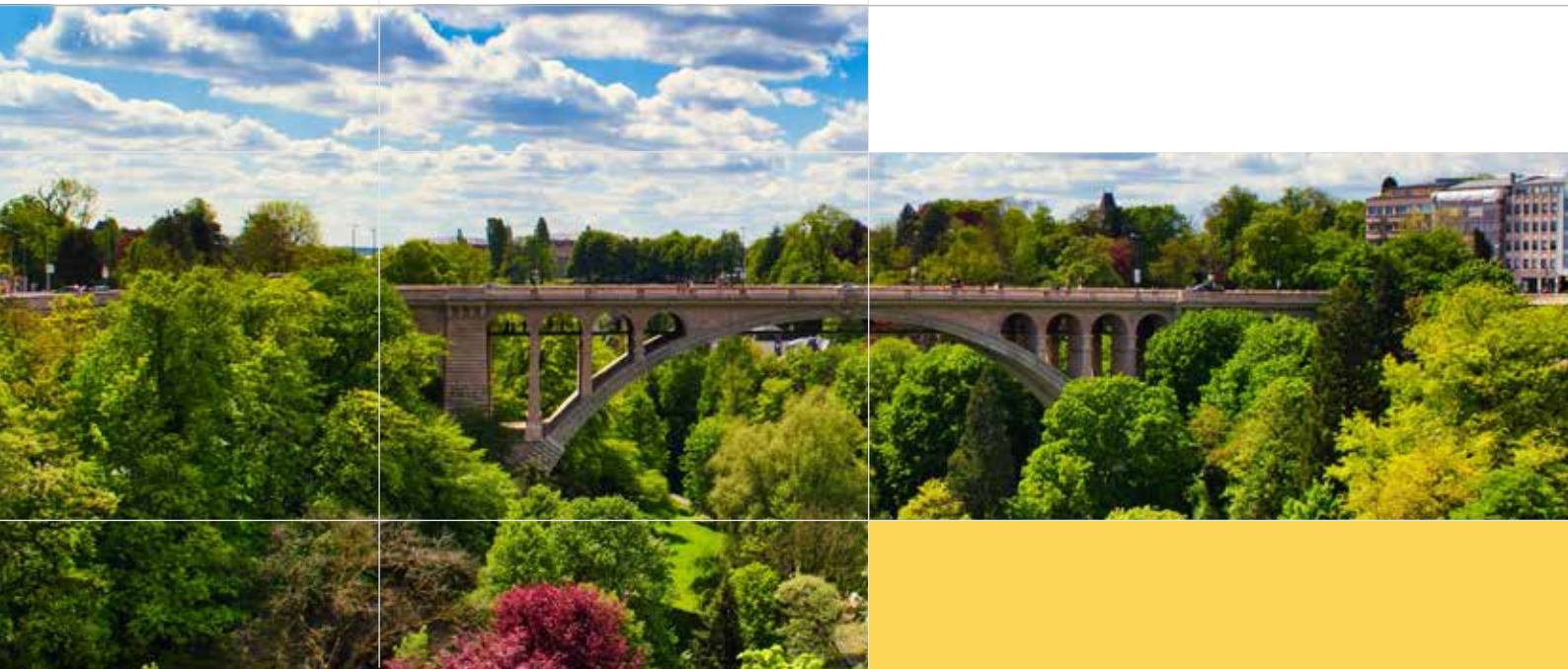
Amidst a complex landscape, banks play a pivotal role in ensuring adherence to export control regulations. Their obligations extend beyond mere financial transactions; they are entrusted with the responsibility to scrutinize and mitigate the risks associated with international trade.

Export Control Compliance: The Imperative for Banks and Financial Services Providers



RespectUs

About RespectUs

Founded in 2019, RespectUs has emerged as a frontrunner in providing cutting-edge export control solutions. Our one-stop-shop online platform, validated by the European Space Agency (ESA), offers an intuitive, up-to-date experience in multiple languages.

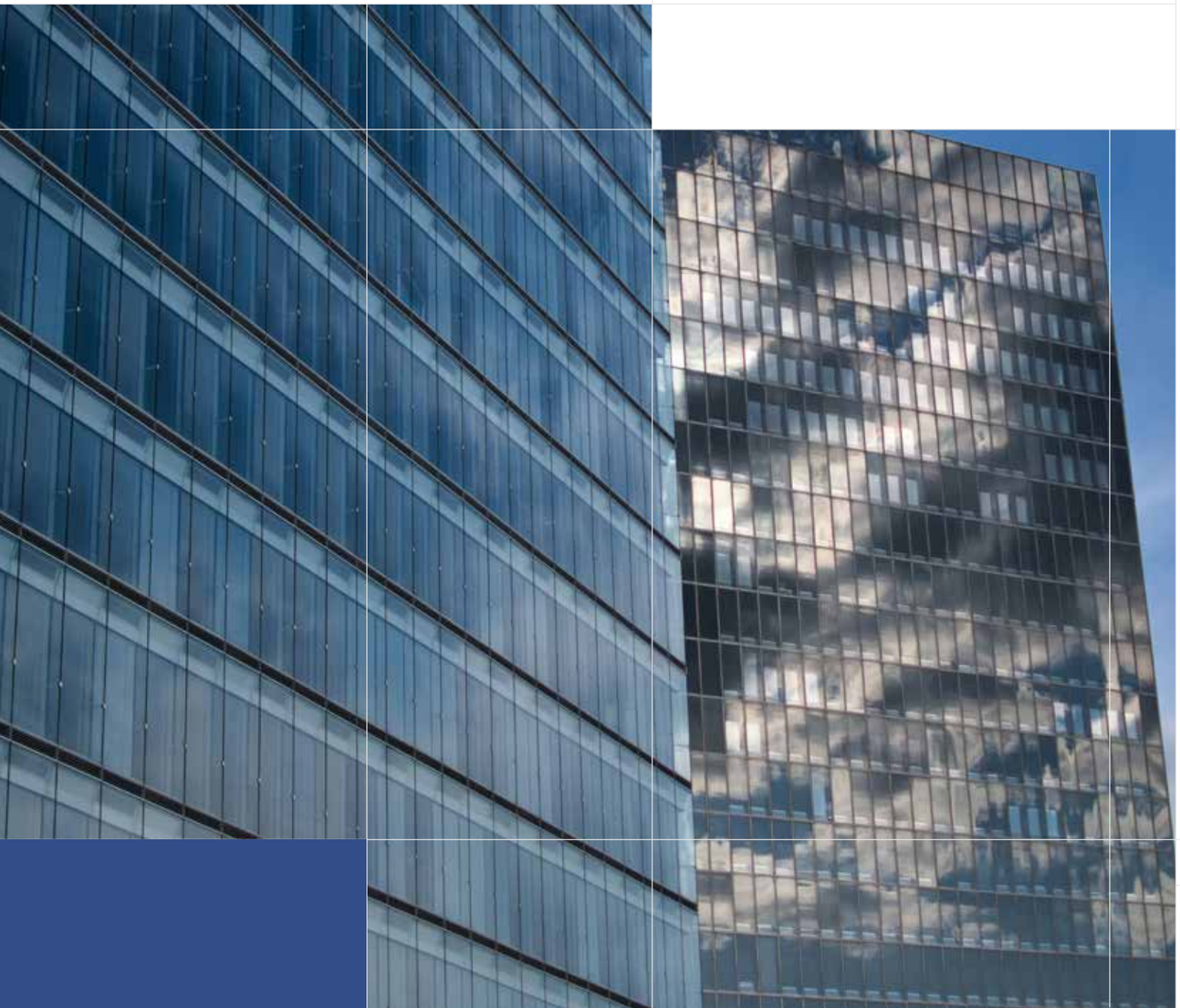
At RespectUs, we recognize the intricate challenges businesses face in the dynamic world of global trade regulations. Our mission is to simplify complexities and streamline compliance processes for exporters of sensitive, export-controlled goods, their suppliers, and banks seeking guidance in product classification, risk assessment, and sanctions and embargoes.

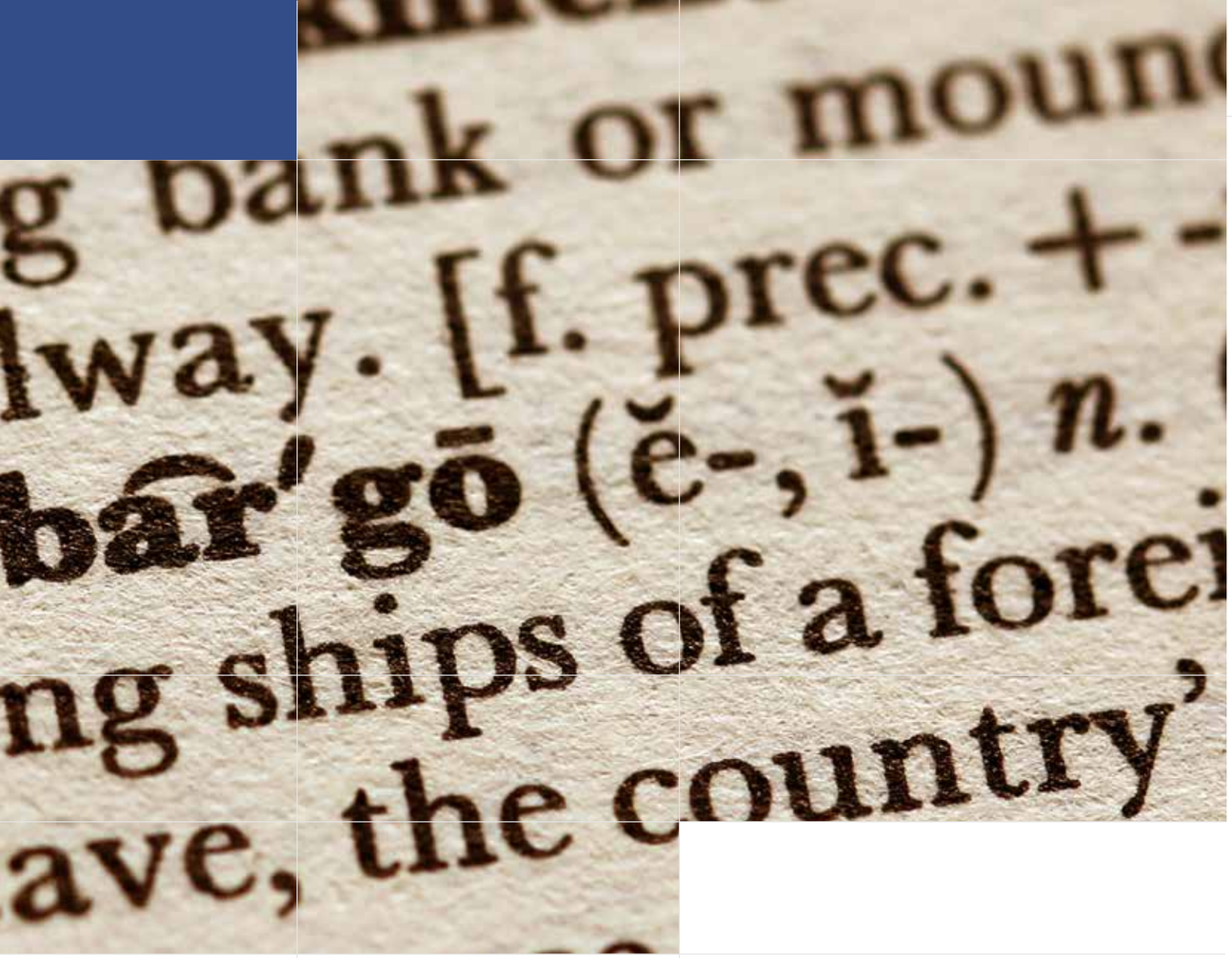
RespectUs ensures businesses stay ahead of regulatory changes, seamlessly adapting to evolving trade landscapes. Our commitment to excellence drives us to continually refine and expand our services, positioning us as a trusted innovator in export control compliance.

MADE IN LUXEMBOURG

What You'll Read About

Content





Chapter One

Introduction To Export Control Compliance

In a globalized world, where trade transcends borders effortlessly, export control compliance stands as a critical safeguard against the proliferation of sensitive technologies and materials to unauthorized entities.

Export control refers to the set of regulations and procedures implemented by governments to manage and monitor the export of goods, services, and technologies with the aim of protecting national security, preventing the proliferation of weapons of mass destruction, and ensuring adherence to international agreements. These regulations encompass various aspects, including the classification of controlled items, the screening of parties involved in transactions, and the reporting of suspicious activities.

Financial institutions have long asked how —and to what extent — they need to comply with export controls.

The reply to that question is now definitely clear. After its invasion of Ukraine, Russia is obliged to get the industrial goods required to prosecute its war and to build weapons of war. To source those materials, they must use the financial system, which makes it a potential chokepoint. Financial institutions are thus responsible for ensuring that they are not becoming the facilitators of the transfer of the inputs that Russia needs, and must take actions.[1]

Funds, the primary asset of financial institutions, were until recently not subject to general trade restrictions. In the banking sector, for that reason, few trade control risk assessments seem to have been conducted, perhaps because of an underestimation of the risks

1 The White House, Background Press Call on Upcoming Action to Continue Holding Russia Accountable. 21 December 2023, https://www.whitehouse.gov/briefing-room/press-briefings/2023/12/22/background-press-call-on-upcoming-action-to-continue-holding-russia-accountable/

connected to the increasing complexity and interconnections between trade controls and economic sanctions. On the other hand, banks serve as the linchpin of international trade transactions, as they facilitate the movement of funds across borders. Consequently, they become instrumental in ensuring compliance with export control regulations. Banks and financial institutions must therefore conduct due diligence on their customers and transactions to mitigate the risk of inadvertently aiding illicit activities such as the proliferation of controlled items to sanctioned entities or countries.

