Sanctions against Russia for the aerospace industry

COMPLIANCE CHALLENGES AND STRATEGIES FOR ORIGINAL EQUIPMENT MANUFACTURERS IN PREVENTING DIVERSION AND CIRCUMVENTION.

C.A.J.M. Delescen
EXECUTIVE MASTER IN CUSTOMS AND SUPPLY CHAIN COMPLIANCE

THE COST OF NOT DOING BUSINESS

Thesis for the executive Master in Customs and Supply Chain Compliance (MCSCC)

Date:	30 March 2025
Author:	Christine Delescen
Student nr.	573115
Academic supervisor:	Ruud Tusveld
Co-reader:	Albert Veenstra
University:	Rotterdam School of Management Erasmus University

NOTE

This document solely represents the views and opinions of the author and does not necessarily reflect the opinion of one specific company or industry participant.

Executive summary

Sanctions imposed on Russia by the EU and U.S. since 2014, which intensified in 2022, have created a complex regulatory landscape for businesses. These sanctions aim to weaken Russia's economy by restricting access to critical technologies, items and markets, thereby limiting its military capabilities.

Since March 2022, regulations have evolved, with governments taking stronger stances on supply chain accountability. A key development has been the focus on circumvention and diversion to close loopholes and ensure sanctions effectively limit Russia's military operations. This shift requires export control and sanctions departments to monitor activities beyond export control classifications, including post-export activities outside the companies' direct control, adding unprecedented complexity.

This thesis evaluates how effectively aerospace companies, specifically Original Equipment Manufacturers (OEMs) can comply with the sanctions against Russia, particularly concerning diversion and circumvention. Literature highlights that the effectiveness of sanctions depends on the regulatory environment, including the clarity of instructions and the capacity to monitor and enforce regulations.

A comparative analysis reveals that aerospace OEMs need a comprehensive approach covering both EU and U.S. regulations due to significant differences between the two jurisdictions. Most companies comply with U.S. regulations out of fear of fines and being shut out of the U.S. market. The regulatory differences pose significant challenges for OEMs in implementing export control and compliance programs, which are not easily adapted to new regulations. Modifying systems and procedures to fast changing regulations, such as those related to sanctions on Russia, presents an additional challenge.

Through semi-structured interviews, qualitative data on the practical challenges and strategies employed by OEMs to prevent diversion of aerospace items and circumvention of sanctions, provide insights into their current compliance practices and challenges. All four OEMs interviewed rated the impact of the restrictive measures on Russia as high, citing the unprecedented volume and complexity of the regulations. Understanding and implementing the regulations involved considerable resources, and the impact on IT systems and processes has been substantial. Compliance departments have had to prioritize sanctions on Russia, often at the expense of other projects. Companies with business units in different EU countries noted that customs authorities reacted differently to the sanctions, leading to inconsistencies. OEMs adapted by implementing stricter compliance based on risk assessments, resulting in blocking more potential new customers and transactions. Banks have become more conservative, making it difficult for some OEMs to receive payments. Increased compliance requirements amongst suppliers are causing common customers to lose support of spare parts and documentation, leading to operational issues for airlines, potentially affecting safety.

Companies are unsure if their measures were too drastic, as they have negative consequences for airlines. The constant shifting of priorities and the risk of alienating customers due to drastic measures remain significant challenges. While the implementation of the measures was feasible, it came at a significant cost to the companies involved. Compliance was mostly achievable but not entirely reasonable or realistic due to the high complexity, frequent updates, and unclear guidelines. These factors resulted in unreasonable resource demands, operational disruptions, and potential loss of future business.

Preface

This thesis marks the culmination of a long journey that began in 2020 when I embarked on the Executive Master in Customs and Supply Chain Compliance during the first COVID-19 lockdown. Although I have a background in export controls, sanctions, and compliance, adding customs and supply chain to my expertise seemed a logical choice, as these regulations often intersect.

It has been an interesting and transformative time. I vividly remember the excitement of starting a new study and am grateful for the engaging lectures and the people I met. Due to the COVID-19 pandemic, we transitioned to a combination of virtual and in-person classes. It was a joy to meet other students from customs departments and various businesses and to collaborate together. During this period, I lost my job of 23 years due to COVID-19 reorganizations, found a new job—thanks in part to starting this master's program—and faced a serious illness that took a long time to recover from.

The choice of this thesis topic stems from its current relevance. It aims to provide businesses and authorities with insights into how restrictive measures affect the parties responsible for implementing them. Writing this thesis has been an enlightening journey, both personally and professionally. I realized that implementing restrictive measures such as sanctions involves not only business considerations but also personal values, and even with the best intentions, questions remain. I was intrigued by how different regulations intersect and yet sometimes oppose each other. I believe that better business decisions can be made when one is aware of these contradictions and their consequences.

Throughout my research, I encountered as many questions as answers. I have included some of these questions as suggestions for additional research, hoping that one day regulations will be clear enough that aerospace companies are no longer caught between export control & sanctions and safety regulations.

I would like to express my heartfelt gratitude to RSM for encouraging me to complete my thesis, especially after I nearly abandoned the idea due to illness. Special thanks to Mariapia Di Palma, whose firm yet kind reminders kept me on track. This thesis would not have been possible without the support and guidance from my supervisors, Ruud Tusveld and Albert Veenstra. I am also deeply grateful to all the interviewees who shared their experiences and insights and allowed me to ask follow-up questions.

Finally, I would like to express my gratitude to my friends and colleagues for their unwavering support and encouragement throughout my academic journey. I also acknowledge and thank my family, whose presence, despite the challenges, has been an integral part of this journey.

Chrianne Delescen

Table of Contents

List of tables and figures

List of abbreviations

AES	Automated Export System
AT	Anti-Terrorism
BIS	Bureau of Industry and Security
CAATSA	Countering America's Adversaries Through Sanctions Act
CCL	Commercial Control List
CD	Council Decision (EU)
CFSP	Common Foreign and Security Policy
CHPI	Common High Priority Items
CIR	Council Implementing Regulation (EU)
CISADA	Comprehensive Iran Sanctions, Accountability, and Divestment Act
CMM	Component Maintenance Manuals
CN	Common Nomenclature
CR	Council Regulation (EU)
DDTC	Directorate of Defense Trade Controls
DOJ	Department of Justice
DTP	Specific Tariff Provisions
EAR	Export Administration Regulation
EASA	European Union Aviation Safety Agency
EC	European Commission
ECP	Export Control Program
EEI	Electronic Export Information
EO	Executive Order
EU	European Union
EUS	End User Statement
FAA	Federal Aviation Administration (U.S.)
FAQ	Frequently Asked Questions
FDPR	Foreign Direct Product Rule
GP	General Prohibition
HS	Harmonized System
HTS	Harmonized Tariff Schedule
IEEPA	International Emergency Economic Powers Act
ITAR	International Traffic in Arms Regulations
ICA	Instructions for Continued Airworthiness
ICAO	International Civil Aviation Organization
ICP	Internal Compliance Program
IT	Information Technology
ITC	International Trade Commission
KYC	Know Your Customer
MEU	Military End User

MRO	Maintenance and Repair Organization
MSN	Manufacturer Serial Number
MTC	Mill Test Certificate
NGO	Non-Governmental Organization
NLR	No license required
OEM	Original Equipment Manufacturer
OFAC	Office of Foreign Assets Control
SDN	Special Designated National
TARIC	Tarif Intégré de la Communauté (Integrated Tariff of the European Communities)
TC	Type Certificate
TCH	Type Certificate Holder
TWEA	Trading with the Enemy Act
UAV	Unmanned Aerial Vehicle
UBO	Ultimate Business Owner
UK	United Kingdom
UN	United Nations
U.S.	United States
USD	U.S. dollar
USITC	United States International Trade Commission
USML	United States Munitions List
UTC	United Technologies Corporation
WCO	World Customs Organization

1 Introduction

1.1 Navigating turbulence: Impact of Western sanctions on Russia for the aerospace industry

In February 2022, the United States (U.S.), European Union (EU), and allies[1] imposed stringent sanctions in response to Russia's aggression against Ukraine, targeting both Russia and Belarus. These sanctions were in continuation of the sanctions introduced in July 2014 in response to Russia's actions destabilizing the situation in Ukraine. The initial measures taken in 2014, among other provisions, prohibited the direct or indirect import, export, or transfer of all defense-related material and established a ban on Dual Use[2] goods for military use or military end-users in Russia.

Escalation in 2022 and impact on the aerospace industry

Following Russia's invasion in Ukraine in 2022, more severe sanctions were published, aimed to restrict the flow of critical technologies and goods that could support Russia's military capabilities and its ongoing aggression. From the first combination of U.S. and EU sanctions, the aerospace industry in the U.S., EU, and allied countries, had to halt all exports of aircraft, parts, technologies, services and customer support to Russia and Belarus and was given only a brief wind-down period to cancel or suspend all contracts and activities. Although these sanctions on Russia were sectorial, for aerospace it was like an embargo.

Initially, it seemed straightforward: aerospace Original Equipment Manufacturers (OEMs[3]), leasing companies, Maintenance and Repair Organizations (MROs), and airline partners, adhering to sanctions, halted all exports and faced their losses on undeliverable equipment and materials in Russia that they couldn't retrieve, as the sanctions provoked immediate counter-sanctions from Russia, preventing the export of foreign-owned aircraft from Russia. This left Western aircraft lessors with about 400 aircraft struck in Russia without a way to get them back. With losses over $10 billion, aircraft owners and lessors are suing insurers and reinsurers.[4]

Meanwhile, many countries do not actively support sanctions against Russia and have shown little interest in respecting them. They use various techniques to circumvent these sanctions, increasing the risk for companies to inadvertently facilitate prohibited activities.

[1] The sanctioning countries in 2022 include Albania, Australia, Bahamas, Canada, EU 27, Iceland, Japan, Korea, Liechtenstein, Montenegro, New Zealand, North Macedonia, Norway, Singapore, Switzerland, Taiwan, the United Kingdom, and the U.S.
[2] Dual Use items are goods, software and technology that can be used for both civil and military purposes. They do not include items of a purely military nature, such as those listed in the EU Common Military List (OJ C 72, 28.2.2023, p. 2–37).
[3] In aerospace, an OEM (Original Equipment Manufacturer) is a company responsible for the design, production, and assembly of aircraft or their components, holding the intellectual property rights for the designs, including all related data, manuals, and schematics. Parts produced by OEMs or their authorized suppliers adhere to specifications and standards established by the aircraft manufacturer and are typically approved by aviation regulatory authorities such as the Federal Aviation Administration (FAA) in the U.S. or the European Union Aviation Safety Agency (EASA) in the EU.
[4] "The Russian Aviation Litigation." *Stewarts*, 30 Jan. 2025, www.stewartslaw.com/news/the-russian-aviation-litigation/.

