

## Export Control Compliance:

## The Imperative for Banks and Financial Services Providers

By Patrick GOERGEN, Founder & CEO, RespectUS<sup>(1)</sup> (Luxembourg)

Part 1<sup>(2)</sup>

**I**n 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.<sup>(3)</sup>

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 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<sup>(4)</sup>. 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<sup>(5)</sup> to secondary sanctions risks when they conduct or facilitate certain Russia-related transactions, even unwittingly.

These new regulations are noteworthy not simply because they expose these financial institutions to new secondary sanctions risks based on the facilitation of trade of certain enumerated goods, and do so under a standard of strict liability.

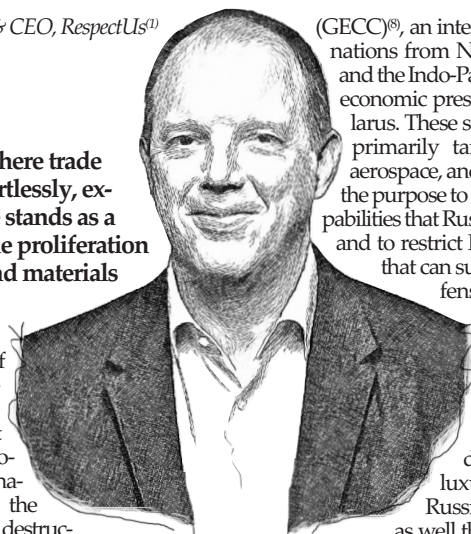
The European Union (EU) has as well chosen to close legal loopholes and improve effective implementation and enforcement of sanctions against Russia and Belarus, which have been strengthened after Russia's illegal full-scale invasion of Ukraine in February 2022. Violation of EU restrictive measures will 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<sup>(6)</sup>. The EU Commission has also issued a guidance to support EU operators' compliance efforts<sup>(7)</sup>.

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.

### 1 - Actions in response to the Russian invasion of Ukraine

Since February 2022, a coordinated international endeavor under the Global Export Control Coalition



(GECC)<sup>(8)</sup>, 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<sup>(9)</sup>.

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.<sup>(10)</sup>

The restrictions applied to Belarus are in response to its substantial enabling of Russia's war effort<sup>(11)</sup>.

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<sup>(12)</sup>.

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.

#### 1.1. 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.;
- 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<sup>(13)</sup> — a list of individuals and entities that have been denied export privileges;
- 2) Entity List<sup>(14)</sup> — 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;
- 3) Unverified List<sup>(15)</sup> — 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<sup>(16)</sup> — a list of foreign parties that are prohibited from receiving controlled items unless export license is granted;
- 5) Consolidated Screening List<sup>(17)</sup> — a list of parties for which the U.S. Government maintains restrictions on certain exports, reexports or transfer of items.

#### 1.2. 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<sup>(18)</sup> 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. Specific export restrictions targeting Russia are delineated in Council Regulation (EU) No. 833/2014<sup>(19)</sup>. 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<sup>(20)</sup>; energy-related items<sup>(21)</sup>; items which might contribute to Russia's military and technological enhancement, or the development of the defense and security sector<sup>(22)</sup>; goods and technology suited for use in oil refining and liquefaction of natural gas<sup>(23)</sup>; items aimed for use in aviation or the space industry<sup>(24)</sup>; maritime navigation and radio-communication items<sup>(25)</sup>; luxury goods (items valued above EUR 300 per item)<sup>(26)</sup>; jet fuel and fuel additives<sup>(27)</sup>; an extensive list of items which could contribute in particular to the enhancement of Russian industrial capacities<sup>(28)</sup>; banknotes denominated in any official currency of an EU Member State; and firearms, their parts and essential components and ammunition<sup>(29)</sup> and firearms and other arms<sup>(30)</sup>.

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<sup>(31)</sup>, the negotiation or arrangement of financial services has been specifically included, in the Russia sanctions regulation, in the definition of "brokering services"<sup>(32)</sup>.

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"<sup>(33)</sup>.

#### 2 – 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<sup>(34)</sup>. 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<sup>(35)</sup>.

According to an analysis by the KSE Institute<sup>(36)</sup>, Russia continues to be able to import large amounts of goods needed for military production. 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. A common tactic used by illicit actors to evade Russia-related sanctions and export controls consists in using third-party intermediaries and transshipment points<sup>(37)</sup>.

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)<sup>(38)</sup>, 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<sup>(39)</sup>.

#### 3 – 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.

#### 3.1. 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. It has issued a list of commodities that present special concern and sought by or prohibited for end-users in Russia and Belarus.<sup>(40)</sup> All of these items 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 list can assist in the risk-based screening of export-related financial transactions.

The list contains aircraft parts / equipment (ECCN 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), spectrophotometers (3A999), test equipment (3B992), thrusters (8A992), underwater communications (5A991), vacuum pumps (2B999), water fabrication equipment (3B001, 3B991) and wafer substrates (3C00x).

#### 3.2. 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<sup>(41)</sup> 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).

#### 3.3. 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<sup>(42)</sup>, 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. 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.

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<sup>(43)</sup> 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 current version (February 2024) contains among others electronic integrated circuits, radio navigational aid apparatus, fixed capacitors, static converters, television and digital cameras, transistors, semiconductor devices, ball bearings, navigational instruments and appliances, units for automatic data-processing machines, printed circuits, signal generators, oscilloscopes, oscillographs, multimeters with recording device.<sup>(44)</sup>

#### 3.4. 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<sup>(45)</sup>. The list, referring to the 10-digit customs code, contains automotive components (83 entries), bearings and transmission shafts (31), communications equipment (80), computer components (15), drones (5), electric and electronic equipment (159), navigation equipment and sensors (62), semiconductors (37) and other components (13).<sup>(46)</sup>

#### 3.5. U.S. Disruptive Technology

On 16 February 2023, the U.S. authorities announced the formation of a Disruptive Technology Strike Force<sup>(47)</sup>. 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.

Continued on right page