These reinforced requirements have been dealt with in the United States, where the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) have issued since June 2022 three specific alerts.[2] On 22 December 2023, the Biden Administration took also further action to add significantly to its Russia-related sanctions by issuing a new Executive Order ("EO") 14114 that, among other things, now subjects foreign financial institutions[3] to secondary sanctions risks when they conduct or facilitate certain Russia-related transactions, even unwittingly.

2 See FinCEN & BIS Joint Alert, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts, 28 June 2022, https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; FinCEN & BIS Joint Alert, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts, 19 May 2023, https://www.bis.doc.gov/index.php/documents/enforcement/3272-fincen-and-bis-joint-alert-final-508c/file; FinCEN & BIS Joint Alert, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Announce New Reporting Key Term and Highlight Red Flags Relating to Global Evasion of U.S. Export Controls, 6 November 2023, https://www.fincen.gov/sites/default/files/shared/FinCEN_Joint_Notice_US_Export_Controls_FINAL508.pdf.

3 A term defined broadly to include "any foreign entity that is engaged in the business of accepting deposits; making, granting, transferring, holding, or brokering loans or credits; purchasing or selling foreign exchange, securities, futures or options; or procuring purchasers and sellers thereof, as principal or agent. It includes depository institutions; banks; savings banks; money services businesses; operators of credit card systems; trust companies; insurance companies; securities brokers and dealers; futures and options brokers and dealers; forward contract and foreign exchange merchants; securities and commodities exchanges; clearing corporations; investment companies; employee benefit plans; dealers in precious metals, stones, or jewels; and holding companies, affiliates, or subsidiaries of any of the foregoing." EO 14024 11(f), as amended by EO 14114.

INTRODUCTION TO EXPORT CONTROL COMPLIANCE

The European Union (EU) has as well chosen to close legal loopholes and improve effective implementation and enforcement of sanctions against Russia and Belarus, which have been strengthened after Russia's illegal full-scale invasion of Ukraine in February 2022. Violation of EU restrictive measures will in the future be subject to harmonized criminal offences and penalties, and the new rules will refer, for example, to failing to freeze assets, breaching arms embargoes and providing prohibited or restricted financial services.[4] The EU Commission has also issued a guidance to support EU operators' compliance efforts.[5]

The guidance issued by U.S. and EU authorities is far strengthening export controls and preventing evasion by

1. providing financial institutions with lists of products of concern and red-flag indicators for export control evasion,
2. obliging financial institutions to apply a risk-based approach to trade finance.

4 See: "Commission welcomes political agreement on new rules criminalizing the violation of EU sanctions", Press release, 12 December 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6535

5 European Commission, Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention, December 2023, https://finance.ec.europa.eu/system/files/2023-12/guidance-eu-operators-russia-sanctions-circumvention_en.pdf

Chapter Two

Actions In Response To The Russian Invasion Of Ukraine

Since February 2022, a coordinated international endeavor under the Global Export Control Coalition (GECC) [6] , an international coalition of 39 nations from North America, Europe, and the Indo-Pacific region, has applied economic pressure on Russia and Belarus. These stringent export controls primarily target Russia's defense, aerospace, and maritime sectors, with the purpose to degrade the military capabilities that Russia uses to wage its war, and to restrict Russia's access to items that can support the country's defense industrial base and military and intelligence services.[7]

The sanctions also include other targets such as Russia's energy production sector as well as luxury goods used by Russian elites. This increases as well the costs on Russian and Belarusian persons who support the government of Russia and its invasion of Ukraine.[8] The restrictions applied to Belarus are in response to its substantial enabling of Russia's war effort.[9]

These recent actions build on export restrictions that were previously established following Russia's occupation of Crimea in 2014, and in response to other malign Russian activities. Some of these prior restrictions remain in effect, while others have been expanded in scope through recent regulatory actions. These actions have imposed controls on a range of items that had not previously required export licenses when destined for Russia or Belarus.

6 The GECC includes Iceland, Liechtenstein, Norway, Switzerland, Australia, Canada, the 27 Member States of the European Union (EU), Japan, South Korea, Taiwan, New Zealand, the United States, and the United Kingdom (UK). These countries are also listed in supplement 3 to part 746 of the Export Administration Regulations (EAR) and have committed to implementing substantially similar export controls on Russia and Belarus.

7 See White House, "Executive Order on Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression," (11 March 2022)

8 The GECC includes Iceland, Liechtenstein, Norway, Switzerland, Australia, Canada, the 27 Member States of the European Union (EU), Japan, South Korea, Taiwan, New Zealand, the United States, and the United Kingdom (UK). These countries are also listed in supplement 3 to part 746 of the Export Administration Regulations (EAR) and have committed to implementing substantially similar export controls on Russia and Belarus.

9 See BIS Press Release, "Commerce Imposes Sweeping Export Restrictions on Belarus for Enabling Russia's Further Invasion of Ukraine," (2 March 2022)

In the last months, additional export control restrictions were imposed to further cut off Russia's defense industrial base and military from critical items it seeks to obtain to sustain Russia's ongoing, unprovoked war against Ukraine. Specifically, these restrictions aim to cut off Russia's access to critical components used for aircraft and tanks, semiconductors, other items needed for advanced military applications, and low technology consumer goods needed for Russia to sustain its war effort.[10]

These additional restrictions also target third countries such as Iran and China, that have served as supply nodes to the Russian war machine. Measures are targeting third countries and impeding Russia's ability globally to obtain commercially available items, such as semiconductors that are components for Iranian Unmanned Aerial Vehicles (UAVs) used by Russia in Ukraine.

United States

On 24 February 2022, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) amended the Export Administration Regulations (EAR) to apply strengthened export control rules to Russia and Belarus including extended scope of the Foreign Direct Product (FDP) Rules. The EAR applies extraterritorially to items subject to the EAR and „follows the goods" anywhere in the world. The EAR regulates exports, re-exports, and in-country transfers of covered items globally, even if a transaction does not involve U.S. entities and takes place outside the U.S. Items subject to the EAR can include:

- items anywhere in the world produced or manufactured in the U.S.;

10 See BIS Press Release, "Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine" (24 February 2023)

- items in or exported from the U.S., regardless of where they were manufactured;
- items manufactured outside the U.S. that include more than de minimis of controlled U.S.-origin content;
- items manufactured outside the U.S. that are the direct product of certain controlled U.S. technology or software, or are manufactured by a plant, or a major component of a plant, that is itself a direct product of such technology or software.

An EAR license is required for the export, re-export, or transfer (in country) of all items subject to the EAR with Export Control Classification Numbers (ECCNs) on the Commerce Control List (CCL) to or within Russia and Belarus when the parties know, or have reason to know, that a foreign-produced item meeting the direct product criteria is destined for Russia or Belarus or will be incorporated into or used for production/development of parts, components, or equipment that is produced in or destined for Russia or Belarus unless a license exception applies. License applications are subject to a policy of denial.

In February 2023, a new Iran Foreign Direct Product Rule addressed the use of Iranian unmanned aerial vehicles by Russia in its war against Ukraine. BIS has five lists of parties of concern:

1. Denied persons list[11] — a list of individuals and entities that have been denied export privileges;
2. Entity List[12] — a list of foreign parties that are prohibited from receiving some or all controlled items unless export license is granted. License applications in this case are normally subject to policy of denial;

11 Accessible under the link https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/denied-persons-list

12 Supplement 4 to Part 744 of the EAR

3. Unverified List[13] — a list of parties whose bona fides BIS has been unable to verify. No license exceptions may be used for exports, re-exports, or transfers (in-country) to unverified parties;
4. Military End User List[14] — a list of foreign parties that are prohibited from receiving controlled items unless export license is granted;
5. Consolidated Screening List[15] — a list of parties for which the U.S. Government maintains restrictions on certain exports, reexports or transfer of items.

European Union

In the European Union (EU), export control regulations are established both by EU legislation and regulations at the national level within Member States. The EU Dual-Use Regulation[16] serves as the overarching framework for dual-use export controls across the EU. This regulation provides EU-wide rules directly applicable in all Member States, encompassing controls on listed dual-use items and exports pertaining to controlled end use. It also outlines provisions for granting individual and global export licenses. Member States must enforce these rules adequately, and implement effective, proportionate, and dissuasive penalties.

Regarding military items, export controls are managed individually by EU Member States. While there exists an EU common military list, adopted annually by the Council, its authority is non-binding, and Member States retain the competence to legislate for national military export controls.

13 Supplement 6 to Part 744 of the EAR
14 Supplement 7 to Part 744 of the EAR
15 Accessible under the link www.trade.gov/consolidated-screening-list
16 Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), http://data.europa.eu/eli/reg/2021/821/2023-12-16

Specific export restrictions targeting Russia are delineated in Council Regulation (EU) No. 833/2014.[17] This regulation imposes limitations on the sale, supply, transfer, or export of various listed items to entities in Russia or for use within Russia.

The covered items include:
- dual-use items[18];
- energy-related items[19];
- items which might contribute to Russia‘s military and technological enhancement, or the development of the defense and security sector[20];
- goods and technology suited for use in oil refining and liquefaction of natural gas[21];
- items aimed for use in aviation or the space industry[22];
- maritime navigation and radio-communication items[23];
- luxury goods (items valued above EUR 300 per item)[24];
- jet fuel and fuel additives[25];
- an extensive list of items which could contribute in particular to the enhancement of Russian industrial capacities[26];
- banknotes denominated in any official currency of an EU Member State; and
- firearms, their parts and essential components and ammunition[27]

17 Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia‘s actions destabilising the situation in Ukraine, http://data.europa.eu/eli/reg/2014/833/2024-02-24
18 as listed in Annex I to EU Dual-Use Regulation 2021/821
19 as listed in Annex II to Regulation (EU) 833/2014
20 as listed in Annex VII to Regulation (EU) 833/2014
21 as listed in Annex X to Regulation (EU) 833/2014
22 as listed in Annex XI to Regulation (EU) 833/2014
23 as listed in Annex XVI to Regulation (EU) 833/2014
24 as listed in Annex XVIII to Regulation (EU) 833/2014
25 as listed in Annex XX to Regulation (EU) 833/2014
26 as listed in Annex XXIII to Regulation (EU) 833/2014
27 as listed in Annex I to Regulation (EU) No 258/2012 of the European Parliament and of the Council of 14 March 2012 implementing Article 10 of the United Nations‘ Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UN Firearms Protocol), and establishing export authorisation, and import and transit measures for firearms, their parts and components and ammunition

and firearms and other arms.[28]

This regulation further prohibits the provision of technical assistance, brokering services, financing, or intellectual property rights related to these listed items to entities in or for use in Russia. Additionally, there are restrictions on providing technical assistance, brokering services, and financing related to goods and technology listed in the EU Common Military List.

To the contrary of the EU Dual-Use Regulation 2021/821[29], the negotiation or arrangement of financial services has been specifically included, in the Russia sanctions regulation, in the definition of “brokering services”[30].

Financing or financial assistance has been defined as being “any action, irrespective of the particular means chosen”, whereby a person “disburses or commits to disburse its own funds or economic resources, including but not limited to grants, loans, guarantees, suretyships, bonds, letters of credit, supplier credits, buyer credits, import or export advances”[31].

28 as listed in Annex XXXV to Regulation (EU) 833/2014

29 Art. 2(7) of EU Dual-Use Regulation 2021/821. See also Art. 2.k. of Regulation (EU) 2019/125 of the European Parliament and of the Council of 16 January 2019 concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment.

30 Regulation 833/2014, Art. 1(d)). See also: Council Regulation (EU) 692/2014 of 23 June 2014 concerning restrictions on the import into the Union of goods originating in Crime or Sevastopol, in response to the illegal annexation of Crimea and Sevastopol, Art. 1(e); Council Regulation (EU) 2022/263 of 23 February 2022 concerning restrictive measures in response to the recognition of the non-government controlled areas of the Donetsk and Luhansk oblasts of Ukraine and the ordering of Russian armed forces into those areas, Art. 1(a). The same is the case for other EU sanctions regulations, see for example, Council Regulation (EC) 1183/2005 of 18 July 2005 imposing certain specific restrictive measures directed against persons acting in violation of the arms embargo with regard to the Democratic Republic of Congo, Art. 1(i); Council Regulation (EU) 224/2014 of 10 March 2014 concerning restrictive measures in view of the situation in the Central African Republic, Art. 1.a.; Council Regulation (EU) 401/2013 of 2 May 2013 concerning restrictive measures in respect of Myanmar/Burma, Art. 1.i.

31 Council Regulation (EU) 833/2014, Art. 1(o)). Such financing or financial assistance is, for example, prohibited when they are related to goods and technology listed in the EU Common Military List (Council Regulation (EU) 833/2014, Art. 4.1.b.) or dual-use items (Art. 2.2.b.) that are exported to Russia.