Russia's civil air fleet is overwhelmingly reliant on Western manufactured airframes and engines. Around 700 out of Russia's 900 aircraft designed for civil aviation are affected by the sanctions[5]. Of the 700 aircraft, just under 650 are either Airbus' or Boeings, split between the two aircraft manufacturers. Two-and-a half years into the conflict, some 530 of these aircraft are still in service. Despite Western sanctions, Russian airlines are limiting the expected reduction in air traffic by maintaining aircraft in operation thanks to spare parts obtained through alternative channels[6]. According to Russia's Air Operators Association, 89% of the country's passengers in 2023 were still carried aboard foreign-made aircraft[7].

Between February 2022 and February 2023, $14 billion worth[8] of aircraft parts ended up with Russian airlines, and military and Dual Use[9] items were discovered on the battlefield on the Russian side. It appears that many companies from coalition countries continue to supply billions of dollars' worth of critical goods to third countries, from where these goods eventually make their way to Russia. $8.8 billion in Russian high-priority goods imports recorded from January to October 2023 consisted of over 800,000 individual transactions.[10] In August of 2024, it was reported that four airplanes were diverted to Minsk, likely to end up in Russia[11], and more than $30 million worth of aircraft tires made by western manufactures were imported into Russia last year via intermediaries despite attempts to ban the trade[12].

Towards to end of 2024, signs of challenges for Russian airlines are becoming evident. Out of 66 Airbus A320neo aircraft, 34 are grounded due to unresolved engine issues[13]. In 2024, globally, around 650 Airbus A320neo's equipped with Pratt & Whitney (P&W) engines, about half the P&W powered A320neo fleet, are estimated to be grounded due to engine issues[14]. Due to the sanctions, Russian airlines are unable to obtain replacement parts for this relatively new product, for which there is likely no black-market yet, possibly leading to early retirement of these new aircraft.

---

[5] Woods, Eric. "Russia's Aerospace Catastrophe: How Export Controls and Sanctions Will Affect Russia." *CNS Trade Compliance*, 22 Mar. 2022, https://www.sites.middlebury.edu/tradecompliance/2022/03/22/russias-aerospace-catastrophe-how-export-controls-and-sanctions-will-affect-russia/.

[6] James, Olivier. "En Russie, l'étonnant Maintien En Vol de Centaines d'airbus et de Boeing." *Www.Usinenouvelle.Com*, L'Usine Nouvelle, 16 Sept. 2024, www.usinenouvelle.com/article/en-russie-l-etonnant-maintien-en-vol-de-centaines-d-airbus-et-de-boeing.N2217848.

[7] "Russia's S7 Develops Engine Blade Capabilities." *Aviation Week Network*, 4 Oct. 2024, aviationweek.com/air-transport/airlines-lessors/russias-s7-develops-engine-blade-capabilities.

[8] "To Keep Flying, Russian Airlines Hunt and Scavenge for Spare Parts." *Kharon*, 23 May 2023, www.kharon.com/brief/to-keep-flying-russian-airlines-hunt-and-scavenge-for-spare-parts.

[9] In the context of the U.S. Export Administration Regulations (EAR) and the EU export regulations, governed by Regulation (EU) 2021/821, an "item" refers to any commodity, software, or technology that is subject to export control regulations.

[10] Ribakova, Elina. *The U.S. Technology Fueling Russia's War in Ukraine: How and Why*, 27 Feb. 2024, www.piie.com/sites/default/files/2024-02/ribakova2024-02-27testimony.pdf. p.5

[11] Aviacionline. "Magical Mistery Tour: An Airbus A320 and Three A330s of a Shady African Airline Flew to Minsk; ¿to End up in Russia?" *Aviacionline*, 21 Aug. 2024, www.aviacionline.com/magical-mistery-tour-an-airbus-a320-and-three-a330s-of-a-shady-african-airline-flew-to-minsk-to-end-up-in-russia?utm_content=cmp-true#google_vignette.

[12] Boffey, Daniel. "Moscow Importing Western Aircraft Tyres despite Ban, Says Ukraine Agency." *The Guardian*, Guardian News and Media, 12 Sept. 2024, www.theguardian.com/business/2024/sep/12/moscow-importing-western-aircraft-tyres-despite-ban-says-ukraine-agency?CMP=Share_iOSApp_Other.

[13] "Half of Russia's Airbus A320neo Fleet Grounded amid Engine Problems, Sanctions – Kommersant." *The Moscow Times*, The Moscow Times, 21 Nov. 2024, www.themoscowtimes.com/2024/11/21/half-of-russias-airbus-a320neo-fleet-grounded-amid-engine-problems-sanctions-kommersant-a87087.

[14] Russell, Edward. "Airbus A320neo Pratt Engine Issues to Ground 650 Planes next Year." *Airline Weekly*, 12 Oct. 2023, airlineweekly.skift.com/2023/09/airbus-a320neo-pratt-engine-issues-to-ground-650-planes-next-year/.

The Guardian reported in February of 2025 that customs data reveals that over 100 western companies have exported aircraft parts to India, which were then re-exported to Russia. This trade, valued at over $50 million, involved 700 cargoes containing various aircraft parts. Most Russian importers were civilian airlines[15].

Sanctioning authorities' responses to sanctions evasion

Historically, sanctions regimes have included measures to prevent circumvention and diversion practices, such as the "Guidance to Address Illicit Shipping and Sanctions Evasion Practices"[16] under the Iran sanctions. Circumvention consists of sophisticated methods to bypass or evade sanctions without directly violating the rules but using complex schemes or loopholes to continue prohibited activities. Diversion happens when items are redirected to avoid restrictions.

It is important to note that the sanction regimes targeting Russia have significantly intensified the focus on preventing diversion and circumvention. The U.S., EU and allies have publishing one sanction update after another to tackle the issue of the evasion of sanctions by diversion and circumvention creating a complex matrixial sanctions environment.

The countries involved in the diversion and circumvention of sanctions against Russia.

Debates continue regarding the impact and effectiveness of sanctions, particularly since major economies like China, India, Turkey, and Brazil have not imposed sanctions on Russia.[17]
The countries involved in the diversion and circumvention of sanctions against Russia often justify their actions based on a mix of economic, strategic, and political reasons. Turkey argues that maintaining trade relations with Russia is crucial for its economy, especially given its significant energy dependence on Russian Imports[18]. Additionally, Turkey positions itself as a mediator in international conflicts, which it believes requires maintaining open channels with all parties[19]. China justifies its actions by highlighting its strategic partnership with Russia and the need to support its own economic stability. By providing the yuan for transactions, China helps mitigate the impact of sanctions on Russia[20]. India maintains a stance of strategic independence and non-alignment and justifies it continued trade with Russia by pointing to historical ties and dependence on Russian military equipment and energy resources[21]. Kazakhstan cites the practical difficulties of strictly adhering to sanctions while maintaining economic cooperation with Russia, given their shared customs union and free currency conversion[22] and emphasizes its role in

---

[15] Matthews, Chris, et al. "British Firms among Companies to Have Exported Aircraft Parts That Reached Russia." *The Guardian*, Guardian News and Media, 20 Feb. 2025, www.theguardian.com/business/2025/feb/20/british-firms-among-those-that-exported-aircraft-parts-which-reached-russia.
[16] *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, ofac.treasury.gov/media/37751/download?inline=. Accessed 13 Aug. 2024.
[17] Welt, Cory. *U.S. Sanctions on Russia: Legal Authorities and Related Actions*, Congressional Research Service, 26 Apr. 2024, crsreports.congress.gov/product/pdf/R/R48052. p.2
[18] KEFALOGIANNIS, Manolis. "Parliamentary Question: Turkey's Refusal to Go along with Sanctions on Russia and Its Transformation into a Russian 'Transit Hub': E-003495/2022: European Parliament." *E*, 25 Oct. 2022, www.europarl.europa.eu/doceo/document/E-9-2022-003495_EN.html.
[19] Jack, Victor. "How Turkey Became Putin's 'pit Stop' for Selling Camouflaged Fuel to the EU." *POLITICO*, POLITICO, 19 June 2024, www.politico.eu/article/how-turkey-become-vladimir-putin-pit-stop-sell-camouflage-fuel-eu/.
[20] Nikoladze, Maia. "How Is China Mitigating the Effects of Sanctions on Russia? ." *Atlantic Council*, 14 June 2023, www.atlanticcouncil.org/blogs/econographics/how-is-china-mitigating-the-effects-of-sanctions-on-russia/.
[21] Chang, Felix K. "India's Neutrality and Strategic Relations with China, Russia, and the West." *Foreign Policy Research Institute*, 25 Apr. 2022, www.fpri.org/article/2022/04/indian-foreign-policy-and-the-russian-ukrainian-war/.
[22] Zhumagulova, Kamshat, and Rahimbek Abdrahmanov. "How Kazakhstan Helps Russia Bypass Western Sanctions." *The Diplomat*, 25 Oct. 2023, thediplomat.com/2023/10/how-kazakhstan-helps-russia-bypass-western-sanctions/.

promoting regional stability and economic interdependence[23]. Armenia justifies its actions by pointing to its economic dependence on Russia and the significant increase in trade between the two countries and argues that the surge in exports to Russia is a natural outcome of their economic relationship and not necessarily a deliberate attempt to circumvent sanctions[24]. The Armenian economy's high dependency on its trade with Russia has made it practically impossible for the country to join the sanctions against Moscow without risking unprecedented economic downfall[25]. Kyrgyzstan acknowledges the involvement of private companies in sanctions evasion but denies state involvement[26].

These justifications reflect a complex interplay of economic necessity, strategic interests, and political considerations. Nonetheless, companies in jurisdictions that support the sanctions on Russia must implement robust compliance programs to ensure they are not involved in circumventing these sanctions.

1.2 Navigating the maze: corporate challenges in adapting to the complex sanctions landscape of the European Union and United States

Even though there have been comprehensive sanctions on Russia for over three years, changes continue to be numerous. The sanctions updates that have been issued present a significant challenge to exporting companies who need to ensure compliance and prevent diversion and circumvention.

The complexity of the sanctions on Russia requires diverse and extensive data, often spread across multiple departments or divisions within companies' information systems. This dispersion necessitates system modifications and specialized expertise in systems implementation. The economic recovery from Covid facilitates hiding unusual demands, making it even harder to find these schemes for diversion and circumvention to Russia.

