EU sanctions regimes
Open Sanctions	Sanctions lists of various countries, including UN and EU lists
OFSI Sanctions Search Tool	Targeted financial sanctions list of the United Kingdom
OFAC Sanctions Search Tool	Sanctions List of the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury
US Consolidated Screening List	Consolidated list of persons subject to US export and re-export restrictions

4.14. Other tools:

Tool	Description
ITMS	Integrated Tariff Management System of the SRS
War Sanctions	Information on sponsors and supporters of Russian aggression and on foreign goods used by Russia in weapons manufacturing
Trade Integrity Project	List of third-country companies that have supplied CHP items to Russia since 2023

4.15. Websites:

Link	Description
FIU sanctions website	FIU sanctions website
National Customs Board of the SRS	Sanctions section on the website of the National Customs Board of the SRS
European Commission	Sanctions section on the website of the European Commission
EU Sanctions Helpdesk	The EU Sanctions Helpdesk provides assistance to small and medium-sized enterprises on sanctions implementation, including the possibility to inquire about sanctions implementation[37]

4.16. Guidelines and explanations:

Author	Name
FIU	"Indicators of Sectoral and Targeted Financial Sanction Evasion"
	Latvian National ML/TF/PF Risk Assessment Reports
	"Assessment of Control by Sanctioned Public Officials (2026)"
European Commission	"Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention"
	"Enhanced due diligence for operators manufacturing and/or trading with CHP items"
	"Commission consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014"

[36] The Republic of Latvia is directly bound by the United Nations (UN) sanctions, the EU sanctions, and the national sanctions of the Republic of Latvia.
[37] More information available here: https://sankcijas.fid.gov.lv/en/aktualitates-apskate/izveidots-es-sankciju-palidzibas-dienests-mazo-un-videjo-uznemumu-atbalstam.

Council of the EU	"Restrictive measures (Sanctions) – Update of the EU Best Practices for the effective implementation of restrictive measures"
EU and G7	"Preventing Russian export control and sanctions evasion – Updated guidance for industry"
OTSI[38]	"Countering Russian sanctions evasion – guidance for exporters"

4.17. EU Sanctions Whistleblower Tool:

Name	Description
EU Sanctions Whistleblower Tool	The EU Sanctions Whistleblower Tool allows anonymous reporting of sanctions violations to the European Commission

[38] Office of Trade Sanctions Implementation – UK competent authority for trade sanctions implementation