Chapter Three

Result Of The Russia-Related Sanctions

As a result of the sanctions, Russia's military-industrial complex and defense supply chains have been significantly degraded.[32] According to U.S. Government assessments, Russia has lost over 10,000 pieces of equipment on the battlefield and is struggling to replace them. This has resulted in Russia tasking its intelligence services with finding ways to circumvent sanctions and export controls to replace needed equipment.

The U.S. Government has also brought several enforcement cases against entities and individuals who violated U.S. export controls against Russia.[33] Many of these actions were brought as part of Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the sanctions and export controls and economic countermeasures that the United States has imposed, along with allies and partners, in response to Russia's unprovoked military invasion of Ukraine.[34]

In addition to Task Force KleptoCapture, the Disruptive Technology Strike Force, created in 2023, is targeting illicit actors, strengthening supply chains and protecting critical technological assets from being acquired or used by nation-state adversaries.[35]

32 See Treasury Press Release, "FACT SHEET: Disrupting and Degrading – One Year of U.S. Sanctions on Russia and Its Enablers" (24 February 2023). See also Department of Justice (DOJ) Press Release, "FACT SHEET: Justice Department Efforts in Response to Russia's February 2022 Invasion of Ukraine" (24 February 2023) and U.S. Department of State Press Release, "The Impact of Sanctions and Export Controls on the Russian Federation" (20 October 2022). See also BIS Press Release, "Remarks by Assistant Secretary Thea D. Rozman Kendler to the Association of Women in International Trade (WIIT)" (2 March 2023).

33 See DOJ Press Release, "Federal Court Orders Forfeiture of $826K in Funds Used in Attempt to Export Dual-Use High Precision Jig Grinder to Russia" (5 April 2023); BIS Press Release, "Microsoft to Pay Over $3.3M in Total Combined Civil Penalties to BIS and OFAC to Resolve Alleged and Apparent Violations of U.S. Export Controls and Sanctions" (6 April 2023); U.S Attorney's Office, Eastern District of New York Press Release, "United States Obtains Warrant for Seizure of Airplane Owned by Russian Oil Company Valued at Over $25 Million" (8 March 2023); BIS Press Releases, "BIS Takes Action Against Russian National and Related Company for Sending Controlled Counterintelligence Items to Russia and North Korea" (24 February 2023), and "Commerce Cuts Off Russia Procurement Network Evading Export Controls" (December 2022 BIS Enforcement Action) (13 December 2022).

34 See DOJ Press Release, "Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture" (2 March 2022); see also FinCEN Alert, "FinCEN Alert on Real Estate, Luxury Goods, and Other High-Value Assets Involving Russian Elites, Oligarchs, and their Family Members" (16 March 2022) at p. 7.

35 See DOJ-Commerce Joint Press Release, "Justice and Commerce Announce Creation of Disruptive Technology Strike Force" (16 February 2023).

RESULT OF THE RUSSIA-RELATED SANCTIONS

In May 2023 were announced the first five strike force enforcement actions.[36] One of those actions involved the arrest of a Greek national on 9 May 2023 involved in a procurement scheme to supply U.S.-origin military and dual-use technologies to Russia. The highly regulated and sensitive components included advanced electronics and sophisticated testing equipment used in military applications, including quantum cryptography and nuclear weapons testing, as well as tactical battlefield equipment. As described in the complaint, some of the Russian end users included nuclear and quantum research facilities, as well as the Russian Foreign Intelligence Service.[37]

According to an analysis by the KSE Institute[38], Russia continues to be able to import large amounts of goods needed for military production. Since the imposition of restrictions, supply chains have adapted and most of the items in question now reach Russia via intermediaries in third countries, including China. Almost half of the imports in the first ten months of 2023 consisted of goods that were produced on behalf of companies from coalition countries, indicating major enforcement challenges. But export controls remain a powerful instrument. Russia has not been able to find substitutes for many products from coalition countries, in particular advanced electronics, as the continued involvement of these producers shows. This means that, fundamentally, the potential of export controls to significantly curtail Russia's ability to wage its

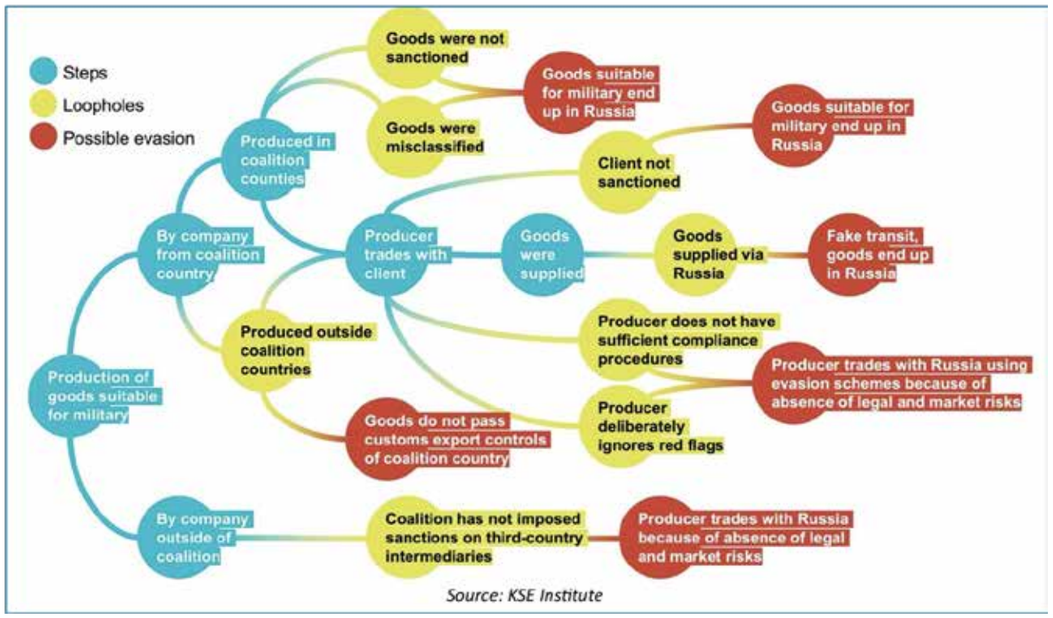
36 See DOJ-Commerce Joint Press Conference, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (16 May 2023); see also DOJ Press Releases, "Assistant Attorney General for National Security Matthew G. Olsen Delivers Remarks Announcing Disruptive Technology Strike Force Cases" (16 May 2023); and BIS Press Release, "BIS Takes Action Against Companies and Individuals for Attempting to Divert Electronics and Aircraft Parts to Russia" (16 May 2023).Strike Force" (16 February 2023).

37 See DOJ Press Release, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (16 May 2023).

38 Challenges of Export Controls Enforcement – How Russia continues to import components for its military production, by Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk and Vladyslav Vlasiuk, January 2024, https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

war of aggression on Ukraine remains intact. However, major changes to the current enforcement approach would be needed to improve their effectiveness.

Loopholes and possible evasion circuits are mapped as follows by the KSE Institute:



Source: KSE Institute

A common tactic used by illicit actors to evade Russia-related sanctions and export controls consists in using third-party intermediaries and transshipment points.[39]

39 See DOJ Press Release, "Departments of Justice, Commerce and Treasury Issue Joint Compliance Note on Russia Related Sanctions Evasion and Export Controls" (2 March 2023).

This tactic is also used to disguise the involvement of persons on Treasury's Office of Foreign Assets Control (OFAC) List of Specially Designated Nationals and Blocked Persons (SDN List)[40], or parties on the BIS Entity List in transactions and to obscure the true identities of Russian end users. Attempts to obfuscate the involvement of such listed parties in transactions and obscure the true identities of Russian end users may involve the use of shell and front companies.[41]

For example, a Russian entity with ties to the defense sector may establish a front company in another country as well as various affiliates of the front company in third countries.

Procurement agents, operating covertly on behalf of the Russian Government, will orchestrate purchases of goods by the front company from various suppliers, who in turn receive payment from the front company's non-Russian bank account, which may transmit funds through a correspondent bank account to route funds back to the supplier.

The front company will then route the goods to Russia, often through permissive jurisdictions such as known transshipment points.

40 See OFAC, "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists"
41 See December 2022 BIS Enforcement Action

Chapter Four

Products Of Concern

The authorities of different coalition countries, as well as some NGOs, have identified lists of commodities as presenting special concern because of their potential diversion to and end use by Russia and Belarus to further their military and defense capabilities.

U.S. Commodities of Concern

BIS remains concerned about exports that support the development of maritime technology, microelectronics, and other technologies that can be used to support Russia's military and defense sector. As such, all of the items listed hereafter require a BIS license prior to export or re-export to Russia or Belarus. Additionally, the use of certain of these items by third countries to create final products that may be subsequently exported to Russia or Belarus is also prohibited. This is not a complete listing of commodities sought by or prohibited for end-users in Russia and Belarus [42], but this list of commodities that present special concern can assist in the risk-based screening of export-related financial transactions.

Item	Export Control Classification Number
Aircraft Parts / Equipment	9A991
Antennas	7A994
Breathing Systems	8A992
Cameras	6A993
GPS System	7A994
Inertial Measurement Units	7A994
Integrated Circuits	3A001, 3A991, 5A991
Oil Field Equipment	EAR99
Sonar Systems	6A991

42 For a full list of items that now require a license if destined for Russia or Belarus, see 15 CFR Part 746, Supp. Nos. 2, 4, and 5, and Part 774, Supp. No. 1, to EAR.

Item	Export Control Classification Number
Spectrophotometers	3A999
Test Equipment	3B992
Thrusters	8A992
Underwater Communications	5A991
Vacuum Pumps	2B999
Water Fabrication Equipment	3B001, 3B991
Wafer Substrates	3C00x

EU Economically Critical Goods List

The sectoral sanctions aim at curtailing Russia's ability to wage the war, depriving it of critical technologies and markets and significantly weakening its industrial base. Regulation 833/2014 imposing sanctions against Russia includes prohibitions to sell, supply, transfer or export, directly or indirectly, goods which could contribute to the enhancement of Russian industrial capacities. Therefore, the Economically Critical Goods List[43] is comprised of mainly industrial goods subject to EU restrictive measures for which anomalous trade flows through certain third countries to Russia have been observed.

These economically critical goods included in the list derive from selected groups of mainly industrial goods classified under HS chapters: 28 (Chemicals); 84 (Machinery); 85 (Electronics); and 87 (Vehicles).

43 Economically Critical Goods List (Version of 18 October 2023): https://finance.ec.europa.eu/document/download/ed41eea6-8d13-4963-ad80-38a8d4f94b78_en?filename=230623-list-economically-critical-goods_en.pdf

The imports of these goods into third countries from the EU and the rest of the world show a significant increase since the start of the Russian invasion and the imposition of EU sanctions, which is mirrored by an increase in exports of those goods from those third countries to Russia. The list includes goods where: i) exports above the threshold of 1 million euro over a 12-month period (2022) has been recorded and ii) at least a 100% increase in exports to Russia from third countries as compared to the average of the three preceding years periods before the Russian invasion of Ukraine has been observed.

Trade statistics are continuously monitored for identifying trends and updating the composition of the Economically Critical Goods List.

HS Code	Item
2847.00	Hydrogen peroxide, whether or not solidified with urea
8409.00	Parts suitable for use solely or principally with compression-ignition internal combustion piston engines (diesel or semi-diesel engines), other than for aircraft engines
8412.21	Hydraulic power engines and motors, linear acting (cylinders)
8412.29	Hydraulic power engines and motors, other than linear acting
8413.30	Fuel, lubricating or cooling medium pumps for internal combustion piston engine
8413.50	Reciprocating positive displacement pumps for liquids (excl. those fitted or designed to be fitted with a measuring device, handpumps, fuel, lubricating or cooling medium pumps for internal combustion piston engines and concrete pumps)

HS Code	Item
8413.60	Rotary positive displacement pumps for liquids (excl. those fitted or designed to be fitted with a measuring device, handpumps, fuel, lubricating or cooling medium pumps for internal combustion piston engines and concrete pumps)
8413.81	Pumps for liquids (excl. those fitted or designed to be fitted with a measuring device, handpumps, fuel, lubricating or cooling medium pumps for internal combustion piston engines, concrete pumps, general reciprocating or rotary positive displacement pumps and centrifugal pumps)
8414.90	Parts of air or vacuum pumps, of air or other gas compressors and fans, of ventilating or recycling hoods incorporating a fan, whether or not fitted with filters, of gas-tight biological safety cabinets, whether or not fitted with filters
8419.89	Machinery, plant or laboratory equipment, whether or not electrically heated, for the treatment of materials by a process involving a change of temperature (excl. furnaces, ovens and other equipment of heading 8514, machinery or plant used for domestic purposes, non-electric instantaneous or storage water heaters, medical, surgical or laboratory sterilisers, dryers, distilling or rectifying plant, heat-exchange units, machinery for liquefying air or other gases, machinery, plant and equipment for making hot drinks or for cooking or heating food)
8421.23	Oil or petrol-filters for internal combustion engines