Non-Governmental Organizations (NGOs)[27] and journalists actively work on tracking sanctioned material, leading to severe reputational risk and extensive and rigorous enforcement actions by authorities, which can result in civil fines and occasionally criminal charges, highlight the critical need for companies to avoid unintentionally engaging in the diversion or circumvention of sanctions against Russia.

Staying updated with all the new sets of sanctions is time-intensive and requires a certain legal expertise. The sanctions measures, with additional requirements to prevent sanctioned goods and services from reaching prohibited entities in Russia indirectly, signify a shift, which not only increases the workload in compliance and export control departments, but also changes the nature of their work.

[23] Gallo, Ernest. "Among Conflicts and Sanctions: Kazakhstan's Role in Navigating Peace and Resolving Crises." *The Geopolitics*, 29 Sept. 2023, thegeopolitics.com/among-conflicts-and-sanctions-kazakhstans-role-in-navigating-peace-and-resolving-crises/.
[24] Baghirov, Orkhan. "Armenia's Role in Helping Russia Circumvent Sanctions." *Jamestown*, 25 May 2023, jamestown.org/program/armenias-role-in-helping-russia-circumvent-sanctions/.
[25] Pambukhchyan, Anna. "Armenia's Exports to Russia Raise Concerns over Sanctions Circumvention." *Euractiv*, 13 Feb. 2025, www.euractiv.com/section/armenia/news/armenias-exports-to-russia-raise-concerns-over-sanctions-circumvention/.
[26] Putz, Catherine. "As Focus on Sanctions Evasion in Kyrgyzstan Intensifies, Government Promises Action." – *The Diplomat*, The Diplomat, 21 July 2023, thediplomat.com/2023/07/as-focus-on-sanctions-evasion-in-kyrgyzstan-intensifies-government-promises-action/.
[27] NGOs are typically nonprofit organizations that operate independently of any government, often focusing on humanitarian, environmental, or social issues, on a local, national, or international level to address various causes and advocate for change.

Traditionally, compliance departments dealt with tasks that were under the direct control of the company. However, the new circumvention and diversion requirements place a significant emphasis on third parties and necessitate analyses that were never needed before. This adds a layer of complexity and demands a more comprehensive approach to compliance.

Fines and penalties, loss of business, and operational disruptions can lead to significant financial losses for the operators, however, the consequences of inadvertently facilitating prohibited activities can be severe and multifaceted. Although sanctioning authorities impose an obligation of means and not an obligation of results, OEMs understand that the consequences for non-compliance are to be avoided. However, in the context of constantly updated sanctions, systems that were not designed to “catch” diversion and circumvention, export controls based on tariff codes, an already busy workforce and tense market for qualified personnel, is it possible to put in place a compliance and export control program that meets the expectation of the authorities and avoid unauthorized exports by third parties? In this context, it is interesting to question the ability of aerospace companies to implement the sanctions requirements regarding diversion and circumvention.

2 Assumptions, scope and problem definition

This thesis aims to assess how the sanctions on Russia impact and reshape the compliance and export programs at aerospace OEMs, and to explore the tension between achieving sufficient compliance and the risk of violations that could trigger actions from sanctioning authorities.

2.1 The compliance imperative for aerospace OEMs: motivations and justifications

For this research, it is reasonable to assume that Western aerospace OEMs are motivated to comply with the sanctions and export controls imposed on Russia, as they do not benefit from evading these sanctions. Additionally, it is assumed that these OEMs have successfully implemented the earliest sanctions packages and compliance notes, which primarily required a complete halt of all exports of aerospace equipment to Russia, a relatively straightforward measure.

These assumptions are supported by legal, ethical, and business considerations for several reasons.

Firstly, directly violating sanctions by selling to sanctioned entities in Russia would be highly visible and likely result in immediate and severe penalties. Additionally, maintaining compliance with sanctions helps aerospace OEMs uphold their reputations, avoid legal repercussions, and ensure continued access to global markets. Therefore, the motivation to comply with sanctions is driven by a combination of legal obligations, ethical standards, and business interests. Aerospace OEMs often publish their codes of conduct, which emphasize their commitment to ethical practices and compliance with international laws.

Secondly, indirectly evading sanctions by collaborating in diversion and circumvention schemes is also not beneficial. Aerospace OEMs need long-lasting relationships with their customer base to ensure sustained business success and growth. Customers rely on a steady stream of aftermarket services, crucial for profitability, as a significant portion of an OEM's revenue comes from maintenance, repair, and overhaul. Additionally, OEMs need to ensure that customers continue to choose them for their needs, rather than switching to competitors. Feedback from customers is valuable and essential to improve existing products and develop new ones to stay competitive in the market. Long-term contracts provide a predictable revenue stream and financial stability, necessary for investing in future projects and technologies and effective communication and collaboration in a complex supply chain leads to fewer disruptions.

Thirdly, the industry today must cope with parts shortages and long lead times, which partly still stem from the lingering impact of the COVID-19 pandemic which caused massive layoffs and disrupted global supply chains, leaving many aerospace companies struggling to obtain essential raw materials, components, and skilled labor[28] [29] [30]. Geopolitical tensions and trade restrictions also impact the availability of certain parts and materials. Additionally, the increased demand for air travel and the

[28] Bodell, Luke. "GE Aerospace: Aviation Supply Challenges Will Continue in 2025." *Simple Flying*, 22 June 2024, simpleflying.com/ge-aerospace-supply-challenges-2025/.
[29] Pitti, Fabrice. "The Latest in Aerospace: An Industry Grounded." *Dow Jones*, 8 Nov. 2022, www.dowjones.com/professional/risk/resources/risk-blog/aerospace-industry-grounded.
[30] Juliano, Laura, et al. "Fixing Aerospace's Supply Chain for Casting and Forging." *BCG Global*, BCG Global, 17 July 2024, www.bcg.com/publications/2024/fixing-aerospaces-supply-chain-for-casting-and-forging.

subsequent need for new aircraft and maintenance have put further pressure on already strained supply chains.[31] Therefore, parts leaking away to Russia would exacerbate the already significant supply chain challenges faced by the aerospace industry.

Fourthly, several major aerospace OEMs have faced investigations for compliance violations, including bribery, corruption, and sanctions and export control breaches. These investigations have resulted in fines and consent agreements[32] with authorities, compelling these companies to develop robust compliance, export control, and sanctions programs to prevent future violations. Their publicly shared experiences act as a deterrent for other companies and help prevent future violations. These agreements help ensure that companies take corrective actions to prevent future violations and maintain compliance with export control and sanctions laws.

When one sanctioning authority conducts an audit, it can attract the attention of other regulatory bodies, leading to a cascade of investigations and potential penalties. Companies are wary of this scenario for several reasons. Increased scrutiny can result in multiple investigations, each focusing on different aspects of compliance, thereby broadening the scope of the initial findings. This leads to higher costs, including legal fees, compliance expenses, and potential fines, as well as operational disruptions that affect productivity. Reputational damage is another concern, as multiple investigations can erode customer trust and investor confidence, especially with media attention amplifying the negative impact. Violations can result in suspension or debarment from government contracts, barring the company from participating in future contracts and potentially leading to significant financial losses.

Regulatory overlap can create challenges due to conflicting requirements and inconsistent findings from different authorities. Additionally, cumulative penalties from various authorities can result in substantial fines and complex, time-consuming settlement negotiations.

Here are a few examples to illustrate the importance of maintaining strong compliance programs to avoid significant financial and reputational damage. In 2020, Airbus agreed to pay over $3.9 billion in penalties to authorities in the United States, France, and the United Kingdom[33]. In 2012, United Technologies Corporation (UTC) and its subsidiaries, Pratt & Whitney Canada, and Hamilton Sundstrand Corporation, faced significant penalties for export control violations. These companies were involved in the illegal export of U.S.-origin military software to China, which was used in the development of a Chinese attack helicopter. As a result, they agreed to a global settlement of over $75 million with the U.S. Department of Justice and the State Department. Up to 20 million could be suspended if UTC applied it to enhance its compliance programs and required UTC to retain an independent monitor to

[31] Loxton, Emma, et al. “Addressing Continued Turbulence: The Commercial-Aerospace Supply Chain.” *McKinsey & Company*, McKinsey & Company, 3 Apr. 2024, www.mckinsey.com/industries/aerospace-and-defense/our-insights/addressing-continued-turbulence-the-commercial-aerospace-supply-chain.

[32] A consent agreement is a legally binding settlement between a company and regulatory authorities to resolve export control or sanctions violations. It typically involves paying fines, which can be reduced if the company uses funds for compliance improvements, implementing compliance measures, appointing a Special Compliance Officer (SCO), undergoing regular audits, and providing employee training to prevent future violations.

[33] “Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and Itar Case.” *Office of Public Affairs | Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and ITAR Case | United States Department of Justice*, 6 Feb. 2025, www.justice.gov/archives/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case.

assess its compliance with export laws for two years.[34] In August of 2024, the U.S. State Department said that RTX, which is a merger of UTC and Raytheon[35], voluntarily disclosed violations related to defense technology and was fined $200 million. Most of the violations stemmed from compliance failures at Rockwell Collins within the RTX group[36] before the formation of RTX. RTX set aside $1.44 billion for remedial compliance measures[37].

Given the significant fines already received by aerospace OEMs, the compliance programs put in place, and the critical need to maintain trust and long-term relationships with their customer base, aerospace companies are motivated to adhere to sanctions. The risk of investigations, penalties, and the risk of losing export privileges only reinforces their commitment to compliance. However, this does not mean that violations never occur, as evidenced by the recent case at RTX. Repeated penalties highlight the complexity of maintaining a robust compliance program. While the company may strive to maintain compliance, individual employees who do not adhere to policies can still cause significant issues. Additionally, data quality problems introduced into systems before the compliance programs were reinforced may remain undetected until an audit reveals them, potentially leading to voluntary disclosure or actions from authorities if they discover the errors first.

The motivation to comply with sanctions is driven by a combination of legal obligations, ethical standards, and business interests. However, companies may sometimes be undercompliant or, conversely, apply sanctions more stringently than legally required, resulting in overcompliance.

Where undercompliance may lead to fines and reputational damage, overcompliance can lead to significant operational disruptions. Compliance departments may face an increased workload, which can divert resources from other critical tasks and projects.
Pierre-Hugues Verdier (2023), in the article titled "Overcompliance-Russia SSRN-4476520,"[38] explores the phenomenon of sanctions overcompliance in the context of U.S. sanctions against Russia. Businesses may refrain from transactions with non-sanctioned entities due to fear of potential future sanctions and legal uncertainty, meaning that ambiguities in sanctions rules lead to cautious behavior. The impact on businesses includes the loss of business opportunities due to excessive caution. Companies may also incur additional costs for implementing overly stringent compliance measures. For policymakers, overcompliance may undermine the targeted nature of sanctions and exacerbate the humanitarian impact on innocent third parties. For example, it can hinder the delivery of essential goods and services to populations in need and create market inefficiencies by restricting legitimate trade and financial transactions beyond what is legally required. Where overcompliance is often a rational response to

[34] "United Technologies Subsidiary Pleads Guilty to Criminal Charges for Helping China Develop New Attack Helicopter." *Office of Public Affairs*, 28 June 2012, www.justice.gov/archives/opa/pr/united-technologies-subsidiary-pleads-guilty-criminal-charges-helping-china-develop-new.

