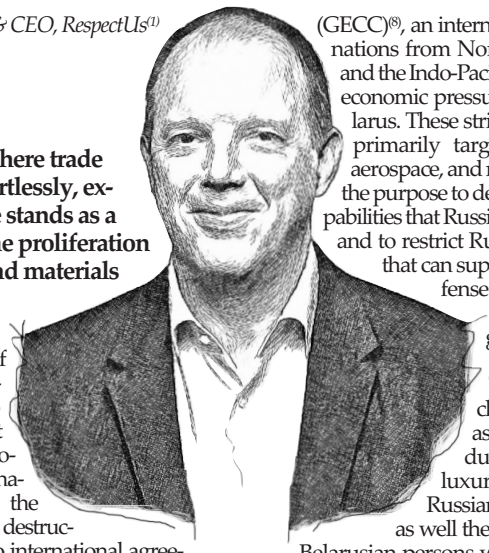
Export Control Compliance:

The Imperative for Banks and Financial Services Providers

By Patrick GOERGEN, Founder & CEO, RespectUs[1] (Luxembourg)

Part 1[2]

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.[3]

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[4]. 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[5] 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[6]. The EU Commission has also issued a guidance to support EU operators' compliance efforts[7].

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)[8], 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[9].

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.[10]

The restrictions applied to Belarus are in response to its substantial enabling of Russia's war effort[11].

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[12].

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[13] —a list of individuals and entities that have been denied export privileges;
2) Entity List[14] —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[15] —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[16] —a list of foreign parties that are prohibited from receiving controlled items unless export license is granted;
5) Consolidated Screening List[17] — 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[18] 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[19]. 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[20]; energy-related items[21]; items which might contribute to Russia's military and technological enhancement, or the development of the defense and security sector[22]; goods and technology suited for use in oil refining and liquefaction of natural gas[23]; items aimed for use in aviation or the space industry[24]; maritime navigation and radio-communication items[25]; luxury goods (items valued above EUR 300 per item)[26]; jet fuel and fuel additives[27]; an extensive list of items which could contribute in particular to the enhancement of Russian industrial capacities[28]; banknotes denominated in any official currency of an EU Member State; and firearms, their parts and essential components and ammunition[29] and firearms and other arms[30].

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[31], the negotiation or arrangement of financial services has been specifically included, in the Russia sanctions regulation, in the definition of "brokering services"[32].

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"[33].

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[34]. 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[35].

According to an analysis by the KSE Institute[36], 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[37].

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)[38], 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[39].

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.[40] 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[41] 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[42], 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[43] 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.[44]

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[45]. 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).[46]

3.5. 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.

Continued on right page

Continued on left page

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

4 – 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:

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. 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".

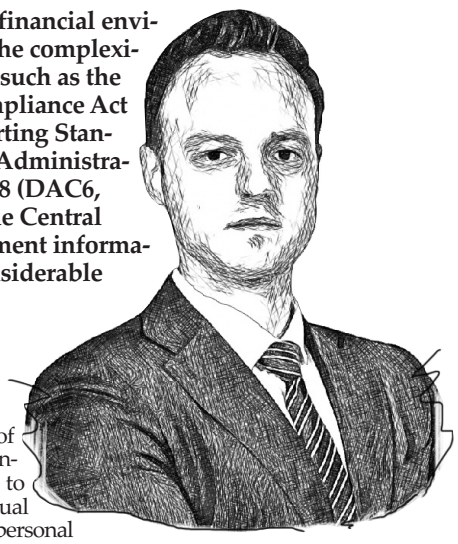
However, financial institutions generally do not have the required internal expertise in qualifying tangible/intangible items, software or technologies as being export controlled.

PART 2 - Continue the reading in AGEFI Luxembourg May 2024 with the following chapter:
5. Applying a risk-based approach to Trade Finance