HS Code	Item
8421.29	Filtering or purifying machinery and apparatus for liquids (excl. for filtering or purifying water and beverages other than water, oil or petrol filters for internal combustion engines)
8421.31	Intake air filters for internal combustion engines
8421.39	Filtering or purifying machinery and apparatus for gases (excl. intake air filters for internal combustion engines for filtering, catalytic converters or particulate filters, whether or not combined, for purifying or filtering exhaust gases from internal combustion engines)
8421.99	Parts of machinery and apparatus for filtering or purifying liquids or gases
8424.89	Mechanical appliances (whether or not hand-operated) for projecting, dispersing or spraying liquids or powders, n.e.s. (excl. agricultural or horticultural appliances)
8424.90	Parts of mechanical appliances (whether or not hand-operated) for projecting, dispersing or spraying liquids or powders, of fire extinguishers, of spray guns and similar appliances, of steam or sandblasting machines and similar jet projecting machines
8426.91	Cranes, including cable cranes; mobile lifting frames, straddle carriers and works trucks fitted with a crane, self-propelled, on tyres (excl. overhead travelling cranes, transporter cranes, gantry cranes, bridge cranes, mobile lifting frames and straddle carriers, tower cranes, portal or pedestal jib cranes)

HS Code	Item
8428.31	Continuous-action elevators and conveyors, for goods or materials, specially designed for underground use (excl. lifts and skip hoists, pneumatic elevators and conveyors)
8428.39	Continuous-action elevators and conveyors, for goods or materials (excl. those specially designed for underground use, lifts and skip hoists, pneumatic elevators and conveyors
8429.51	Self-propelled front-end shovel loaders
8429.52	Self-propelled mechanical shovels, excavators and shovel loaders (other than front-end), with a 360 degree revolving superstructure
8429.59	Self-propelled mechanical shovels, excavators and shovel loaders (excl. machinery with a 360 degree revolving superstructure and front-end shovel loaders)
8430.10	Pile-drivers and pile-extractors
8431.39	Parts of machinery of heading 8428 (excl. parts of lifts, skip hoists or escalators)
8431.43	Parts for boring or sinking machinery of subheading 8430.41 or 8430.49
8431.49	Parts of machinery of heading 8426, 8429 and 8430, n.e.s.
8457.109	Machining centres for working metal
8466.10	Tool holders and self-opening die-heads, suitable for use solely or principally with the machines of headings 8456 to 8465
8471.30	Portable automatic data-processing machines, weighing not more than 10 kg, consisting of at least a central processing unit, a keyboard and a display

HS Code	Item
8471.60	Input or output units for automatic data-processing machines, whether or not containing storage units in the same housing
8471.70	Storage units for automatic data-processing machines
8473.30	Parts and accessories (other than covers, carrying cases and the like) suitable for use solely or principally with machines of heading 8471)
8474.10	Sorting, screening, separating or washing machines for earth, stone, ores or other mineral substances, in solid (including powder or paste) form
8474.31	Concrete or mortar mixers
8479.10	Machinery for public works, building or the like
8479.82	Mixing, kneading, crushing, grinding, screening, sifting, homogenizing, emulsifying or stirring machines
8479.89	Machines and mechanical appliances, n.e.s.
8479.90	Parts of machines and mechanical appliances, n.e.s.
8481.10	Pressure-reducing valves
8481.20	Valves for oleohydraulic or pneumatic transmission
8481.40	Safety or relief valves
8482.80	Roller bearings, including combined ball/roller bearings (excl. ball bearings, tapered roller bearings (incl. cone and tapered roller assemblies), spherical roller bearings, needle and other cylindrical roller bearings (incl. cage and roller assemblies)
8482.01	Balls, needles and rollers for ball or roller bearings
8481.10	Gaskets and similar joints of metal sheeting combined with other material or of two or more layers of metal

HS Code	Item
8484.90	Sets or assortments of gaskets and similar joints, dissimilar in composition, put up in pouches, envelopes or similar packings
8501.53	AC motors, multi-phase, of an output exceeding 75 kW, n.e.s.
8502.13	Generating sets with compression-ignition internal combustion piston engine (diesel or semi-diesel engine) of an output exceeding 375 kVA
8502.20	Generating sets with spark-ignition internal combustion piston engine
8503.00	Parts suitable for use solely or principally with electric motors and generators, electric generating sets and rotary converters
8507.10	Lead-acid accumulators of a kind used for starting piston engine “starter batteries”
8636.50	Switches for a voltage not exceeding 1.000 V
8537.10	Boards, panels, consoles, desks, cabinets and other bases, equipped with two or more apparatus of heading 8535 or 8536, for electrical control or the distribution of electricity, including those incorporating instruments or apparatus of chapter 90, and numerical control apparatus, other than switching apparatus of heading 8517, for a voltage not exceeding 1 000 V
8538.10	Boards, panels, consoles, desks, cabinets and other bases for the goods of heading 8537, not equipped with their apparatus
8538.90	Parts suitable for use solely or principally with the apparatus of heading 8535, 8536 or 8537 (excl. boards, panels, desks, cabinets and other bases for the goods of heading 8437, not equipped with their apparatus)

HS Code	Item
8544.49	Electric conductors, for a voltage not exceeding 1.000 V, insulated, not fitted with connectors, n.e.s.
8544.70	Optical fibre cables made up of individually sheated fibres, whether or not assembled with electric conductors or fitted with connectors
8701.21	Road tractors for semi-trailers, with only compression-ignition internal combustion piston engine “diesel or semi-diesel”
8704.21	Motor vehicles for the transport of goods, with compression-ignition internal combustion piston engine (diesel or semi-diesel) of a gross vehicle weight not exceeding 5 tonnes
8704.23	Motor vehicles for the transport of goods, with compression-ignition internal combustion piston engine (diesel or semi-diesel) of a gross vehicle weight not exceeding 20 tonnes
8704.31	Motor vehicles for the transport of goods, with spark-ignition combustion poiston engine, of a gross vehicle weight not exceeding 5 tonnes
8705.10	Crane lorries
8708.30	Brakes and servo-brakes; parts thereof, for motor vehicles of headings 8701 to 8705
8707.40	Gear boxes and parts thereof, for motor vehicles of headings 8701 to 8705
8708.50	Drive-axles with differential, whether or not provided with other transmission components, and non-driving axles, and parts thereof, for motor vehicles of headings 8701 to 8705
8708.70	Road wheels and parts and accessories thereof, for motor vehicles of headings 8701 to 8705

HS Code	Item
8708.80	Suspension systems and parts thereof (including shock-absorbers), for motor vehicles of headings 8701 to 8705
8708.91	Radiators and parts thereof, for motor vehicles of headings 8701 to 8705
8708.93	Clutches and parts thereof, for motor vehicles of headings 8701 to 8705
8708.94	Steering wheels, steering columns and steering boxes, and parts thereof, for motor vehicles of headings 8701 to 8705
8708.99	Other parts and accessories, for motor vehicles of headings 8701 to 8705
8716.39	Trailers and semi-trailers for the transport of goods, not designed for running on rails (excl. self-loading or self-unloading trailers and semi-trailers for agricultural purposes and tanker trailers and tanker semi-trailers)
8716.90	Parts of trailers and semi-trailers and other vehicles not mechanically propelled, n.e.s.

High Priority Items List by Harmonized System Code

The European Commission, in coordination with the competent authorities in the U.S., the UK and Japan[44], have identified several prohibited dual-use goods and advanced technology items used in Russian military systems found on the battlefield in Ukraine or critical to the development, production or use of those Russian military systems.

44 On 14 September 2023, the U.S. BIS published a tiered list of 45 "common high-priority items" by HS Code that consolidated and expanded on previous notices. Two weeks later, the United States, Australia, Canada, New Zealand, and the United Kingdom (collectively the "Export Enforcement Five" or "E5") released a joint guidance notice prioritizing the new tiered list for export enforcement in all five countries.

These items include electronic components such as integrated circuits and radio frequency transceiver modules, as well as items essential for the manufacturing and testing of the electronic components of the printed circuit boards, and manufacturing of high precision complex metal components retrieved from the battlefield.

This High Priority Items List is primarily based on the HS code classification of Russian weapons system components recovered on the battlefield in Ukraine. Items described by these HS codes have been found in multiple Russian weapons systems used against Ukraine, including the Kalibr cruise missile, the Kh-101 cruise missile, and the Orlan-10 UAV.

The High Priority Items List is not an exhaustive list of all items Russia is attempting to procure, but provides prioritized targets for customs and enforcement agencies around the world.

The List of Common High Priority Items[45] is divided into four Tiers containing a total of 50 (Harmonised System codes) dual-use and advanced technology items involved in Russian weapons system used against Ukraine.

The list is divided into four Tiers:

- Tier 1 comprises four HS codes which describe integrated circuits (also referred to as microelectronics).
- Tier 2 comprises five HS codes containing electronics items related to wireless communications, satellite-based radio-navigation and passive electronic components.

45 List of Common High Priority Items (Version of February 2024): https://finance.ec.europa.eu/document/download/5a2494db-d874-4e2b-bf2a-ec5a191d2dc0_en?filename=230623-list-high-priority-battlefield-items_en.pdf

- Tier 3 is itself divided in two sets: - Tier 3.A, which comprises 16 HS codes containing discrete electronic components, electrical plugs and connectors, navigation equipment and digital cameras. - Tier 3.B, which lists nine HS codes used to export mechanical and non-electronic components, such as bearings and optical components.
- Tier 4 is also divided in two sets: - Tier 4.A, which includes 11 HS codes concerning manufacturing equipment for production and quality testing of electric components and circuits. - Tier 4.B, which lists 5 HS codes concerning Computer Numerical Control (CNC) machine tools for working metal, and related components.

The List is not static and will be periodically adjusted in the light of what is found in Russian military systems on the battlefield and Russia's use of sanctioned sensitive items.

The current version (February 2024) has the following content:

Code	Item
TIER 1	
8542.31	Electronic integrated circuits: Processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits or other circuits
8542.32	Electronic integrated circuits: Memories
8542.33	Electronic integrated circuits: Amplifiers
8542.39	Electronic integrated circuits: Other
TIER 2	
8517.62	Machines for the reception, conversion and transmission or regeneration of voice, images or other data, including switching and routing apparatus

Code	Item
8526.91	Radio navigational aid apparatus
8532.21	Other fixed capacitors: Tantalum capacitors
8532.24	Other fixed capacitors: Ceramic dielectric, multilayer
8548.00	Electrical parts of machinery or apparatus, not specified or included elsewhere in chapter 85
TIER 3.A	
8471.50	Processing units other than those of subheading 8471 41 or 8471 49, whether or not containing in the same housing one or two of the following types if unit: storage units, input units, output units
8504.40	Static converters
8517.69	Other apparatus for the transmission or reception of voice, images or other data, including apparatus for communication in a wired or wireless network
8525.89	Other television cameras, digital cameras and video cameras recorders
8529.10	Aerials and aerial reflectors of all kinds; parts suitable for use therewith
8529.90	Other parts suitable for use solely or principally with the apparatus of headings 8524 to 8528
8536.69	Plugs and sockets for a voltage not exceeding 1 000 V
8536.90	Electrical apparatus for switching electrical circuits, or for making connections to or in electrical circuits, for a voltage not exceeding 1 000 V (excluding fuses, automatic circuit breakers and other apparatus for protecting electrical circuits, relays and other switches, lamp holders, plugs and sockets)
8541.10	Diodes, other than photosensitive or light-emitting diodes (LED)

Code	Item
8541.21	Transistors, other than photosensitive transistors with a dissipation rate of less than 1 W
8541.29	Other transistors, other than photosensitive transistors
8541.30	Thyristors, diacs and triacs (excl. photosensitive semiconductor devices)
8541.49	Photosensitive semiconductor devices (exc. Photovoltaic generators and cells)
8541.51	Other semiconductor devices: Semiconductor-based transducers
8541.59	Other semiconductor devices
8541.60	Mounted piezo-electric crystals
TIER 3.B	
8482.10	Ball bearings
8482.20	Tapered roller bearings, including cone and tapered roller assemblies
8482.30	Spherical roller bearings
8482.50	Other cylindrical roller bearings, including cage and roller assemblies
8807.30	Other parts of aeroplanes, helicopters or unmanned aircraft
9013.10	Telescopic sights for fitting to arms; periscopes; telescopes designed to form parts of machines, appliances, instruments or apparatus of this chapter of Section XVI
9013.80	Other optical devices, appliances and instruments
9014.20	Instruments and appliances for aeronautical or space navigation (other than compasses)
9014.80	Other navigational instruments and appliances

Code	Item
TIER 4.A	
8471.80	Units for automatic data-processing machines (excl. processing units, input or output units and storage units)
8486.10	Machines and apparatus for the manufacture of boules or wafers
8486.20	Machines and apparatus for the manufacture of semiconductor devices or of electronic integrated circuits
8486.40	Machines and apparatus specified in note 11/C) to this chapter
8534.00	Printed circuits
8543.20	Signal generators
9027.50	Other instruments and apparatus using optical radiations (ultraviolet, visible, infrared)
9030.20	Oscilloscopes and oscillographs
9030.32	Multimeters with recording device
9030.39	Instruments and apparatus for measuring or checking voltage, current, resistance or electrical power, with recording device
9030.82	Instruments and apparatus for measuring or checking semiconductor wafers or devices
TIER 4.B	
8457.10	Machining centres for working metal
8458.11	Horizontal lathes, including turning centres, for removing metal, numerically controlled
8458.91	Lathes (including turning centres) for removing metal, numerically controlled (excluding horizontal lathes)

Code	Item
8459.61	Milling machines for metals, numerically controlled (excluding lathes and turning centres of heading 8458, way-type unit head machines, drilling machines, boring-milling machines, boring machines, and knee-type milling machines)
8466.93	Parts and accessories suitable for use solely or principally with the machines of headings 8456 to 8461, n.e.s.