[35] Raytheon merged with United Technologies in 2020 and changed its name to RTX in 2023. RTX Investors. "SEC Filing." *RTX*, 17 July 2023, investors.rtx.com/node/40741/html.

[36] Vanderfort, Richard. "RTX to Pay $200 Million over Export Control Violations." *The Wall Street Journal*, 30 Aug. 2024, www.wsj.com/articles/rtx-to-pay-200-million-over-export-control-violations-46d653b1.

[37] Tokar, Dylan. "RTX Sets aside $1.24 Billion to Resolve Government Probes." *The Wall Street Journal*, 25 July 2024, www.wsj.com/articles/rtx-sets-aside-1-24-billion-to-resolve-government-probes-d91a0aaf.

[38] Verdier, Pierre-Hugues. "Sanctions Overcompliance: What, Why, and Does It Matter?" *SSRN*, 18 June 2023, ssrn.com/abstract=4476520.

uncertainty in sanctions rules, this can lead to excessive caution and risk aversion, which may stifle innovation and growth.

2.2 Research questions

The main research question is:

Is it reasonably and realistically possible to effectively implement enhanced due diligence processes to identify and mitigate the risk of circumvention and diversion of aerospace items to Russia, in a way that meets the authorities' requirements, considering the legal obligations to prevent such activities without the obligation of result, while maintaining operational continuity in a cost-effective manner?

To answer the main research question, it needs to be seen if companies can achieve a balanced approach to compliance that meets legal requirements without incurring unnecessary costs or operational burdens. To gather comprehensive information that will contribute to answering the main research question effectively two supporting questions were formulated.

- What measures do aerospace OEMs take to comply with the diversion and circumvention aspects of the sanctions on Russia?

This subquestion helps to understand the specific actions and strategies that aerospace OEMs are employing to adhere to these sanctions and how they differ from the export control and sanctions programs already in place. By examining these measures, we can assess their effectiveness or lack thereof.

- Does the implementation of sanctions on Russia result in overcompliance or undercompliance in other areas?

This subquestion evaluates the broader impact of sanctions on compliance in other areas, highlighting the undesirability of both under- and overcompliance, and providing insights into potential unintended consequences.

2.3 Defining the scope of the study

The scope of this research will be confined to aerospace OEMs and commercially classified items subject to EU and U.S. sanctions and export controls, intended for commercial airlines. This focus is necessary to maintain a manageable scope and is justified by several factors.

Items produced by Original Equipment Manufacturers (OEMs), such as aircraft, systems, components, parts, and technical documentation, are particularly vulnerable to circumvention and diversion due to Russia's heavy reliance on equipment from Western manufacturers.

Sanctions on Russia, first introduced on July 29, 2014, in response to Russia's actions destabilizing the situation in Ukraine, already prohibited the direct or indirect import, export, or transfer of all defense-related material and established a ban on Dual Use goods for military use or military end-users in Russia.

This thesis will not delve into military export controls, as all support of military equipment was already comprehensively restricted in 2014. Instead, the focus will be on the sanctions imposed as of February 2022 on the commercial part of aviation OEMs. It is important to note, though, that there are commercial aerospace parts that can be used in military equipment.

Sanctions have also been applied to Belarus in response to its substantial enabling of Russia's invasion. While this thesis will not separately address the sanctions on Belarus, it is important to note that compliance with Russian restrictions generally covers Belarus as well. Where there is a specific requirement to implement compliance measures regarding the sanctions against Belarus, these are mentioned, otherwise the same compliance programs and measures applicable to Russia can be extended to Belarus, ensuring comprehensive adherence to the relevant sanctions.

This thesis will include all measures up to and including the EU's 14th sanctions package, as well as all U.S. sanctions against Russia within this timeframe.

2.4 Defining "reasonably and realistically possible"

The main research questions of this thesis intents to determine if it is "reasonably and realistically possible" to comply to diversion and circumvention criteria as per the prescribed "obligation of means" per the regulations.

The term "obligations of means", also known as "obligations of conduct," refers to a legal duty where the obligated party must take all reasonable steps to achieve a particular outcome but is not required to guarantee that the outcome will be achieved. This concept is particularly relevant in the context of compliance with sanctions related to diversion and circumvention, where companies are expected to implement robust compliance measures but are not held strictly liable if, despite these efforts, a violation occurs. This entails the demonstration of reasonable efforts to assure appropriate measures to comply with sanctions, such as implementing due diligence processes, training, and monitoring of transactions. The compliance efforts to show that the company acts diligently must be documented as evidence, with regular reviews and updates to address new risks as regulatory changes unfold.

Reasonably and realistically possible can be explained in both legal and practical aspects. In the legal context, the term reasonable efforts is often used to imply that measures should be taken to mitigate the risk as far as is sensibly achievable, considering the severity of the risk balancing against the difficulty, cost, and practicality of the measures needed. Realistically possible involves assessing what can be feasibly achieved given the current resources, technology, and operational constraints.

In the context of this thesis, the definition of "reasonably and realistically possible" is:

> Implementing enhanced due diligence processes that are feasible within the current operational and financial constraints, while effectively mitigating the risk of sanctions circumvention and diversion, and meeting the legal requirements set by authorities.

3 Research structure, design, and methodology

This research will look at the requirements that are imposed on aerospace OEMs to avoid diversion and circumvention and which actions can be taken to ensure a satisfactory implementation of these measures. It will highlight the issues which can be experienced when implementing these measures into the day-to-day operations at the OEM. Where these experienced difficulties are caused by the legislation and regulations versus issues stemming from withing the company, this will be pointed out. To conclude, suggestions for actions that can be undertaken to reduce the risk of non-compliance, both from a regulatory and company point of view will be suggested. The literature review will examine the existing literature of export control and sanctions regulations implementation by businesses and look at previous studies on compliance challenges faced by business.

3.1 Structure of the thesis

In the introduction, the context and complex situation for companies needing to comply with sanctions on Russia were explained. From this, the research objective and questions were formulated, and the boundaries for the research are established.

The research structure, design, and methodology will be explained in this chapter, followed by a short overview of literature on sanctions in chapter 4. Chapter 4 will also cover the theoretical framework relevant to the research question regarding sanctions and how companies react to them, including pertinent theories on sanctions and corporate responses.

Understanding the complexity of the regulations and the role of regulators is crucial to appreciate the challenges companies face in fully implementing these regulations. Therefore, the extensive regulations concerning sanctions and their connection to export control and continued airworthiness regulations will be discussed in chapter 5, focusing on topics pertinent to the research questions.

Chapter 6 will explore the most impactful sanctions measures that OEMs have faced and their effects on companies, focusing on strategies to prevent circumvention and diversion. It will link the theory and reality of these sanctions to assess the OEMs' ability to fully implement them. Additionally, it will analyze and conclude findings from interviews with major OEMs and providing general conclusions. Business relevance, validity, reliability, and ideas for further research are discussed in the last chapter.

3.2 Research methodology

The aims to evaluate how effectively aerospace OEMs can comply with sanctions on Russia, particularly concerning diversion and circumvention, which present new challenges as these activities occur after items have been shipped and are outside the direct control of the companies.

Qualitative research

An exploratory approach is adopted to investigate how aerospace OEMs implement diversion and circumvention prevention measures in response to sanctions on Russia. Given the limited existing knowledge on this specific topic, an exploratory methodology is appropriate to gain deeper insights and identify emerging patterns.

The research begins with a review of existing literature to develop a conceptual model. This model serves as a theoretical framework to guide the investigation and provide a basis for understanding the key factors influencing compliance with sanctions in the aerospace industry.

Legal research will provide a comparative analysis of export control and sanctions regulations across different jurisdictions to which aerospace OEMs are subject. This will involve identifying key regulatory frameworks in major jurisdictions and analyzing the specific requirements for diversion and circumvention prevention in these regulations.

To complement the literature and legal reviews, semi-structured interviews will be conducted with compliance officers and legal experts directly involved in sanctions compliance within aerospace OEMs. These interviews aim to gather qualitative data on the practical challenges and strategies employed by these companies to prevent diversion and circumvention of aerospace items to Russia. This approach will provide insights into their current compliance practices and the challenges they face in implementing these measures.

The data from the interviews will be analyzed to highlight how similarities and differences in regulatory requirements across jurisdictions influence the OEMs' compliance programs. This analysis will assess the feasibility of implementing these requirements within the operational frameworks of aerospace OEMs and identify common challenges and best practices. The findings from the legal research and interviews will be compared to the existing literature on export control and sanctions implementation. The implications of these findings will be discussed to evaluate the overall ability of aerospace OEMs to comply with the diversion and circumvention requirements.

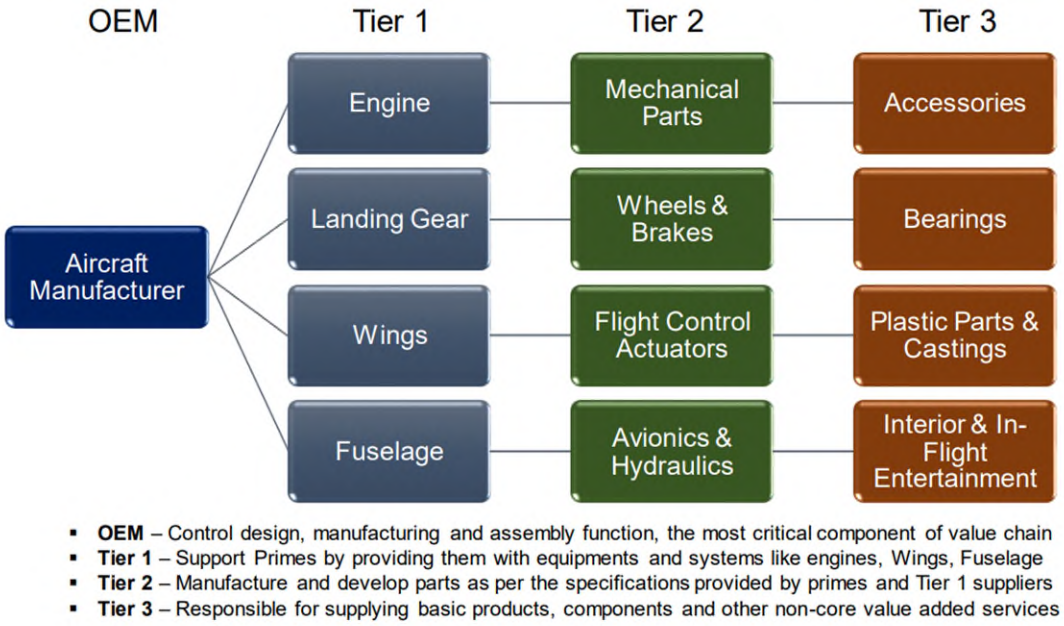
In the conclusions and recommendations, the findings of this research will be summarized, recommendations for aerospace OEMS will be provided and areas for future research suggested.