1) RespectUs is a Luxembourg start-up, graduated from Fit4Start (9th ed., 2020) in the space vertical. It has built a digital one-stop-shop digital platform for export control compliance (www.respectus.eu), in the frame of the Luxembourg national space programme LuxIMPULSE (2021-2023) through an ESA contract. The software has been validated by the European Space Agency in August 2023. Web www.respectus.space
2) Part 2 will be published in the May 2024 edition of AGEFI. The complete eBook "Export Control Compliance: The Imperative for Banks and Financial Services Providers", may be downloaded under the link https://respectus.space/knowledge-hub/
3) The White House, Background Press Call on Upcoming Action to Continue Holding Russia Accountable. 21 December 2023, https://lc.cx/E4WNtM
4) 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://lc.cx/YAS-bc; 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://lc.cx/nnENlz; 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://lc.cx/LoXPqc.
5) 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.
6) See: "Commission welcomes political agreement on new rules criminalizing the violation of EU sanctions", Press release, 12 December 2023, https://lc.cx/_KG_6E
7) European Commission, Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention, December 2023, https://lc.cx/mjRolL
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 White House, "Executive Order on Prohibiting Certain Imports, Exports, and New Investment with Respect to Continued Russian Federation Aggression," (11 March 2022)
10) See BIS Press Release, "Commerce Restricts the Export of Luxury Goods to Russia and Belarus and to Russian and Belarusian Oligarchs and Malign Actors in Latest Response to Aggression Against Ukraine," (11 March 2022).
11) See BIS Press Release, "Commerce Imposes Sweeping Export Restrictions on Belarus for Enabling Russia's Further Invasion of Ukraine," (2 March 2022)
12) See BIS Press Release, "Commerce Imposes Additional Export Restrictions in Response to Russia's Brutal War on Ukraine" (24 February 2023).
13) Accessible under the link https://lc.cx/k5x7e9
14) Supplement 4 to Part 744 of the EAR
15) Supplement 6 to Part 744 of the EAR
16) Supplement 7 to Part 744 of the EAR
17) Accessible under the link www.trade.gov/consolidated-screening-list
18) 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
19) 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
20) as listed in Annex I to EU Dual-Use Regulation 2021/821
21) as listed in Annex II to Regulation (EU) 833/2014
22) as listed in Annex VII to Regulation (EU) 833/2014
23) as listed in Annex X to Regulation (EU) 833/2014
24) as listed in Annex XI to Regulation (EU) 833/2014
25) as listed in Annex XVI to Regulation (EU) 833/2014
26) as listed in Annex XVIII to Regulation (EU) 833/2014
27) as listed in Annex XX to Regulation (EU) 833/2014
28) as listed in Annex XXIII to Regulation (EU) 833/2014
29) 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
30) as listed in Annex XXXV to Regulation (EU) 833/2014
31) 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
32) 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..
33) 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.
34) 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).
35) 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).
36) 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://lc.cx/pHuHlr
37) 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).
38) See OFAC, "Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists"
39) See December 2022 BIS Enforcement Action
40) 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.
41) Economically Critical Goods List (Version of 18 October 2023): https://lc.cx/1a0GJ6.
The complete list is also published in the eBook "Export Control Compliance: The Imperative for Banks and Financial Services Providers", that may be downloaded under the link https://respectus.space/knowledge-hub/
42) 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.
43) List of Common High Priority Items (Version of February 2024) : https://lc.cx/s34d5D.
44) The complete list is published in the eBook "Export Control Compliance: The Imperative for Banks and Financial Services Providers", that may be downloaded under the link https://respectus.space/knowledge-hub/
45) 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://lc.cx/BAtFz5
46) The complete list is published in the eBook "Export Control Compliance: The Imperative for Banks and Financial Services Providers", that may be downloaded under the link https://respectus.space/knowledge-hub/
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).
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

Navigating through operational tax complexities

In the dynamic global financial environment, navigating the complexities of tax regulations such as the Foreign Account Tax Compliance Act (FATCA), Common Reporting Standard (CRS), Directive on Administrative Cooperation 6, 7 and 8 (DAC6, DAC7 and DAC8), and the Central Electronic System of Payment information (CESOP) present considerable challenges.



Challenge #1 – Evolving regulations

Since the entry into force of DAC7, each Luxembourg financial institution (FI) is required to notify each reportable individual in the scope of CRS that their personal and financial information will be gathered and transmitted in accordance with the law. In this context, personal information refers to individual data such as name, address, jurisdiction of tax residency/residencies, and tax identification number, while financial information refers to the total gross amount paid or credited, and/or the value of the debt or equity position within the financial institution at the end of the calendar year or another relevant reference period.

Reporting FIs must notify their individual clients and the controlling persons of passive non-financial entity clients subject to reporting under CRS about their personal and financial information which will be reported to the Luxembourg tax authority. This notification should be performed every year prior to the exchange of information with the authorities.