Critical components

The KSE Institute has published a list of critical components to which export controls should be extended, because important inputs for the Russian military industry are still not export controlled.[46]

Automotive components and equipment (83)			
8407 10 0003	8407 21 1000	8407 21 9100	8407 21 9900
8407 29 0000	8407 32 1000	8407 34 3009	8408 20 9907
8408 90 6500	8408 90 6700	8409 91 0008	8409 99 0009
8411 11 0001	8411 12 3009	8411 21 0009	8411 81 0001
8411 81 0008	8411 91 0001	8411 91 0002	8411 91 0008
8411 99 0019	8411 99 0091	8411 99 0098	8412 21 2002
8412 21 2009	8412 21 8008	8412 29 2009	8412 29 8109
8412 29 8909	8412 31 0009	8412 39 0009	8412 80 8009
8412 90 4008	8412 90 8009	8479 89 9707	8479 90 7000
8501 10 1001	8501 10 1009	8501 10 9100	8501 10 9300
8501 10 9900	8501 20 0009	8501 31 0000	8501 32 0008
8501 33 0008	8501 34 0000	8501 40 2004	8501 40 2009

46 Challenges of Export Controls Enforcement – How Russia continues to import components for its military production, by Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk and Vladyslav Vlasiuk, January 2024, https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

PRODUCTS OF CONCERN

Automotive components and equipment (83)			
8501 40 8009	8501 51 0001	8501 51 0009	8501 52 2001
8501 52 2009	8501 52 3000	8501 61 7000	8501 62 0000
8511 10 0009	8511 30 0008	8511 40 0008	8511 50 0008
8511 80 0008	8511 90 0009	8708 10 9009	8708 29 9009
8708 30 9109	8708 30 9909	8708 40 5009	8708 40 9109
8708 40 9909	8708 50 9909	8708 70 5009	8708 70 9909
8708 80 3509	8708 80 5509	8708 80 9909	8708 91 3509
8708 91 9909	8708 92 3509	8708 93 9009	8708 94 3509
8708 94 9909	8708 99 9309	8708 99 9709	
Bearings and transmission shafts (31)			
8482 10 1009	8482 10 9001	8482 10 9008	8482 20 0009
8482 30 0009	8482 40 0009	8482 50 0009	8482 80 0009
8482 99 0000	8483 10 2108	8483 10 2509	8483 10 2909
8483 10 5000	8483 10 9500	8483 20 0000	8483 30 3209
8483 30 3809	8483 30 8007	8483 40 2100	8483 40 2308
8483 40 2500	8483 40 2900	8483 40 3009	8483 40 5900
8483 40 9000	8483 50 8000	8483 50 8000	8483 60 2000
8483 60 8000	8483 90 8100	8483 90 8909	
Communications equipment (80)			
8517 80 0000	8517 61 0002	8517 61 0008	8517 62 0002
8517 62 0003	8517 62 0009	8517 69 9000	8517 70 9009
8517 71 1100	8517 71 1500	8517 71 1900	8517 79 0001
8517 79 0009	8521 90 0009	8523 21 0000	8523 29 1505
8523 29 1509	8523 29 3102	8523 29 3901	8523 29 3908
8523 41 9000	8523 49 2500	8523 49 3900	8523 49 4500
8523 49 5100	8523 49 5900	8523 49 9900	8523 51 1000
8523 51 9101	8523 51 9109	8523 51 9300	8523 51 9900
8523 52 9001	8523 52 9009	8523 59 1000	8523 59 9101
8523 59 9109	8523 59 9300	8523 59 9900	8523 80 9300
8523 80 9900	8525 50 0000	8525 60 0009	8525 81 9100

8525 81 9900	8525 89 1900	8525 89 3000	8525 89 9109
8525 89 9900	8526 10 0001	8526 10 0009	8526 91 2000
8526 92 0008	8527 13 9900	8527 19 0000	8527 21 2009
8527 21 5909	8527 21 9800	8527 29 0009	8527 91 1900
8527 91 3500	8527 91 9900	8527 92 1000	8527 99 0000
8529 10 1100	8529 10 6500	8529 10 6901	8529 10 6909
8529 10 8000	8529 10 9500	8529 90 2002	8529 90 6502
8529 90 6508	8529 90 6509	8529 90 9600	
Computer components (15)			
8471 41 0000	8471 50 0000	8471 70 2000	8471 70 3000
8471 70 5000	8471 70 7000	8471 70 8000	8471 70 9800
8471 80 0000	8471 90 0000	8473 30 2002	8473 30 2008
8473 30 8000	8473 50 2000	8473 50 8000	
Drones (5)			
8806 22 0001	8806 92 0001	8807 20 0000	8807 30 0000
8807 90 0009			
Electric and electronic equipment (159)			
8504 10 2000	8504 10 8000	8504 21 0000	8504 22 9000
8504 23 0009	8504 31 2109	8504 31 2909	8504 31 8001
8504 31 8007	8504 32 0002	8504 32 0009	8504 33 0009
8504 34 0000	8504 40 3004	8504 40 3008	8504 40 3009
8504 40 5500	8504 40 8300	8504 40 8500	8504 40 8700
8504 40 9000	8504 40 9100	8504 50 2000	8504 50 9500
8504 90 0600	8504 90 1100	8504 90 1700	8504 90 9200
8504 90 9800	8505 11 0000	8505 19 1000	8505 19 9000
8505 20 0000	8505 90 2009	8506 10 1100	8506 10 1801
8506 10 1809	8506 10 9100	8506 10 9809	8506 40 0000
8506 50 1000	8506 50 3000	8506 50 9000	8506 60 0000
8506 80 8000	8507 10 2003	8507 20 2000	8507 20 8001
8507 20 8008	8507 30 2009	8507 50 0000	8507 60 0000
8507 80 0001	8507 80 0009	8532 10 0000	8532 21 0000

8532 22 0000	8532 23 0000	8532 24 0000	8532 25 0000
8532 29 0000	8532 30 0000	8532 90 0000	8533 10 0000
8533 21 0000	8533 29 0000	8533 31 0000	8533 39 0000
8533 40 1000	8533 40 9000	8533 90 0000	8534 00 1100
8534 00 1900	8534 00 9000	8535 10 0000	8535 21 0000
8535 29 0000	8535 30 2000	8535 40 0000	8535 90 0008
8536 10 1000	8536 10 5000	8536 10 9000	8536 20 1007
8536 20 9007	8536 20 2000	8536 30 4000	8536 30 8000
8536 41 1000	8536 41 9000	8536 49 0000	8536 50 0400
8536 50 0600	8536 50 0700	8536 50 1109	8536 50 1509
8536 50 1904	8536 50 1906	8536 50 8008	8536 61 1000
8536 61 9000	8536 69 1000	8536 69 3000	8536 69 9002
8536 69 9008	8536 70 0001	8536 70 0002	8536 70 0003
8536 70 0004	8536 90 0100	8536 90 1000	8536 90 8500
8537 10 1000	8537 10 9100	8537 10 9800	8537 10 9900
8537 20 9200	8537 20 9800	8538 10 0000	8538 90 1200
8538 90 9200	8538 90 9901	8538 90 9908	8540 20 8000
8540 71 0001	8540 71 0009	8540 81 0000	8540 89 0000
8543 20 0000	8543 40 0000	8543 70 3008	8543 70 8000
8543 70 9000	8543 90 0000	8544 11 9000	8544 19 0009
8544 20 0000	8544 30 0002	8544 30 0003	8544 30 0007
8544 42 1000	8544 42 9003	8544 42 9007	8544 42 9009
8544 49 2000	8544 49 9101	8544 49 9108	8544 49 9309
8544 49 9501	8544 49 9509	8544 49 9900	8544 60 1000
8544 60 9009	8544 70 0000	8545 11 0089	8545 20 0009
8545 90 9000	8548 00 9000	8549 99 0000	
Navigation equipment and sensors (62)			
9002 11 0000	9002 19 0000	9002 20 0000	9002 90 0009
9013 20 0000	9013 80 0000	9013 90 0000	9014 10 0000
9014 20 2009	9014 20 8001	9014 20 8009	9014 80 0000
9014 90 0000	9015 10 1000	9015 10 9000	9015 30 9000

9015 40 1000	9015 90 0000	9025 11 8000	9025 19 2000
9025 19 8009	9025 80 2000	9025 80 4000	9025 80 8000
9025 90 0003	9025 90 0008	9026 10 2100	9026 10 2900
9026 10 8100	9026 10 8900	9026 20 2000	9026 20 4000
9026 20 8000	9026 80 2000	9026 80 8000	9026 90 0000
9027 50 0000	9029 10 0009	9029 20 3109	9029 20 3809
9029 90 0009	9030 10 0000	9030 20 1000	9030 31 0000
9030 32 0009	9030 33 1000	9030 33 9100	9030 33 9900
9030 39 0009	9030 40 0000	9030 82 0000	9030 84 0009
9030 89 3000	9030 89 9009	9030 90 8500	9032 10 2000
9032 10 8100	9032 10 8900	9032 20 0000	9032 81 0000
9032 89 0000	9032 90 0000		
Semiconductors (37)			
8541 10 0001	8541 10 0009	8541 21 0000	8541 29 0000
8541 30 0009	8541 41 0001	8541 41 0002	8541 41 0004
8541 41 0006	8541 41 0007	8541 41 0008	8541 41 0009
8541 42 0000	8541 43 0000	8541 49 0000	8541 51 0000
8541 59 0000	8541 60 0000	8541 90 0000	8542 31 1001
8542 31 1009	8542 31 9010	8542 31 9090	8542 32 1000
8542 32 3100	8542 32 3900	8542 32 4500	8542 32 5500
8542 32 6100	8542 32 6900	8542 32 7500	8542 32 9000
8542 33 9000	8542 39 1000	8542 39 9010	8542 39 9090
8542 90 0000			
Other components (13)			
8486 20 9009	8486 90 1000	8486 90 9008	9024 80 9000
9024 90 0000	9031 49 9000	9031 80 3400	9031 80 3800
9031 80 9100	9031 80 9800	9031 90 2000	9031 90 3000
9031 90 8500			

U.S. Disruptive Technology

On 16 February 2023, the U.S. authorities announced the formation of a Disruptive Technology Strike Force[47]. This group works to protect U.S. advanced technologies from being illicitly acquired and used by nation state adversaries to support their military modernization efforts designed to counter U.S. national security interests or their mass surveillance programs that enable human rights abuses. As part of this effort, strike force cells stationed in twelve American cities are using all-source information to pursue investigations and impose criminal and/or administrative penalties as appropriate.

While this list is not exclusive, disruptive technology may include:

- Advanced Semiconductors: logic/artificial intelligence (AI) chips, associated fabrication equipment, electronic design automation (EDA) software/technology, and novel materials for production below 14 nanometers (nm)
- Supercomputer Computing Hardware: including graphics processing units (GPUs), and software (including for modeling/simulations)
- Quantum Technologies
- Hypersonic Technologies
- Military Bioscience/Technology (e.g., human performance enhancements like brain computer interfaces)
- Advanced Aerospace Technology

47 See DOJ Press Release, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023); see also DOJ Press Release, "Justice Department Announces Five Cases as Part of Recently Launched Disruptive Technology Strike Force" (May 16, 2023).

Chapter Five

Challenges Faced By Banks

Despite their best efforts, banks encounter several challenges in fulfilling their obligations concerning export control compliance. These challenges include the following:

Complex Regulatory Landscape

The ever-evolving nature of export control regulations poses a significant challenge for banks, requiring them to constantly adapt their compliance frameworks to align with new regulatory requirements and international standards.

Resource Constraints

Implementing robust compliance programs requires substantial financial and human resources, which may pose challenges for smaller banks with limited budgets and staffing capabilities.

Technological Limitations

The effectiveness of banks‘ compliance efforts heavily relies on the sophistication of their technological infrastructure. However, many banks struggle with outdated systems and legacy processes, hindering their ability to effectively monitor and mitigate compliance risks.

Cross-border Transactions

The proliferation of cross-border transactions further complicates banks‘ compliance efforts, as they must navigate disparate regulatory regimes and coordinate with foreign counterparts to

ensure adherence to export control regulations.

Reliance On Client Declarations

To face the new restrictions, the primary reaction of financial institutions seemed to rely on declarations provided by their clients. This approach can nevertheless result in the liability of the financial institution not being discharged should economic sanctions restrictions be breached. The EU Commission is requiring banks to exercise due diligence because they "cannot rely on the sole declaration of their customer that the goods and technology concerned are not covered by restrictive measures"[48].

The reason for that requirement resides in that, "while it is true that primary responsibility for the classification of goods and technology lies with those responsible for sending or receiving such items, the prohibition to provide financial assistance for the goods subject to a ban is (…) incumbent upon banks".

However, financial institutions generally do not have the required internal expertise in qualifying tangible/intangible items, software or technologies as being export controlled.

48 Commission Guidance Note on the implementation of certain provisions of Regulation (EU) No 833/2014, Commission Notice of 25.8.2017, C(2017) 5738 final

Chapter Six

Applying A Risk-Based Approach To Trade Finance

Financial institutions, particularly banks but also credit card operators and foreign exchange dealers, may be involved in providing financing, processing payments, or performing other services associated with international trade. These services include, but are not limited to:

- processing payments for exported goods,
- issuing lines of credit for exporters,
- providing or handling the payments supported by letters of credit,
- processing payments associated with factoring of accounts receivables by an exporter,
- providing general credit or working capital loans, and
- issuing or paying insurance on the shipping and delivery of goods to protect the exporter from nonpayment by the buyer.