3.3 Sample and data description

The sample population and data sources for this research will include aerospace OEMs only. An Original Equipment Manufacturer, or OEM, is a company that produces parts and equipment that are used in the products of another company. OEMs typically design and manufacture components or systems that are then integrated into the final products sold by other companies. In the aerospace industry, a manufacturer can be both a Tier 1, 2 or 3 supplier and an OEM. This dual role is common in industries where complex systems and components are involved, allowing companies to specialize in both designing and manufacturing and supplying critical parts.

As Figure 1 illustrates, the aerospace supply chain is intricate, involving multiple levels of supply networks that provide essential equipment and materials for the production of final products. These networks are typically categorized into three tiers: Tier 1, Tier 2, and Tier 3. Most items in aerospace can be traced back to the Aircraft OEM and Tier 1, 2, and 3 suppliers. OEMs produce aircraft, parts, and components, which are then distributed to airlines, Maintenance, Repair, and Overhaul (MRO) facilities, and brokers. Brokers act as intermediaries, trading parts between OEMs, authorized distributors, MROs, and airlines. Additionally, airlines may engage in inter-airline trading to meet immediate needs. This interconnected network ensures that all parts can ultimately be traced back to the OEMs.

Figure 1: Aerospace Supply Chain and Manufacturing



Source: NASA, and Parimal Kopardekar. Aerospace Supply Chain and Manufacturing, https://nari.arc.nasa.gov/sites/default/files/attachments/1-pk-feb4-5-SupplyChainManagement.pdf. Accessed 16 Oct. 2024.

3.4 Validity and reliability

It is important to recognize key points about the interviews conducted in this research. Firstly, profit-driven entities have a vested interest in not being investigated by authorities for breaches of sanctions, which means they might withhold information or present biased perspectives. Drawing conclusions and generalizing from the findings must be done with caution, considering potential unknowns.

To ensure the validity of the research, data were collected from multiple interviews and legal documents to cross-verify the information and reduce bias. Only individuals directly involved in sanctions compliance were interviewed to ensure that the information gathered was relevant and accurate.

Regarding reliability, the research was designed to be consistent and replicable by using a standardized interview protocol. The interviews were semi-structured, based on a consistent set of questions to ensure uniformity in data collection.

Secondly, no attempt was made to contact companies that intentionally evade the sanctions. The goal was to determine how OEMs approach sanctions and specifically how they implement diversion and circumvention prevention in their decision-making and compliance programs. This ensures that the findings are relevant to companies striving to comply with regulations, rather than those seeking to circumvent them.

By acknowledging these limitations and implementing measures to enhance validity and reliability, the research aims to provide a robust analysis of how aerospace OEMs manage compliance with sanctions.

4 Theoretical Framework

There are several major sanctions regimes currently in place around the world, complex and constantly evolving, imposed by different countries and organizations. It is therefore not possible to provide an exact number of sanctions. However, several major sanctions regimes currently shape the compliance programs at companies such as the most significant sanctions on:

- **Russia:** Following its invasion of Ukraine in 2022, Russia has faced sanctions from the EU, U.S., Canada, UK, Australia, and Japan. These sanctions target various sectors such as finance, energy, aerospace, and technology.
- **Cuba:** The U.S. has maintained a comprehensive embargo on Cuba for decades, targeting trade, travel, and financial transactions.
- **Iran:** Sanctions on Iran, primarily from the U.S. and EU, focus on its nuclear program, human rights abuses, and support for terrorism. These include restrictions on financial transactions, oil exports, and access to international markets. The U.S. maintains a comprehensive embargo on Iran. The EU sanctions on Iran[39] can be described as targeted[40] and sectoral[41].
- **North Korea:** Sanctions from the UN, U.S., and EU aim to curb its nuclear weapons program and include bans on arms sales, luxury goods, and certain financial transactions.
- **Syria:** Both EU and U.S. had sanctions targeting the Assad regime. The European Union lifted key sanctions on Syria on February 25, 2025, to support the country's economic recovery and reconstruction following the ousting of President Bashar al-Assad in December 2024. However, the United States has maintained its sanctions due to ongoing human rights concerns, the need to influence the new government, security risks related to extremist groups, and the political and technical challenges of lifting and potentially re-implementing sanctions.
- **Belarus:** Sanctions from the EU, U.S., and other countries have been imposed due to human rights violations and the suppression of political opposition. These include asset freezes and travel bans on key individuals and entities.
- **Myanmar:** Sanctions from the EU, U.S., and other countries target the military junta following the 2021 coup, focusing on arms embargoes and restrictions on military-owned businesses.
- **Venezuela:** Sanctions from the U.S. and EU target the Maduro regime for human rights abuses and corruption, including restrictions on financial transactions and oil exports.

4.1 Literature review

This chapter briefly reviews existing literature on the effectiveness of sanctions, the phenomenon of overcompliance, and how firms adjust to sanctions and other crises. Additionally, it examines the behavior of for-profit actors in response to sanctions, the impact of external pressures on companies' compliance strategies, and the broader implications for business operations and international trade.

[39] *EU Sanctions against Iran - Consilium*, European Council, www.consilium.europa.eu/en/policies/sanctions-against-iran/. Accessed 24 July 2024.

[40] Targeted sanctions on Iran are aimed at specific individuals and entities, such as travel bans and asset freezes for those involved in human rights abuses, nuclear proliferation, and military support for Russia.

[41] Sectoral Sanctions on Iran affect specific sectors of the economy, such as bans on the export of Dual Use goods, arms, and components used in drones and missiles.

4.1.1 The effectiveness of sanctions

This approach of trying to determine if sanctions are effective, typically measures success by evaluating the extent to which sanctions compel the targeted entities to comply, either fully or partially, with the demands of the sanctioning nations (Beeson)[42]. Scholars have debated the efficacy of sanctions, noting that their success rates vary significantly. For instance, unilateral sanctions imposed by the U.S. have achieved their foreign policy objectives in only about 13% of cases since 1970 (Nasr et al. *Do sanctions actually work? experts evaluate the efficacy of this widely used foreign policy tool*)[43]. More generous estimates suggest that sanctions lead to meaningful behavioral changes in the targeted country approximately 40% of the time[44].

4.1.2 Sanctions and business as profit-maximisers

The behavior of for-profit actors in the implementation phase of sanctions is in line with the assumption that firms and business are profit-maximisers. Weighing the profits from business against the costs of (non-)compliance, firms make the decisions which in their view maximize their profits. Indeed, de-risking seems to be the most common approach by companies due to the uncertainties produced by the multiple and overlapping sanction regimes imposed sometimes by the UN, the EU and, especially, by the U.S.[45].

Private actors undertake a conservative approach in implementing and, as such, they tend to over-comply with the regulations in order to minimize their own economic risks[46].

4.1.3 The Impact of External Pressure on Companies' Responses to Sanctions

In an article, published in the *European Journal on Criminal Policy and Research* (2024), titled "The Impact of External Pressure on Companies' Responses to Sanctions – an International Comparative Study"[47], the authors (Stępień et al.), investigated how different types of external pressure influence companies' compliance behaviors and strategic responses to economic sanctions, particularly those imposed on Russia following its 2022 invasion of Ukraine.

The study aims to uncover why firms respond differently to sanctions, focusing on compliance behaviors, undercompliance, compliance, and overcompliance and strategic responses which can be reactive or proactive. The authors state that economic sanctions create a mixed set of risks and rewards that alter the business environment for firms to which they can respond either reactively or proactively. Risk-

[42] Beeson, Mark, Adjunct professor. "Sanctions Rarely Work, but Are They the Least Worst Option?" *University of Technology Sydney*, 12 Feb. 2024, www.uts.edu.au/news/business-law/sanctions-rarely-work-are-they-least-worst-option.
[43] Nasr, Vali R, et al. "Do Sanctions Actually Work? Experts Evaluate the Efficacy of This Widely Used Foreign Policy Tool." *Johns Hopkins in Washington, D.C.*, 15 May 2024, washingtondc.jhu.edu/news/do-sanctions-actually-work-experts-evaluate-the-efficacy-of-this-widely-used-foreign-policy-tool/.
[44] "When Do Economic Sanctions Work Best?" When Do Economic Sanctions Work Best? | Center for a New American Security (en-US) (cnas.org), *CNAS*, www.cnas.org/publications/commentary/when-do-economic-sanctions-work-best. Accessed 14 Aug. 2024.
[45] Onderco, M, and F Giumelli, *States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands — the University of Groningen Research Portal*, research.rug.nl/en/publications/states-firms-and-security-how-private-actors-implement-sanctions-. Accessed 10 Oct. 2024.
[46] Arnold Aaron, 'The true costs of financial sanctions', *Survival,* 58:3 (2016), pp. 77–100.
[47] Stępień, Beata, et al. "The impact of external pressure on companies' responses to sanctions – an international comparative study." *European Journal on Criminal Policy and Research*, vol. 30, no. 2, 7 Mar. 2024, pp. 1–26, https://doi.org/10.1007/s10610-024-09576-y.

acceptant companies may seek to exploit legal loopholes that allow them to circumvent sanctions or engage in deliberate sanctions-busting activities that violate sanctions requirements.

Their research uses a survey of 610 medium-sized companies operating in Germany, Poland, and the United States, employing structural equation modeling to analyze the data. The study examined how companies react to economic sanctions on Russia, aiming to understand why their responses vary. It categorizes corporate behavior into undercompliance, compliance, and overcompliance, and looks at whether firms use reactive or proactive behaviors. Undercompliance occurs when firms fail to meet sanctions requirements, while overcompliance happens when firms go beyond what is legally required by severing ties with sanctioned or sanctions-exposed parties. Regarding business strategies, they state that reactive strategies involve responding to crises as they happen, minimizing immediate costs, while proactive strategies anticipate future threats and opportunities, planning to benefit from the changes that sanctions bring. Reactive approaches focus on winding down affected operations and reducing exposure, while proactive ones seek to leverage new opportunities created by the sanctions.