In addition, the FI must provide those individuals with details about how to request the data controller, and also provide access to the information within a reasonable timeframe. If required, they will also allow the individuals to exercise their data protection rights. This requirement must be met before any information is shared with the Luxembourg tax authority.

During the year 2023, the following five jurisdictions were added to the list of reportable jurisdictions: Jamaica, Moldova, Montenegro, Thailand, and Uganda. Other participating jurisdictions, such as Kenya, Rwanda, Ukraine, may also be added to the list of reportable jurisdictions.

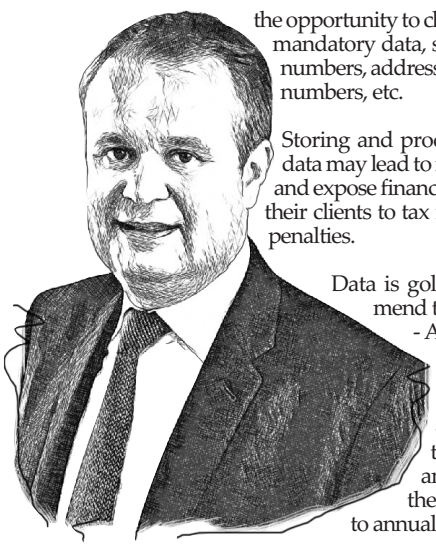
In this evolving context we recommend that:
- The notification process be integrated within the existing reporting process.
- Financial institutions remain informed about any modifications in reporting requirements and update their systems and processes for reporting preparation accordingly.

Challenge #2 – Data quality

To meet all the necessary data standards and legal requirements, Luxembourg financial institutions collect, maintain, and process data. It is critical for FIs to maintain a high level of data accuracy, and for that purpose, internal and external checks must be performed.

To support FIs in their duties, the OECD, the IRS and the European Commission websites provide the opportunity to check plausibility of mandatory data, such as foreign tax numbers, addresses, GIIN, and VAT numbers, etc.

Storing and processing inaccurate data may lead to incorrect reporting and expose financial institutions and their clients to tax investigations and penalties.



Data is gold and we recommend that:
- A full data check be carried out from data collection to report submission.
- Financial institutions continually analyze and clean their data leading up to annual filing.

Challenge #3 – Complexity

It is important to mention that the (Automatic Exchange of Information (AEOI) requirements are closely related to Anti-Money Laundering (AML) rules, the Anti-Tax Avoidance Directive 2 (ATAD 2), and the General Data Protection Regulation (GDPR). In addition to the regulations mentioned earlier, DAC8, a new directive, was issued in October 2023. This Directive focuses on imposing transaction reporting obligations on crypto-asset service providers, but it also extends its reach to existing directives, particularly DAC2 (CRS) and DAC6 (Mandatory Disclosure Regime).

A critical aspect of simplifying this complexity is ensuring data accuracy and integrity.

Tax topics cannot be handled in silos and we recommend that:
- Financial institutions develop and execute a comprehensive strategy that addresses these interconnected aspects of global finance.
- They continuously improve data security measures to maintain compliance.

Challenge #4 – Governance

Policies and procedures must be well documented, and FIs must remain informed about filing deadlines and changes to reporting requirements and schemes.

FIs must also be prepared to respond to various type of inquiries from tax authorities regarding data exchanged, governance and compliance programs, and evidence on proper tax data management.

Based on the statistics provided by the tax authority (*Administration des contributions directes* (ACD)), the penalties are more than doubling on a yearly basis and increased by 398% between 2021 and 2023. This confirms the increased scrutiny of the authorities and that penalties for instances of non-compliance are not only a possibility but a reality.

Years	2021	2022	2023
Fines	108	177	216
Penalties	441 000	950 000	2 197 050
	-	+115% vs previous year	+131% vs previous year

These facts highlight the importance of investing the right effort and means to properly manage AEOI regulations. The operational challenges to comply with tax regulations such as FATCA, the DACs, and CESOP should not be underestimated.

Regulations are transversal topics and multi-disciplinary teams should be involved. Various stakeholders, such as banks, financial institutions, digital platforms, and crypto-asset service providers should remain pragmatic when putting in place procedures and defining their target operating models.

Due to high level of specialization of key players, outsourcing of operational tax duties is also part of the possible robust approaches to tackle these challenges.

Dan ZANDONA
EY Luxembourg Partner,
FSO Tax, Business Tax Services

Patrice FRITSCH
EY Luxembourg Partner,
Tax