Financial institutions directly involved in providing trade finance for exporters also may have access to information relevant to identifying potentially suspicious activity. This may include their customers' end-use certificates, export documents, or other more extensive documentation associated with letters of credit-based trade financing. Or it may include information about the other parties to the transactions that may be contained in payment transmittal orders they receive or handle as an intermediary institution, such as SWIFT messages, which are increasingly associated with open account trade transactions.

Financial institutions with customers in maritime or export/import industries should rely on their internal risk assessments to employ appropriate risk mitigation measures. This may include appropriate due diligence policies and beneficial ownership requirements[49], but also verification of HS codes of the exported goods (which may be found on trade documents including commercial invoices, packing slips, airway bills, sea bills, or other supporting trade documentation), identification of possible third-party intermediaries and attempts at evasion of export controls[50].

49 See, for example, customer identification program requirements established in 31 CFR § 1010.220 as applicable to specific types of financial institutions in 31 CFR § 1020.220 (banks), § 1023.220 (broker-dealers), § 1024.220 (mutual funds), and § 1026.220 (futures/commodities). See also the beneficial ownership requirements for legal entity customers established in 31 CFR § 1010.230.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

Elaborate a strategic risk assessment

To mitigate to the maximum extent possible their exposure to sanctions circumvention schemes, banks should conduct a strategic risk assessment, following these successive steps:

A. Identification of threats and vulnerabilities

Financial institutions should stay alert to the main techniques used by Russian actors to circumvent sanctions, as well as to emerging patterns. They should also map out the types of products, transactions and economic activities within their range of services that are at risk of being involved in Russia sanctions circumvention techniques.

Examples of customers who might be particularly impacted and to whom banks must exercise particular vigilance

Example (1): An manufacturer of semiconductor devices. It is well known that these goods are in high demand in Russia and their export to Russia is prohibited. The volume of exports is

50 See "Departments of Commerce, Treasury and Justice Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls" (2 March 2023), pp. 1-2. 13. See FinCEN June 2022 and May 2023 Alerts

increasing towards third countries with which trade in such goods was previously limited or non-existent.

Example (2): A manufacturer of items identified in the Common High Priority list. It is well known that battlefield items are in high demand in Russia and their export to Russia is subject to export restrictions.

Example (3): A manufacturer of goods that have a very specific tariff classification and as such may or may not fall in the scope of the export ban.

Example (4): A manufacturer of goods that may be often and easily miscategorised under an HS code not subject to sanctions.

Example (5): A freight forwarder company that is organising the transport of the exported goods.

B. Risk analysis

Banks should assess the nature of the risks to which their customer's sector, products and economic activities are exposed to, and understand how those risks can materialise.

To this end, they may use risk indicators, typologies and any other relevant information that is publicly available or forms part of their specialised knowledge.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

Example

- Main risks identified: attempts of transferring goods to Russia via third countries;
- How can the risks be prevented: enhanced evaluation of the risk by trained staff, monitoring of contractual arrangements for customers and business partners, ensuring the processing and end-use of the product.

C. Design of mitigating measures

How can the risks be prevented? What are the measures to implement in order to mitigate these risks? Which are the relevant national authorities to raise operators' awareness of the risk and provide guidance?

D. Implementation of mitigating measures

To mitigate the risk of circumvention, banks that identify higher risk areas in their business may proactively incorporate, as appropriate, the results of steps B) and C) into their internal risk management practices and procedures, and have controls in place to test the effective functioning of those procedures.

E. Regular updating

The evolution of circumvention techniques and the use of increasingly complex methods of circumvention require that the mapping of threats and vulnerabilities is updated whenever necessary, for instance when sanctions are amended or new

sanctions are adopted, and in any case on a regular basis. This requires that the bank has satisfactory procedures in place for following and maintaining the necessary information (for example, sanctions legislation, circumvention techniques, circumvention trade flows) up-to-date. The training of the staff on these issues is of critical importance as well.

Moreover, it is recommended that the senior management is personally involved and informed regularly by compliance officers on risks identified and measures taken.
By adopting a risk assessment and risk management approach to circumvention, banks will help ensure that measures taken to prevent or mitigate circumvention are commensurate with the risks identified. The implementation of risk assessment and risk management should also enable them to concentrate their efforts on the most sensitive cases and thus allocate their resources in the most effective way.

Perform Risk-Based Due Diligence

Once their risk exposure has been identified, banks shall set up processes and controls to mitigate and manage the identified risks.

A. Enhanced due diligence

There is no single model for conducting due diligence. Banks should, following their assessment of circumvention risks and typologies outlined here before, align their efforts to comply with the risks identified. This risk assessment and risk management approach should lead them to adopt a proportionate approach, in particular by focusing on those sectors that are deemed to be most

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

critically exposed to circumvention risks, and to accordingly put in place adequate commensurate systems to prevent those risks from occurring (“enhanced due diligence”).

Internal trade compliance program. As there is no one-size-fits-all model of due diligence, compliance measures may depend – and be calibrated accordingly – on the business specificities and the related risk exposure. It is for each bank to develop, implement, and routinely update a trade sanctions compliance program that reflects their individual business models, geographic and sectoral areas of operations and related risk assessment.

Customer Due Diligence (CDD). Banks are obligated to perform robust CDD procedures to ascertain the identity of their customers, understand the nature of their business activities, and assess the risk associated with their transactions. This entails verifying the legitimacy of the goods or services being traded and screening customers against various watch-lists and sanction lists maintained by regulatory authorities.

Transaction Monitoring. Banks are required to implement sophisticated transaction monitoring systems capable of flagging suspicious activities indicative of potential export control violations. This involves scrutinizing the parties involved in transactions, identifying unusual patterns or deviations from established norms, and promptly reporting any anomalies to the relevant authorities.

Screening of Transactions. Banks are mandated to screen transactions against various sanctions lists and export control regulations to prevent the transfer of funds in support of illicit activities. This entails leveraging advanced screening tools

capable of detecting prohibited transactions and entities involved in the proliferation of controlled items.

Red flag transactions. Sanctions compliance programs can assist in detecting red flag transactions that can be indicative of a circumvention pattern[51].

Specific queries on the customer's level. Whenever implementing enhanced due diligence (for example because banking activities create exposure to a particular risk), specific queries should be made on the stakeholders' level. The purpose is to identify and verify customers, business partners, their representatives, their beneficial owners and other possible persons of interest.

- Is there any proven business record?
- Is there any effort from the stakeholder to maintain sanctions internal control systems / ensure sanctions compliance?
- Who are the main stakeholders involved/relevant for our business?
- Are any of the direct stakeholders (customers, distributors, agents, etc.) or indirect stakeholders (end-user, intermediaries, banks etc.) targeted by sanctions? Are all stakeholders known?
- If yes, has the stakeholder undergone changes in their ownership structure upon or after the adoption of sanctions? Was it set up or established after the introduction of the sanctions?
- Are these stakeholders affected by sanctions through ownership or control?
- Who is the end-user? Can the end-user certificate be provided?

Specific queries on the level of the transaction and flows of money, as well as transportation/logistics and route of goods.

51 See point B. here after

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

- What is the country of origin of the goods?
- What is the country of transit and of destination? Is this country neighboring Russia or Belarus, does it have easy transport / access (i.e. passport/shipping controls) to Russia or Belarus, or is it otherwise known to re-export goods to those jurisdictions? Should the export be subject to enhanced vigilance/end-use controls?
- Are complex/unusual transportation routes being used?
- Has the value of goods changed since the imposition of sanctions? Has the method of trading/transacting changed, for example the contract conditions imposed?
- What is the business rationale for the transaction? Does the transaction or shipment seem in line with expectations regarding the (prospective) customer from a business perspective? Or does the transaction or shipment seem unjustified from a business perspective?
- Does the transaction use complex financial schemes which are not justified by its purpose?
- Has the method of transport/shipping changed since the imposition of sanctions?
- Are there unusual or abnormal elements in the documentation that do not match (for example between financial documents and the contract)?

Specific queries on the goods level.

- Are the goods subject to any sanctions or export/import control rules?
- Are the goods included in the Common High Priority items list or the economically critical goods list?

- Do the goods contain components that are more likely to be disassembled and diverted for non-intended purposes?
- Are the goods similar to sanctioned ones?
- If the goods are shipped through Russia or Belarus, is the route standard and economically viable? Particular attention should be paid for exports to countries which do not apply restrictions on exports of sensitive goods to Russia and Belarus.

Enhanced vigilance with regard to the use of correspondent accounts. Transactions relying on correspondent accounts can lead to a higher residual risk of sanctions circumvention. Correspondent accounts are relationships between financial institutions that facilitate the provision of services from one (the correspondent) to another (the respondent). These services can relate to transactions for the respondent financial institution itself or on behalf of its customers, including processing wire transfers, international trade settlements, remittances, and cross-border payments.

Financial institutions that maintain correspondent accounts for foreign financial institutions are required to establish appropriate, risk-based enhanced due diligence frameworks, with policies, procedures, and processes that are reasonably designed to assess and mitigate the risks inherent with these relationships.

In the context of sanctions implementation, financial institutions should monitor transactions related to correspondent accounts to detect and prevent potential attempts to breach sanctions. Without prejudice to Anti-Money-Laundering and Counter Financing of Terrorism (AML/CFT) requirements, their due diligence frameworks should take into account the level of risk of sanctions circumvention posed by the foreign respondent.
The risks can vary depending on the respondent's profile.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

In practice, this means that financial institutions may conduct an adequate assessment of risks and appropriate due diligence of the risks present in:
1. the foreign respondent's business and markets;
2. the type, purpose and anticipated activity;
3. the nature and duration of the relationship with the foreign respondent; and
4. the supervisory regime of the jurisdiction in which the foreign respondent is licensed,

and design and implement controls to manage these risks effectively.

B. Red Flag indicators of export control evasion

Illicit actors use a variety of methods when trying to acquire items which are export controlled.[52] To evade scrutiny, these actors often attempt to procure low-tech consumer goods not specified on the dual-use lists and therefore not requiring a license for export, re-export, or transfer to most destinations. Illicit actors also will engage complicit shippers (or customs brokers) to obscure either the nature of the goods or their ultimate destinations, similar to efforts with other illicit goods.[53]

Enforcing sanctions and trade controls has required regulators to identify an evolving series of tactics being used to move financial assets and supply controlled goods to Russia or Belarus. To do so, Governments have publicized "red flags", or potential indicators that a party in a transaction is trying to evade government scrutiny. Red

52 See FinCEN "Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering," (18 February 2010).
53 For information on common deceptive shipping practices and general approaches to tailor due diligence and sanctions compliance policies and procedures, see U.S. Department of State, U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), and the U.S. Coast Guard, "Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities," (14 May 2020).

flags are warning signals that indicate an increased risk of fraudulent or illicit activity, like a connection to a sanctioned individual or abrupt changes in buying or shipping patterns.

Red flags aren't just guidelines – they also have legal implications. Exporters or financial institutions who are ignoring red flags, or worse, are "self-blinding" by discouraging customers from sharing information about the ultimate end use or destination of the transaction, incur liability.

The red flags listed hereafter are compiled from different governmental[54] and academic[55] sources.

Red flags can arise in connection with many aspects of an export transaction, including (1) the product to be exported, (2) the customer buying the product, (3) the network or corporate structure of the customer, (4) the export destination, (5) the logistics of the transaction, and (6) the alleged end use.

54 The Financial Crimes Enforcement Network (FinCEN) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) have issued red flags lists in their joint alerts. Other countries have also published their own lists of risk indicators of Russia-related sanctions evasion, including Estonia, Latvia, Lithuania, Finland, and Poland, as well as Australia, Canada, the United Kingdom, and the European Union. See e.g. the following:
- "Practical Guidance for Economic Operators to Detect and Prevent Circumvention of Sanctions Has Been Published," Ministry of Foreign Affairs of the Republic of Lithuania, 17 July 2023, available at https://urm.lt/default/en/news/practical-guidance-for-economic-operators-to-detect-and-prevent-circumvention-of-sanctions-has-been-published
- "European Commission Guidance for EU Operators: Implementing Enhanced Due Diligence to Shield Against Russia Sanctions Circumvention," European Union, 2023, available at https://finance.ec.europa.eu/system/files/2023-09/230905-guidance-eu-operators-russia-sanctions-circumvention_en.pdf
- "Red Alert – Financial Sanctions Evasion Typologies: Russian Elites and Enablers," Office of Financial Sanctions Implementation, HM Treasury, July 2022, available at https://database.riskreport.org/sites/default/files/2022-07/uk-red-alert-financial-sanctions-evasions-russia-typologies-07122022.pdf
- "Special Bulletin on Russia-Linked Money Laundering Activities," Financial Transactions and Reports Analysis Centre of Canada, May 2023, available at https://fintrac-canafe.canada.ca/intel/bulletins/rlml-eng.pdf
- "Advisory to the Australian Exports Sector on Russian Evasion – Third Country Transhipment Hubs, Shell Companies and End Users," Department of Foreign Affairs and Trade, available at https://www.dfat.gov.au/sites/default/files/advisory-australian-export-sector-russian-sanctions-evasionithird-country-transhipment-hubs-shell-companies-end-users.pdf

55 Paul Esau, Red Flags in Real Cases: Enforcement and Evasion of Russia Sanctions, 6 October 2023, https://www.wisconsinproject.org/red-flags-in-real-cases-enforcement-and-evasion-of-russia-sanctions/ Copyright © 1999 – 2024. Wisconsin Project on Nuclear Arms Control

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

Product Red Flags

Although the spectrum of goods under export controls is vast, the alerts and guidance issued by authorities have highlighted certain categories as especially important. The direct export of military articles and services is obviously prohibited because of their utility on the Ukrainian battlefield. High-value luxury goods, such as real estate, aircraft, yachts, artwork, and precious metals, stones, and jewelry have also been targeted as means of imposing pain on Russian elites. Finally, computer chip and microelectronic controls have been identified as crucially important to slowing Russian military industry, especially production of missiles and UAVs.