The study found that higher levels of external pressure are associated with both compliance and overcompliance behaviors, but also with undercompliance in some cases. This suggests that while many firms respond to external pressure by adhering to or exceeding sanctions requirements, some firms still seek to circumvent these sanctions. The findings indicate that firms' compliance behaviors significantly influence their strategic responses, with compliant firms often adopting a mix of reactive and proactive strategies. Interestingly, even firms that comply with sanctions may proactively seek legal means to circumvent them through third-party countries not participating in the sanctions.

Overall, external pressure has generally pushed firms towards disengaging from Russia. However, some firms have found opportunities in violating the sanctions despite significant pressure to comply. Firms that do not fully comply with Russian sanctions actively look for ways to profit from these sanctions. Notably, the study also found that many compliant firms are adopting proactive business strategies, indicating they might be seeking legal ways to circumvent sanctions through third-party countries not involved in the sanctions.

Country-specific insights reveal that U.S. firms tend to comply strongly with sanctions due to robust enforcement by the Office of Foreign Assets Control (OFAC). In contrast, German and Polish firms show significant variations in compliance behaviors, influenced by their regulatory environments and public pressure. The study concludes that external pressures play a crucial role in shaping how firms respond to sanctions, with compliance behaviors leading to a combination of reactive and proactive strategic responses.

In summary, the article highlights the complex interplay between external pressures and firms' responses to sanctions, providing valuable insights for policymakers on the effectiveness of sanctions and the challenges in ensuring compliance.

4.1.4 The Role of For-Profit Actors in Implementing Targeted Sanctions: The Case of the European Union

Giumelli, in "The Role of For-Profit Actors in Implementing Targeted Sanctions: The Case of the European Union," [48] discusses the evolution of sanctions from comprehensive to targeted, emphasizing the role of private companies in implementing these sanctions. His work highlights the importance of banks, financial institutions, trading companies, and producers in ensuring compliance with sanctions. The author explores how private actors have become integral to the provision of security, both domestically and internationally, and mentions the involvement of private actors in various security-related tasks, such as administering prisons, protecting critical infrastructure, and participating in military operations.

The EU's approach to sanctions is discussed, including the legal framework and the role of various EU institutions. It is explained how the EU's targeted sanctions are designed to minimize the impact on civilians while focusing on specific individuals and entities. By analyzing the behavior of for-profit actors in different regulatory environments, using the EU's targeted sanctions as a case study, common problems such as overcompliance, lack of compliance, and uneven compliance are identified.

The author proposes a typology of regulatory environments to understand the behavior of for-profit actors in implementing sanctions. Four typologies, based on the clarity of instructions provided by state authorities and their capacity to monitor and enforce compliance, are identified:

Table 2: A typology by regulatory environments

	Detailed instructions	Vague instructions
High monitoring capacity	Type A: Enforceable implementation Problem: not considered	Type C: Enforceable delegation of implementation Problem: overcompliance
Low monitoring capacity	Type B: Implementation by persuasion Problem: behavior depends on location of company	Type D: Delegation of implementation by persuasion Problem: lack of compliance, behavior depends on type of company

Source: Giumelli (2017).

Enforceable Implementation: Clear instructions and strong monitoring/enforcement; governments can specifically outline what private actors are supposed to do and monitor their behavior to enforce the regulation.

Implementation by Persuasion: Clear instructions but weak monitoring/enforcement; public authorities can provide detailed regulation, but monitoring cannot be properly done.

Enforceable Delegation of Implementation: Vague instructions but strong monitoring/enforcement; the authorities have the power to monitor the behavior of non-state actors, but clear and specific instructions cannot be provided.

[48] Giumelli, Francesco. "The role of for-profit actors in implementing targeted sanctions: The case of the European Union." Security Privatization, 1 Oct. 2017, pp. 123–141, https://doi.org/10.1007/978-3-319-63010-6_6.

Delegation of Implementation by Persuasion: Vague instructions and weak monitoring/enforcement; private actors do not know exactly what they have to comply with, and public authorities cannot monitor what they do. Examples include instructions such as “block suspicious activities” and “no funds shall be made available indirectly or directly,” where "suspicious" and "indirectly" are not clearly defined.

Giumelli (2017) argues that these four types of regulatory environments are likely to create problems of overcompliance, uneven compliance, and lack of compliance. The regulatory environment is determined by the clarity of instructions provided by the regulations adopted by public authorities and by the monitoring/enforcing capacities of the authorities. He also states that when it comes to enacting legislation, state authorities need to have at least as much knowledge as private actors to provide these private actors with specific guidelines on what needs to be done.

In situations where companies are unsure about how to proceed, although they feel that their actions can be sanctioned, it likely leads to overcompliance, where private actors avoid the risk of violating public regulations on restrictive measures by choosing to adopt extremely cautious behavior towards any transaction to and from targeted countries.
The analysis highlights that the effectiveness of sanctions depends on the regulatory environment, including the clarity of instructions and the capacity to monitor and enforce regulations. Effective implementation occurs when the authorities have high monitoring capacity with detailed instructions. High monitoring capacity with vague instructions leads to the risk of overcompliance. Low monitoring capacity with detailed instructions leads to implementation that depends on company location. Low monitoring capacity with vague instructions leads to a lack of compliance, with behavior depending on the company type.

The study suggests that the EU's lack of a robust monitoring structure is problematic. It recommends adopting models like the UN's Panel of Experts to improve compliance and suggests that the EU should develop mechanisms to involve and train private actors in implementing sanctions. This would enhance the resilience of the system and reduce the gap between regulations and their outcomes.

The research emphasizes the importance of regulatory environments in shaping the behavior of for-profit actors and suggests that better monitoring and enforcement mechanisms are needed to ensure effective implementation of sanctions. It also highlights the need for clearer guidelines and better coordination among EU Member States.

4.2 Conclusions literature

The behavior of for-profit companies during the implementation of sanctions aligns with the idea that businesses aim to maximize profits. Firms weigh the profits from business activities against the costs of compliance or non-compliance with sanctions. Due to the uncertainties created by multiple and overlapping sanction regimes from entities like the UN, EU, and especially the U.S., companies often adopt a de-risking approach. This conservative strategy leads them to over-comply with regulations to minimize economic risks.

The study (Stępień et al.), which surveyed 610 medium-sized companies in Germany, Poland, and the United States, found that, that while many firms adhere to or exceed sanctions requirements, some still seek to circumvent them. Compliant firms often adopt a mix of reactive and proactive strategies,

sometimes seeking legal ways to bypass sanctions through third-party countries not participating in the sanctions.

Giumelli's (2017) work on the role of for-profit actors in implementing targeted sanctions shows that effective implementation occurs when authorities provide clear instructions and have strong monitoring capabilities. Conversely, vague instructions and weak monitoring lead to overcompliance or lack of compliance. The study suggests that the EU's lack of a robust monitoring structure is problematic and emphasizes the need for clearer guidelines and better coordination among EU Member States to ensure effective implementation of sanctions.

In conclusion, the effectiveness of sanctions depends significantly on the regulatory environment, including the clarity of instructions and the capacity to monitor and enforce regulations. Both studies underscore the importance of external pressures and regulatory frameworks in shaping how firms respond to sanctions, highlighting the challenges and opportunities in ensuring compliance.

5 From regulations to managing export controls and sanctions compliance in aerospace

Understanding the fundamentals of the regulatory landscape is crucial to grasp how the sanctions on Russia challenge and expand existing export control and compliance programs within companies. Effective implementation of any compliance program requires a thorough understanding of both export control and sanctions regulations, as well as how they are interconnected. Companies need to have a thorough understanding of the authorities who control exports and sanctions in order to determine the elements to be included in their compliance program. Both BIS and EU provide guidance on how to compose an internal compliance program and their guidance contains comparable elements following the diverse applicable regulatory requirements but are not necessarily built in the same way[49].

Sanctions and export controls are tools used by governments to regulate international trade and maintain national security. However, they serve different purposes and operate in distinct ways. Sanctions are punitive measures imposed by countries or international organizations to influence the behavior of targeted entities. In contrast, export controls regulate the export of specific goods, technologies, and services through specific regulatory measures. These measures are designed to prevent the proliferation of sensitive technologies and ensure that exports do not enhance the military capabilities of adversaries.

Firstly, this chapter will provide an overview of the implementation of export controls and sanctions in the U.S., followed by a similar overview for the EU. Subsequently, it will compare both frameworks to highlight the complexity of the organizational structures and regulations. The chapter aims to clarify the minimum understanding of the requirements that exporting aerospace companies must have to be able to implement a program to ensure compliance with both sanctions and export control regulations.

Secondly, the aerospace industry is heavily regulated for safety reasons, imposing significant obligations on OEMs to provide comprehensive documentation to operators. This documentation is crucial for maintaining airworthiness and safety standards. However, conflicts can arise when these regulatory requirements intersect with sanctions or export controls, and such conflicts will be highlighted.

5.1 U.S. export controls and sanctions in a nutshell

This section will describe the export controls and sanctions in the U.S. starting with the explanation of why U.S. regulations can apply to non-U.S. companies, followed by the overview of the regulating

[49] The BIS defines the elements in the export compliance guidelines as: management commitment, risk assessment, export authorization, recordkeeping, training, audits, handling export violations and taking corrective actions, and build and maintain the export compliance manual. The EU recommendations define the essential elements as: top-level management commitment to compliance, organization structure, responsibilities, and resources, training and awareness raising, transaction screening process and procedures, performance review, audits, reporting and corrective actions, recordkeeping and documentation, and physical and information security.

authorities. For the purposes of this thesis, only the commercial export controls will be described in more detail, and only where useful for completeness, the military export controls are mentioned.

Extraterritoriality of U.S. export control and sanctions regulations

The U.S. has broad jurisdiction, including the concept of extraterritoriality. This means that the U.S. can assert jurisdiction based on the involvement of U.S. persons, regardless of their location, as well as parties located within the U.S. It also extends to the U.S. financial system, such as USD payments that involve U.S. banks, and equipment like data servers located in the U.S. Additionally, it covers goods subject to U.S. export controls. It also includes parties owned or controlled by U.S. persons, specifically in the context of Iran and Cuba programs. On top of this, there are secondary sanctions that primarily target the sanctions programs of Iran, North Korea, Syria, Venezuela, and Russia.

5.1.1 Export control regulators in the U.S.

In the United States, export controls are primarily regulated by the Bureau of Industry and Security (BIS) and the Directorate of Defense Trade controls (DDTC).

The BIS is part of the U.S. Department of Commerce and oversees the Export Administration Regulation (EAR). The Directorate of Defense Trade Controls (DDTC) within the Bureau of Political-Military Affairs, which itself is part of the U.S. Department of State (DOS), manages the International Traffic in Arms Regulations (ITAR)[50] which controls the export of defense articles and services.

The U.S. EAR and ITAR are both extraterritorial[51]. This extraterritoriality helps the U.S. protect its national security interests by controlling the spread of sensitive technologies and materials, ensuring that certain items[52] do not fall into the hands of adversaries. This includes reexports[53], transfers and retransfers[54], which might otherwise escape U.S. jurisdiction and is found crucial by the U.S. for addressing global security threats and ensuring that allied nations adhere to similar standards[55].

Export Administration Regulations (EAR)

The Export Administration Regulations, EAR, aims to advance U.S. national security, foreign policy, and economic objectives by regulating the export of sensitive goods and technologies, which cover Dual Use items, commercial, and less sensitive military items, both tangible and intangible, and participates in international export control regimes[56]. The Department of Commerce has enforcement and protective

[50] *U.S. Department of State*, U.S. Department of State, www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_itar_landing. Accessed 3 Oct. 2024.

[51] Extraterritoriality in U.S. export regulations is mostly described by the restrictions on reexport of controlled items in Section 736.2(b), GENERAL PROHIBITIONS AND DETERMINATION OF APPLICABILITY of the EAR.

[52] In export control regulations, an "item" generally refers to any product, technology, or software that is subject to export control laws.

[53] The definition of “reexport” per EAR, 15 CFR § 734.14 is the shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, which includes the release of technology or software subject to the EAR to a foreign national outside the U.S.

[54] Transfer refers to a change in end use or end user of an item within the same foreign (to the U.S.) country. Retransfer refers to the transfer of an item from one foreign person to another within the same foreign country from a U.S. perspective.

[55] Voetelink, J. (2022). Limits on the Extraterritoriality of United States Export Control and Sanctions Legislation. In: Beeres, R., Bertrand, R., Klomp, J., Timmermans, J., Voetelink, J. (eds) NL ARMS Netherlands Annual Review of Military Studies 2021. NL ARMS. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-471-6_11

[56] “Bureau of Industry and Security.” *U.S. Department of Commerce*, www.commerce.gov/bureaus-and-offices/bis. Accessed 12 Sept. 2024.

measures available to ensure that recipients of items subject to the EAR[57] comply with the reexport license requirements of the EAR. If they determine that an export violation has taken place, it may institute administrative enforcement proceedings, resulting in the possible imposition of civil penalties and/or denial of eligibility to receive U.S. exports[58].
There are ten General Prohibitions under the Export Administration Regulations (EAR) which outline specific activities related to exports, reexports, and transfers that are prohibited without a license or license exception.

There are ten affirmative statements regarding which activities require authorization, known as the General Prohibitions, contained in Part 736[59] of the EAR. Applicability of the General Prohibitions depends primarily on four factors:

1. What: The classification of the item
2. Where: The destination
3. Who: The end user
4. Why: The end use

In addition, the EAR prohibits certain activities by U.S. persons, even if they do not involve items subject to the EAR.

The ten General Prohibitions under the EAR[60]:

1. **Export and reexport of controlled items to listed countries:** One cannot export or reexport items controlled under the EAR to certain countries without a license.
2. **Reexport and export from abroad of foreign-made items with U.S. content**: Foreign-made items that incorporate more than a de minimis amount of controlled U.S. content require a license.
3. **Foreign-direct product rules (FDPR)**: Items that are the direct product of U.S. technology of software may require a license for export, reexport, or transfer.
4. **Engaging in actions prohibited by a denial order:** One must not engage in activities prohibited by a denial order issued by the EAR.
5. **Export, reexport, or transfer to prohibited end-uses or end-users:** Items cannot be exported, reexported, or transferred to end-users that are prohibited under the EAR.
6. **Export, reexport, and transfer to embargoed destinations**: Items cannot be exported, reexported, or transferred to countries or regions under U.S. embargoes without a license.
7. **Support of proliferation activities and certain military-intelligence end uses and end users**: U.S. persons are prohibited from supporting proliferation activities and certain military-intelligence and end uses and end users[61].
8. **In-transit shipments and items to be unladen from vessels or aircraft:** Certain in-transit shipments and items to be unladen from vessels of aircraft require a license.
9. **Violation of any orders, terms, and conditions of licenses:** One must comply with all terms and conditions of licenses issued under the EAR.

---

[57] "§ 734.3 Items Subject to the Ear." *§ 734.3 Items Subject to the EAR. | Bureau of Industry and Security*, www.bis.gov/ear/title-15/subtitle-b/chapter-vii/subchapter-c/part-734/ss-7343-items-subject-ear. Accessed 17 Sept. 2025.
[58] Part 764 of the EAR
[59] *Part 736 - General Prohibitions - Bureau of Industry and Security*, www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file. Accessed 17 Sept. 2024.
[60] "The Federal Register." *Request Access*, www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736/section-736.2. Accessed 17 Sept. 2024.
[61] "The Federal Register." *Federal Register: Request Access*, www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736. Accessed 17 Sept. 2024.

10. **Proceeding with transactions with knowledge that a violation has occurred or is about to occur:** One cannot proceed with transactions if one knows a violation of the EAR has occurred or is about to occur.

From the ten General Prohibitions, we deduce that two rules specifically highlight extraterritoriality, namely the second and third prohibitions. The first rule on reexport and export from abroad of foreign-made items with U.S. content, which requires a license for foreign-made items that incorporate more than a de minimis amount of controlled U.S. content. The second is the Foreign-direct product rules (FDPR), which apply U.S. export controls to certain items produced outside the United States that are the direct product of U.S.-origin technology or software. In this manner, the U.S. extends the reach of its export controls beyond its borders, ensuring that sensitive U.S. items are not used in ways that conflict with U.S. foreign policy or national security interests. This topic will be further discussed in the following paragraph.

Key U.S. export provisions

The first rule is the De Minimis rule[62] determines the threshold below which foreign-made items incorporating U.S.-origin controlled content are not subject to U.S. export controls. It specifies the percentage of U.S. content that can be included in a foreign product without triggering U.S. export regulations.

The second provision under the EAR is the Foreign Direct Product Rule (FDPR), which applies U.S. export controls to certain items produced outside the United States. This means that items with no physical U.S. origin content can still be subject to the EAR. As a result, they may require a license for export, reexport, or transfer, depending on their classification, destination, end-use, and end-user [63]. There are distinct conditions under which this can happen. The first one is that the FDPR applies to foreign-produced items that are either the direct product of U.S.-origin technology or software or are produced by a plant or major component of a plant that is itself a direct product of U.S.-origin technology or software.[64] The second condition is that the foreign-made product is intended for a country listed in Country Groups[65] D:1 (Russia), E:1 (Iran, North Korea, and Syria), or E:2 (Cuba). Another criterion that triggers the relevance of the FDPR is when entities are listed on the U.S. Entity List[66], maintained by the BIS. This list includes organizations and individuals subject to specific license requirements due to their involvement in activities contrary to U.S. national security or foreign policy.

5.1.2 U.S. classification systems for export control and trade.

Exporters are concerned with the proper classification of goods; however different classification systems have different purposes.

[62] The de minimis rules in the EAR are outlined in Section 734.4. and Supplement 2 to Part 734 with thresholds and guidance on how to calculate the percentage of U.S.-origin controlled content, to determine when non-U.S.-origin items are subject to the EAR. Note that specific U.S.-origin items are never eligible for de minimis treatment.

[63] eC The Federal Register, www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.9. Accessed 18 Sept. 2024.

[64] "Foreign Direct Product Rules." *Foreign Direct Product Rules | Bureau of Industry and Security*, www.bis.gov/foreign-direct-product-rules. Accessed 17 Sept. 2024.

[65] *The Federal Register*, www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/appendix-Supplement No. 1 to Part 740. Accessed 17 Sept. 2024.

[66] "Entity List." *BIS Website*, www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list. Accessed 18 Sept. 2024. Supplement No. 4 to part 744, Entity List, used to inform the public of entities that are involved in activities contrary to the national security or foreign policy interest of the U.S.

Classification for export control is used to determine whether an item requires special controls before export and if an export license is required or if a license exception can be used.

Classification for international trade is essential for accurately classifying and documenting goods. It facilitates customs procedures, determines tariff rates, and import duties and generates trade statistics which indirectly support export control compliance.

U.S. classification of items for export control

In the United States, the classification of export-controlled items, as regulated by the first General Prohibition, is primarily organized through two lists: the Commerce Control List (CCL) and the United States Munitions List (USML). The USML controls the export and temporary import of defense articles and services. These are items specifically designed, developed, configured, adapted, or modified for military applications. An item is either on one or the other list but cannot be listed on both. The list it appears on will have the conditions that must be met to export it.

The CCL is maintained by the BIS under the EAR. Its purpose is to regulate the export and reexport of commercial and Dual Use items. The CCL is divided into ten categories, each covering different types of items, and five product groups. Each item on the CCL is assigned an Export Control Classification Number (ECCN), which determines the level of control and licensing requirements[67] which depend upon technical characteristics, destination, end use and the end user of the item.

Because of the extraterritoriality, non-U.S.-exporters need to check whether a U.S.-origin product requires a license and to do so, three pieces of information are needed; the Export Control Classification Number (ECCN), the ultimate destination of the item and the end use and end user of the item.

ECCNs are alphanumeric codes, essential for determining what restrictions or licensing requirements may apply. Certain items, notably those controlled by multilateral export control regimes, are on the CCL[68] and are included in a specific ECCN. If the item is not on the CCL, it may be classified as EAR99, a general category of goods and technology that encompasses many widely traded consumer and industrial items[69]. EAR99 items generally consist of low-technology consumer goods and do not require a license in many situations. However, exporting an EAR99 item to an embargoed country or to an end-user of concern, or in support of a prohibited end-use, may require obtaining a license.

The ECCN in the CCL also includes the reason(s) for control in the License Requirement section. These reason(s), in conjunction with the Commerce Country Chart[70] determine if a license is required for the ultimate destination. If the reexport transaction requires a license, a License Exceptions may be available[71]. The license requirement will also depend on the end-use or end-user if the entity or person is identified on the Entity List. If the end-use or end-user is military, the license requirements might be different from a commercial end-use or end-user.