- The product is at high risk of diversion because of its potential end use by a Russian military producer or in another sanctioned sector. See the "products of concern" lists.
- The product is at high risk of diversion because of its previous use in Russian munitions or military systems. See the "High Priority Items" list, including integrated circuits, capacitors, and wireless transceivers, because of their similarity to components in Russian systems recovered from the battlefield.
- The product is identified as a key component in the production of Iranian UAVs being used by the Russian military.
- Transactions use products identified as a disruptive technology or included on the dual-use lists.

Customer Red Flags

Since February 2022, escalating sanctions have forced Russian and Belarusian entities to both create new illicit supply chains and adapt existing chains to illicit purposes. Increasingly, new entities have

been incorporated or adapted to maintain the flow of military or dual-use products to sanctioned entities and to facilitate payment to suppliers.

- The customer is found on a sanctions list.
- A new customer whose line of business is in trade of products associated with the HS codes on the "High Priority Items" list, is based in a non-GECC country, and was incorporated after 24 February 2022.
- Transactions are related to payments for defense or dual-use products from a company incorporated after 24 February 2022, and based in a non-GECC country.
- The entity has a history of shipping to Russia or Belarus, even if the exported item is allegedly going to a non-sanctioned destination.
- An existing customer who did not receive exports associated with the HS codes on the "High Priority Items" list prior to 24 February 2022, is receiving such items now.
- An existing customer received exports associated with one or more of the HS codes on the "High Priority Items" list prior to 24 February 2022, and requested or received a significant increase in exports with those same codes thereafter.
- The entity has any connection with the Russian Federal Security Services (FSB), the Russian military, or to an entity owned by the Russian state. Russian or Belarusian entities occasionally display FSB certificates on the Russian language version of their websites to indicate that they are authorized to work on classified projects. The phrase "special purpose projects" may also be used as a designation for military use. State-linked companies often have the following designations within their business name: RAO, FGUP/FSUE, GK, SPRE/NIPP, and NPO/GNPO[56].
- The entity recently changed its name or was reincorporated.
- Change of ownership of a corporate holding reduces ownership stakes below the 50 percent threshold. Change of ultimate beneficial owner occurs shortly before or after sanctions were imposed.
- The entity recently purchased shipping vessels for no obvious business purpose. The entity is situated on a shipping corridor with access to sanctioned countries.[57]
- The nature of a customer's underlying business (specifically military or government-related work), type of service(s) or product(s) offered, and geographical presence pose additional risks of unintentional involvement in the evasion of export controls for Russia and Belarus.
- A customer purchases or sells vessels or other properties and goods identified as having been involved with or being blocked property under sanctions regulations.
- Transactions involve entities with little to no web presence, such as a website or a domain-based email account.
- Parties to transactions with addresses do not appear consistent with the business or are otherwise problematic (e.g., either the physical address does not exist, or it is residential).
- Transactions involve customers with phone numbers with country codes that do not match the destination country.
- Complex corporate or trust structures are linked to countries friendly to Russia or are presenting a complexity that is not

56 TRAO (Rossiyskaya Aktsionernaya Kompaniya) designates a Russian joint stock company; FGUP/FSUE (Federal'noye Gosudarstvennoye Unitarnoye Predpriyatiye) designates a Russian Federal State Unitary Enterprise; GK (Gorsudarstvennaya Korporatsiya) designates a Russian State Corporation; SPRE/NIPP (Nauchno-Issledovatel'skoye Proizvodstvennoye Predpriyatiye) designates a Russian Scientific Research Production Enterprise; NPO/GNPO (Gosudarstvennyy Nauchno-Proizvodstvennyy Tsentr) designates a Russian State Research and Production Center.

57 Old tankers may operate as part of a "ghost fleet" trafficking in Russian oil.

justified by the business profile of the customer. Trust arrangements or complex corporate structures involve offshore companies.
- Numerous transfers of shares from sanctioned entities to non-sanctioned entities involve corporations incorporated by the same individuals or entity (often with a registered office at the same physical address).
- Potential control of an entity is operated by a designated person, despite apparent direct ownership under the 50 percent threshold (member of Board of Directors, beneficial owner, managing director, other entities or persons on the ownership structure linked with a designated person);
- CEO/manager is never available for discussions, i.e., all communications go via a regular employee or a representative who seems to have a general Power of Attorney (PoA).

Network Red Flags

The most common method of sanction evasion is the use of front or shell companies, third-party intermediaries, and/or transshipment points to disguise the involvement of sanctioned entities or Russian end users. The use of networks of intermediaries allows sanctioned individuals or corporations to disguise both the destination of the purchased goods as well as the origin of payment for those goods.

- The entity involved in the transfer has a connection to a previously sanctioned person, company, or address.
- Not all entities involved in the transfer have a web presence. The alleged address does not correspond to a physical office.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

- An entity involved in the transfer is using a personal email address or home address.
- Transactions involve companies that are physically co-located with or have shared ownership with an entity listed on a sanctions list.
- The entity's order is similar in content and value to a previously rejected order from a different party.
- New or existing accounts and transactions by individuals with previous convictions for violating export control laws appear to involve export and import activities or services.
- There is a common set of financial institutions, individuals, or addresses linking multiple transactions to a sanctioned individual.
- Companies or individuals with links to Russian state-owned corporations (including shared ownership, as well as branches of, subsidiaries of, or shareholders in such state-owned corporations) are involved in export-related transactions or the provision of export-related services.
- Export transactions identified through correspondent banking activities involve parties that have shared owners or addresses with Russian state-owned entities or designated companies.
- The transaction does involve law firms in offshore financial locations, especially those with historical connections to Russian elites.

Destination Red Flags

Since most strategic goods can no longer be shipped directly to Russia or Belarus, illicit transactions are often routed through transshipment points in other, less-scrutinized jurisdictions.

Common destinations for transshipment include Armenia, Brazil, China, Georgia, India, Kazakhstan, Kyrgyzstan, Mexico, Nicaragua, Serbia, Singapore, South Africa, Taiwan, Tajikistan, Turkey, United Arab Emirates (UAE), and Uzbekistan. Countries such as Armenia, Brazil, China, India, Nicaragua, Turkey, and Uzbekistan have been particularly reluctant to increase export monitoring and enforcement, making them favorable vectors for sanctions evasion. Many countries proximate to Russia, including Armenia, Kazakhstan, and Turkey have experienced exponential growth in imports and exports of electronics and other sanctioned goods – indicating the increased importance of those countries to the Russian market.

- The exported item is being shipped or delivered to a common transshipment point or by an abnormal route.
- Transactions are associated with atypical shipping routes for a product and destination.
- A customer in the maritime industry transports commodities of concern and uses trade corridors known to serve as possible transshipment points or circumvention hubs for exports to Russia and Belarus.
- A bank or financial institution is listed as the item's final destination.
- Transactions involve freight-forwarding firms[58] that are also listed as the product's final end customer, especially items going to traditional Russian transshipment hubs.

58 A freight forwarder is a person or company that loads, or charters and loads, any form of transport or a person whose business is to receive and forward goods. The goods are often sent in a container for multimodal transport.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

Transaction Red Flags

Since most strategic goods can no longer be shipped directly to Russia or Belarus, illicit transactions are often routed through transshipment points in other, less-scrutinized jurisdictions.

- The entity prefers to pay cash for an item that would usually be financed.
- When combined with other derogatory information, large dollar or volume purchases, including through the use of business credit cards, of items designated as EAR99 (or large volume or dollar purchases at wholesale electrical/industrial merchants, electrical parts and equipment providers, or electronic parts providers), in the United States or abroad, especially if paired with purchases at shipping companies.
- Transactions involving smaller-volume payments from the same end user's foreign bank account to multiple, similar suppliers of dual-use products.
- The customer is significantly overpaying for a commodity based on known market prices.
- The entity attempts last-minute changes to shipping instructions that seem to contradict customer history or previous practice.
- The invoice or other business documents have been altered to obscure the ultimate customer.
- The buyer has declined routine maintenance for the purchased commodity.
- The payment is coming from a third-party country or business.
- The entity is purchasing small numbers of dual-use products from multiple, similar suppliers.

- The entity undervalues, or asks to undervalue, the purchase price on shipping documentation.
- Transactions involve a change in shipments or payments that were previously scheduled to go to Russia or Belarus, or a company located in Russia or Belarus, but that are now going to a different country/company.
- Transactions involve payments being made from entities located in third-party countries not otherwise involved with the transactions and known to be a potential transshipment point for exports to Russia and Belarus.
- Last-minute changes occur to transactions associated with an originator or beneficiary located in Russia or Belarus.
- Transactions involving consolidated shipments of luxury goods that previously would have been destined for Russia or Belarus, but are now destined for a transshipment country or a country without restrictions on exports/re-exports to Russia or Belarus.
- Transactions involving restricted luxury goods are rapidly shifted to new purchasers.
- Business checking or foreign exchange accounts are used by merchants in the import and export of electronic equipment where transactions are conducted with third-country-based electronics and aerospace firms that also have offices in Russia or Belarus.
- Transactions identified through correspondent banking activities are connected to Russian petroleum-related firms or firms that resell electronics and other similar items to Russian firms.
- Transactions use open accounts/open lines of credit when the payment services are conducted in conjunction with known transshipment jurisdictions.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

- Transactions involve payments being made from entities located at potential transshipment points or involve atypical shipping routes to reach a destination.
- Indirect transactions (such as those using intermediaries, shell companies etc.) that make no or little economic sense.
- Assets previously associated with a sanctioned person are oved by family members or otherwise on their behalf.

End-Use Red Flags

Exporters of controlled goods are generally required to follow due diligence obligations in researching potential customers and how they will use the goods. In many cases, the ultimate consignee is required to sign an “End User Statement” explaining the final purpose of the good and promising to notify the supplier before any re-export. End User Statements are an essential source of red flags for exporters.

- The alleged end use matches historical patterns of evasion.
- Parties to transactions listed as ultimate consignees or listed in the “consign to” field do not typically engage in business consistent with consuming or otherwise using commodities (e.g., other financial institutions, mail centers, or logistics companies).
- The customer or purchasing agent is reluctant to answer questions about the end use of the item.
- A customer lacks or refuses to provide details to banks, shippers, or third parties, including about end users, intended end-use, or company ownership.

- The item is incompatible with the stated end use.
- The item is more sophisticated (advanced) than needed for the stated end use.
- Purchases under a letter of credit are consigned to the issuing bank, not to the actual end-user. In addition, supporting documents, such as a commercial invoice, do not list the actual end-user.
- Parties to transactions listed as ultimate consignees or listed in the “consign to” field appear to be mail centers, trading companies, or logistics companies.
- The item (commodity, software or technology) does not fit the purchaser’s line of business.
- Transactions involve a purported civil end-user, but basic research indicates the address is a military facility or co-located with military facilities in a country of concern.

Consideration of these indicators, in conjunction with conducting appropriate risk-based customer and transactional due diligence, will assist in determining whether an identified activity may be connected to export control evasion. As no single financial red flag is necessarily indicative of illicit or suspicious activity, all the surrounding facts and circumstances should be considered before determining whether a specific transaction is suspicious or associated with potential export control evasion.

Such reasonable steps should not, however, put into question a financial institution’s ability to maintain or continue appropriate relationships with customers or other financial institutions and should not be used as the basis to engage in wholesale or indiscriminate de-risking of any class of customers or financial institutions.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

C. „No Re-Export to Russia“ contractual clause

Especially when exporting goods subject to restrictions, exporters need to know their counterparts and how reliable they are. They should include, in particular, contractual clauses with their third-country business partners prohibiting further re-exports of the items to Russia and Belarus. For example, such a clause may oblige the importer in third countries not to export the concerned goods to Russia or Belarus, and not to resell the concerned goods to any third-party business partner unless that partner commits not to export the concerned goods to Russia or Belarus.

Banks should verify that their customers are implementing such no re-export clauses in their export business. It is vital that the contractual clause gives rise to liability and can be enforced under the law applicable to the contract. The clause may also entail ex post verifications, and may be identified an essential element of the contract.

Article 12g of the Council Regulation (EU) 833/2014 aims to combat the circumvention of EU export bans and more specifically the situation where goods exported to third countries are re-exported to Russia. Article 12g turns the no re-export clauses into a legal requirement for certain sensitive goods, improving legal certainty in the context of business negotiations and relations.
Concretely, Article 12g obliges EU exporters to insert a „no re-export to Russia“ clause in their export/sale/supply/transfer or similar contracts. This applies only to specific types of sensitive goods, including goods related to aviation, jet fuel (Annexes XI, XX to the Regulation), firearms (Annex XXXV to the Regulation, as well as Annex I to Regulation (EU) 258/2012) and common high priority items1 (Annex XL to the Regulation).

Exporters should not sell their products to any non-EU operator that is not ready to incorporate a “no re-export to Russia” clause in contracts falling under the scope of Article 12g. Banks should verify that their customers are complying with this prohibition.

Due diligence measures that exporters and importers are advised to take (and that banks should verify) are, for instance, the introduction in import and export contracts of provisions destined to ensure that any imported or exported goods are not covered by the restrictions. These may take the form of e.g. a statement that the respect of such provision is an essential element of the contract, or of contractual clauses committing the importer in third countries not to export the concerned goods to Russia or Belarus, and not to resell the concerned goods to any third-party business partner that does not take a commitment not to export the concerned goods to Russia or Belarus giving rise to liability in case the latter re-exports the items to those countries.”

EU exporters’ contracts must comply with the obligation in Article 12g prior to or at the latest at the time of the export, sale, supply or transfer of the relevant goods to a third country. Exporters should be able to prove this if requested by their competent authorities. Moreover, paragraph 4 of Article 12g requires exporters to inform their national competent authorities as soon as they become aware of a breach or circumvention of the “no re-export to Russia” clause.

The obligation to include the “no re-export to Russia“ clause depends on the contract’s date of conclusion. Contracts concluded before 19 December 2023 benefit from a one-year transition period until 19 December 2024 included or until the contracts’ expiry, whichever is earliest. For any execution of these contracts as of 20 December 2024, they need to be amended to include the “no re-

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

export to Russia” clause. Contracts concluded as of 19 December 2023 must contain the “no re-export to Russia” clause as of 20 March 2024.

The obligation to include a “no re-export to Russia“ clause applies to contracts with operators based in any non-EU country, with the exception of the U.S., Japan, UK, South Korea, Australia, Canada, New Zealand, Norway and Switzerland.

To ensure its effectiveness, the „no re-export to Russia” clause must contain adequate remedies to be activated in case of its breach. These remedies should be reasonably strong and aim to deter non-EU operators from any breaches. They can include, for instance, termination of the contract and the payment of a penalty.

Operators are free to choose the appropriate wording for the “no re-export to Russia” clause, as long as the outcome fulfils the requirements of Article 12g. In any event, it is recommended that the clause is identified as an essential element of the contract.

While it does not preclude the use of other wordings, the template below can be considered as meeting the obligation in Article 12g. It is recommended in particular for contracts with non-EU operators doing business in jurisdictions seen as posing a high risk of circumvention.

- “(1) The [Importer/Buyer] shall not sell, export or re-export, directly or indirectly, to the Russian Federation or for use in the Russian Federation any goods supplied under or in connection with this Agreement that fall under the scope of Article 12g of Council Regulation (EU) No 833/2014.

(2) The [Importer/Buyer] shall undertake its best efforts to ensure that the purpose of paragraph (1) is not frustrated by any third parties further down the commercial chain, including by possible resellers.

(3) The [Importer/Buyer] shall set up and maintain an adequate monitoring mechanism to detect conduct by any third parties further down the commercial chain, including by possible resellers, that would frustrate the purpose of paragraph (1).

(4) Any violation of paragraphs (1), (2) or (3) shall constitute a material breach of an essential element of this Agreement, and the [Exporter/Seller] shall be entitled to seek appropriate remedies, including, but not limited to: (i) termination of this Agreement; and (ii) a penalty of [XX]% of the total value of this Agreement or price of the goods exported, whichever is higher.

(5) The [Importer/Buyer] shall immediately inform the [Exporter/Seller] about any problems in applying paragraphs (1), (2) or (3), including any relevant activities by third parties that could frustrate the purpose of paragraph (1). The [Importer/Buyer] shall make available to the [Exporter/Seller] information concerning compliance with the obligations under paragraph (1), (2) and (3) within two weeks of the simple request of such information."

Digitizing Internal Processes For Export Control Compliance

Digitization can significantly enhance the efficiency and effectiveness of banks' compliance efforts while mitigating the risk

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

of non-compliance.

Adopting RegTech solutions specifically designed for export control compliance can help banks automate compliance-related processes, such as screening, monitoring, and reporting. These solutions can streamline regulatory reporting requirements, generate compliance reports, and facilitate regulatory audits, thereby reducing the burden on compliance teams and improving overall efficiency.

Perform training and awareness-raising activities

Training and awareness raising are indispensable components of effective export control compliance for banks. By investing in comprehensive training programs, banks not only fulfill their regulatory obligations but also strengthen their risk management practices, safeguarding both their interests and the broader national security objectives.

Training programs help bank staff comprehend the intricacies of export control regulations, enabling them to make informed decisions in their day-to-day operations. Banks should empower their employees to recognize potential compliance risks and take appropriate measures to mitigate them. This proactive approach not only protects the bank's interests but also contributes to the broader national security objectives.

Heightened awareness ensures that red flags are promptly identified and escalated for further investigation, thereby reducing the risk of inadvertently facilitating illicit activities.

Compliance with export control regulations should be ingrained within the organizational culture of banks. Regular training sessions and awareness campaigns serve to reinforce the importance of compliance among employees at all levels. By fostering a culture of compliance, banks demonstrate their commitment to upholding regulatory standards and ethical business practices. Training programs should also enable bank staff to stay ahead of the evolving threats by providing them with up-to-date information on emerging risks, trends, and best practices in export control compliance.

Complete Performance Reviews, Audits, Reports And Corrective Actions

To fulfil their responsibility as crucial gatekeepers in international trade, banks must establish robust mechanisms for performance reviews, audits, reports, and corrective actions.

Regular performance reviews are essential for evaluating the effectiveness of a bank‘s export control compliance program.

Banks should conduct comprehensive assessments to gauge the adherence of their staff to regulatory requirements and internal policies. These reviews help identify areas of strength and weakness, allowing banks to implement targeted improvements to enhance compliance measures.

Independent audits provide an objective evaluation of a bank‘s export control compliance processes and procedures. Banks should engage external auditors with specific “export control” related expertise in regulatory compliance to conduct thorough

assessments of their compliance programs. Audit findings offer valuable insights into areas requiring attention or improvement, enabling banks to address deficiencies proactively.
Accurate and timely reporting is a cornerstone of effective export control compliance. Banks must maintain meticulous records of transactions, including those involving potentially sensitive goods or entities. Regular reporting to relevant regulatory authorities ensures transparency and accountability in the bank‘s operations. Additionally, internal reporting mechanisms enable the timely escalation of compliance issues for appropriate action.
When compliance deficiencies are identified through performance reviews, audits, or reports, banks must take prompt corrective actions. This may involve implementing remedial measures to address systemic weaknesses, conducting additional training for staff, or enhancing internal controls to prevent recurrence of compliance lapses. By taking decisive corrective actions, banks demonstrate their commitment to upholding regulatory standards and mitigating compliance risks.

Reporting

Pursuant to Article 12 of Council Regulation (EU) No 833/2014, it is prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent sanctions law. Operators should also remain vigilant of any attempts by third parties to draw them into circumvention schemes. These considerations apply regardless of which non-EU country the counterpart is based in. If you believe you are witnessing sanctions violations or circumvention, these should be reported to your national competent authority or anonymously via the EU whistle-blower tool.

In parallel, as soon as they become aware of a breach of Article 12g of Council Regulation (EU) 833/2014, exporters must inform the competent authority of the Member State where they are resident or established.

Banks should report any suspicious activity in the field of trade, in line with legal requirements, to the relevant national authority, such as financial intelligence units, customs and border authorities or relevant supervisory authority, if any.

Under U.S. law, EAR General Prohibition Ten (GP 10) bans proceeding with transactions with knowledge that a violation has occurred or is about to occur. Specifically, no person may sell, transfer, export, reexport, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR and exported, reexported, or transferred (in-country) or to be exported, reexported, or transferred (in-country) with knowledge that a violation of the Export Administration Regulations, the Export Control Reform Act of 2018, or any order, license, license exception, or other authorization issued thereunder has occurred, is about to occur, or is intended to occur in connection with the item.

Under the EAR, "knowledge" includes not only positive knowledge that the circumstance exists or is substantially certain to occur but also the awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. Merely having the information at your disposal gives you "reason to know" under the EAR "knowledge" standard, even if you never review the information.

APPLYING A RISK-BASED APPROACH TO TRADE FINANCE

Financial institutions that, for example, finance items "subject to the EAR" that are to be exported or transferred—with knowledge that a violation of the EAR or any order, license, or other authorization has occurred, is about to occur, or is intended to occur in connection with the item—could be in potential violation of GP 10[59]. The EAR also contain causing, aiding, or abetting and conspiracy enforcement provisions that could conceivably be brought against a financial institution under egregious circumstances[60].

The EAR assert jurisdiction based largely on the U.S. origin of the Item at issue in a transaction. EAR jurisdiction rarely relies on (a) the nationality of the individual or entity involved with the Item or (b) where the Item is currently located outside the United States. Therefore, BIS asserts enforcement authority against non-U.S. individuals and entities, wherever located, for transactions involving Items "subject to the EAR," wherever located.

Those persons (including financial institutions) that may have identified "significant" violations but "deliberately" chose not to voluntarily self-disclose them will see that fact work against them as an "aggravating" factor in any BIS enforcement action of those violations[61].

59 EAR, § 736.2
60 EAR, § 764.2(b) and (d)
61 https://www.bis.doc.gov/index.php/documents/enforcement/3262-vsd-policy-memo-04-18-2023/file

RespectUs

Chapter Seven

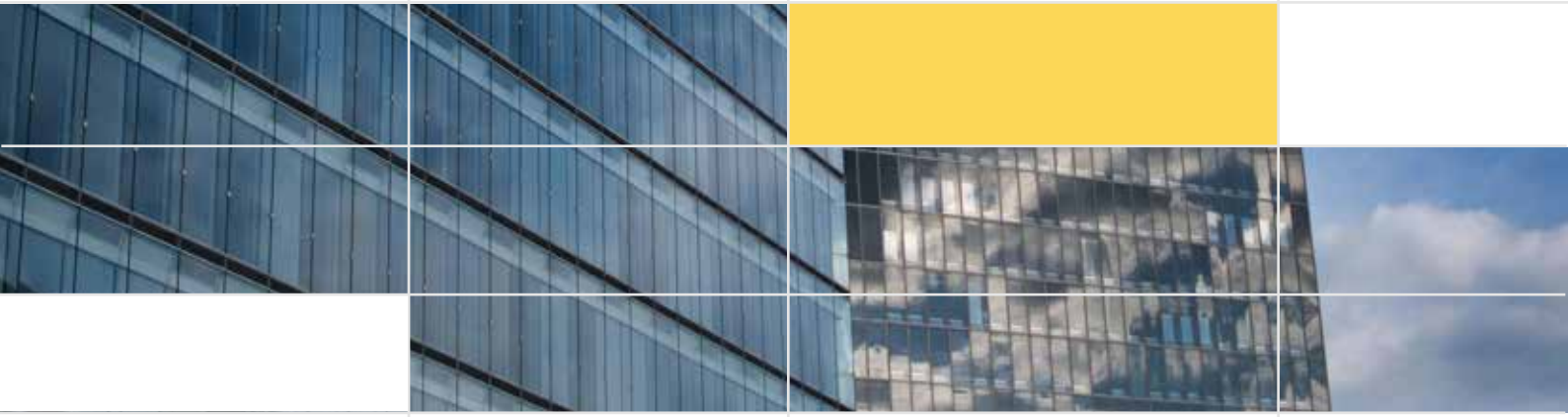
What Respectus Is Offering To Banks With Regard To Trade Compliance

RespectUs is the one-stop-shop digital platform for export control compliance, made in Luxembourg and validated by the European Space Agency in August 2023. A subscription to the platform allows users to:

1. Access export control legislations and regulations of up to 50 countries, in a version always up-to-date;
2. Classify products, software and technology according to military, dual-use and other control lists, with the purpose to determine if the specifications of different export control codes are fulfilled by the item under classification;
3. Determine if sanctions and other restrictive measures are prohibiting or submitting to a license requirement the export (or any other activity) of an item to a specific destination country, with the result displaying the precise legal text applying to the situation under assessment;
4. Operating a name check screening on a particular person, entity or vessel, with the result displaying, in case of a match, the restrictive measure (freeze of funds, immigration restrictions, export restrictions …) applicable to the entity under screening;
5. Documenting and maintaining a customer profile (KYC) centralizing in one place all information about a customer or a stakeholder in a transaction, including red flag questionnaires;
6. Assessing the end-use of the products or activity with the purpose to determine if the end-use is critical because related to proliferation, military use, or affecting human rights in the destination country or the national or international security of the country of export;
7. Operating a risk assessment, in order to determine the level of exposure to export violations or sanctions evasion;
8. Performing a license determination, meaning receiving for a particular product, customer, destination country and end-use, an information, based on the current applicable legislation, if a license is required or not.

Navigating new horizons in the world of
export control compliance solutions

Export Control Compliance Made Easy



Patrick GOERGEN
CEO & Founder

+352 27 39 85 20
+352 621 166 506
patrick.goergen@respectus.space

24 rue Léon Laval
L-3372 Leudelange
G.D. Luxembourg

Business Permit 10111778/2
RCS B238962
VAT LU31877869