---

[67] "Commerce Control List (CCL)." *BIS Website*, www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl. Accessed 19 Sept. 2024.
[68] Supplement No. 1 to part 774 of the EAR
[69] "Guidance on Reexports." *BIS Website*, www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions. Accessed 19 Sept. 2024.
[70] Supplement No. 1 to part 738 of the EAR
[71] Part 740 of the EAR

U.S. trade classification coding systems

Trade classification systems, such as HS codes, HTS codes, and Schedule B codes, are crucial for both customs and export control purposes.

The Harmonized Tariff Schedule (HTS) of the United States, administered by the U.S. International Trade Commission (USITC), uses the international Harmonized System (HS), administered globally by the World Customs Organization (WCO) as its foundation. The first six digits of an HTS code are identical to the HS code, which is used globally to classify goods for customs purposes. The HTS then adds four additional digits to provide more specific classification details required for U.S. import regulations. This extended coding helps determine the applicable tariff rates and import duties for goods entering the United States. Exporters in the U.S. must use HTS codes on shipping documents to ensure compliance with customs and export control regulations. These codes also facilitate the collection of trade statistics, informing export control policies and identifying trends in controlled goods.

Schedule B codes, administered by the U.S. Census Bureau, are a 10-digit subset of HTS codes and used by U.S. exporters for statistical purposes and to file electronic export information through the Automated Export System.

While HS codes do not directly determine export control requirements, they can be used alongside ECCNs to meet regulatory standards.

5.1.3 Sanctions in the U.S.

The U.S. government can impose sanctions under several key acts. The International Emergency Economic Powers Act (IEEPA) provides the President broad authority to regulate a variety of economic transactions following a declaration of national emergency. IEEPA, like the Trading with the Enemy Act (TWEA) from which it branched, sits at the center of the modern U.S. sanctions regime[72].

Other acts, such as the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) enhance U.S. sanctions against Iran, particularly targeting its energy sector and financial institutions. Through the Countering America's Adversaries Through Sanctions Act (CAATSA) sanctions are also imposed on Iran, North Korea, and Russia for various activities, including human rights abuses, cyber-attacks, and interference in democratic processes. The Magnitsky Act allows the U.S. to impose sanctions on foreign individuals involved in human rights abuses and corruption and the Foreign Narcotics Kingpin Designation Act targets significant foreign narcotics traffickers, allowing the U.S. to block their assets and prohibit transactions with them.

Sanctions are typically established through executive orders issued by the President or legislation passed by Congress. When the United Nations (UN) Security Council mandates a sanction, the U.S. President enforces it domestically by issuing an Executive Order. Additionally, under the IEEPA, the President can declare a national emergency to address threats to national security, foreign policy, or the economy, and impose sanctions accordingly.

Agencies, such as the Department of State and the Department of Commerce play roles in developing and implementing sanctions policies, particularly in areas like export controls and visa restrictions, however, the Office of Foreign Asset Control (OFAC), part of the Department of Treasury, is responsible for administering and enforcing these economic and trade sanctions based on U.S. foreign policy and

[72] *Product Details R45618*, crsreports.congress.gov/product/details?prodcode=R45618. Accessed 20 Oct. 2024.

national security goals. These sanctions can target specific individuals and entities by maintaining the Specially Designated Nationals and Blocked Persons List (SDN List) but also target entire countries such as Iran or North Korea.

The prominent role of the U.S. in global finance and the widespread use of the U.S. dollar makes OFAC's blocking sanctions a highly effective tool in sanction regulations. When an individual or entity is designated as a Specially Designated National (SDN)[73] or another type of blocked person, their property and interests within U.S. jurisdiction are frozen. U.S. persons are generally prohibited from conducting transactions with these blocked individuals or entities unless authorized by OFAC. Additionally, OFAC's Fifty Percent Rule extends these restrictions to entities that are 50% or more owned by one or more blocked persons, even if the entity itself is not explicitly listed.

Blocking sanctions are a potent tool in the U.S. sanctions arsenal, especially because the U.S.'s outsized role in the global financial system. Upon becoming designated a Special Designated National (SDN), or other type of blocked person, the targeted individual or entity's property and interests in property that come within U.S. jurisdiction are blocked and U.S. persons are, except as authorized by OFAC, generally prohibited from engaging in transactions involving the blocked person.

Non-U.S. companies can be affected by primary and secondary sanctions from the OFAC. Primary sanctions directly apply to U.S. persons and entities, including U.S. citizens, permanent residents, entities organized under U.S. laws, and anyone physically present in the U.S. These sanctions prohibit U.S. persons from engaging in transactions with sanctioned countries, entities, or individuals, encompassing activities like trade embargoes, asset freezes, and travel bans. Violations of primary sanctions can result in civil and criminal penalties, including fines and imprisonment.
However, the extraterritorial reach of these sanctions means that a non-U.S. company with business dealings involving U.S. persons and permanent residents, located anywhere in the world, all nationalities located within the U.S., entities organized in the U.S. or incorporated in the U.S., or any transaction processed vis the U.S. financial system or in U.S. collars, must also comply with OFAC regulations due to the so-called U.S. nexus[74]. Furthermore, non-U.S. entities are prohibited from causing or conspiring to cause U.S. persons to violate U.S. sanctions. This means that if a non-U.S. entity engages in activities that would be illegal for a U.S. person, they can be held accountable.

Under secondary sanctions regimes, such as those included in the Iran and Russia-related sanctions[75] programs, OFAC targets individuals and entities that engage in specified activities. These secondary sanctions are designed to deter foreign entities from conducting business with sanctioned parties by

[73] "18. What Is an SDN?" *Office of Foreign Assets Control | U.S. Department of the Treasury*, ofac.treasury.gov/faqs/18. Accessed 28 Oct. 2024. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked, and U.S. persons are generally prohibited from dealing with them.

[74] In the context of U.S. sanctions, a "U.S. nexus" refers to any connection or involvement with the United States that makes a transaction subject to U.S. laws and regulations. This can include U.S. Dollar transactions, using U.S. financial system or involvement of U.S. persons or entities regardless of their location.

[75] On December 22, 2023, the Biden administration issued Executive Order (EO) 14114 which, among other things, authorizes the OFAC to impose secondary sanctions on foreign financial institutions that facilitate transactions that support Russia's military-industrial base and broadens existing import restrictions on Russian-origin goods to include third-country goods incorporating Russian content. Exec. Order No. 14114, 88 Fed. Reg. 89,271 (2023), https://www.govinfo.gov/content/pkg/FR-2023-12-26/pdf/2023-28662.pdf. EO 14114 amends EO 14024 and EO 14068.

threatening to restrict their access to U.S. markets and financial systems. Consequently, any transactions involving the specified activities can pose a sanctions risk for non-U.S. persons, even in the absence of a direct U.S. nexus.

5.1.4 Conclusion U.S. export controls and sanctions

The extensive reach of U.S. export controls and sanctions significantly impacts non-U.S. companies, compelling them to navigate complex compliance requirements. U.S. export regulations, such as the EAR and ITAR, extend beyond U.S. borders through extraterritoriality, primarily due to the presence of U.S. content in items. This imposes significant compliance burdens on non-U.S. entities, forcing them to understand how U.S. regulations apply to their operations and determine the licensing requirements for reexports or transfers involving items with U.S. content.

The United States can enforce primary and secondary sanctions due to the extensive reach of its economic and financial networks. The U.S. dollar's status as the world's primary reserve currency and the central role of U.S. financial institutions in global transactions create a U.S. nexus that extends the impact of primary sanctions beyond its borders. Added to this is the direct applicability of secondary sanctions, ensuring that OFAC sanctions have a broad reach, forcing non-U.S. entities to align their business practices and compliance strategies with U.S. regulations to maintain access to the U.S. market and financial system.

The U.S. recently extended the statute of limitations for most civil and criminal violations of certain sanctions administered by the OFAC from 5 to 10 years[76].

5.2 Export controls and sanctions in the EU

Export control and trade in the EU is organized through a combination of EU-wide regulations and national measures by individual Member States.

The European Commission regulates export controls, in collaboration with national authorities within each EU Member State. The European Commission sets the overarching framework and guidelines in the Regulation (EU) 2021/821 of 20 May 2021, while the national authorities are responsible for the actual administration and enforcement of the regulation.

Although the European Union establishes a common framework for military export controls, including the Common Military List of the European Union, the actual implementation and management of these controls are the responsibility of national authorities in each Member State. Each Member State maintains its own list of controlled military items and issues licenses for their export and intra-EU transfer. Consequently, while the EU list provides a degree of harmonization, the specifics of military export controls can differ between Member States, reflecting their unique security and foreign policy considerations.

Administrative and criminal penalties for offense on export control regulations are not harmonized at the EU level but determined by the Member States.

[76] "OFAC Guidance on Extension of Statute of Limitations." *Office of Foreign Assets Control | U.S. Department of the Treasury*, ofac.treasury.gov/recent-actions/20240722. Accessed 11 Dec. 2024.

EU legal instruments aimed at blocking U.S. extraterritorial laws

The EU does not recognize the extra-territorial application of laws adopted by third countries and considers such effects to be contrary to international law. This is why it adopted the "blocking statute". The purpose of the blocking statute (Council Regulation (EC) No 2271/96) is to protect EU operators from the extra-territorial application of third country laws. The blocking statute prohibits compliance by EU operators with any requirement or prohibition based on the specified foreign laws. EU operators whose economic and financial interests are affected by the extra-territorial application of those laws are obligated to inform the European Commission[77].

The Blocking Statute aims to protect EU operators by nullifying the impact of any foreign court rulings based on foreign laws within the EU. It allows EU operators to seek compensation in court for damages caused by the extraterritorial application of these specified foreign laws. Additionally, it prohibits EU operators from complying with any requirements or prohibitions stemming from these foreign laws. If EU operators believe that non-compliance with a foreign extraterritorial law would significantly harm their interests or those of the EU, they can request authorization from the European Commission to comply with such a law.

5.2.1 Export control regulators in the EU.

The EU's primary framework for export controls is the Dual Use Regulation, Regulation (EU) 2021/821, which governs the export, transfer, brokering, and transit of Dual Use items. The regulation aims to prevent the proliferation of weapons of mass destruction and ensure that sensitive technologies do not fall into the wrong hands[78]. Each EU Member State maintains its own national control lists, which include items subject to export controls. The European Commission compiles these lists to facilitate better coordination and ensure that Member States can impose authorization requirements on exports of items included in other Member States' control lists.

Dual Use items, which can be used for both civilian and military applications, are controlled under Regulation (EU) 2021/821. In the EU, the administration of Dual Use licenses is managed by national authorities within each Member State, despite the overarching framework being set by EU regulations. Trade classification systems, such as HS codes and TARIC codes, are crucial for both customs and export control purposes in the European Union.

The EU's licensing process for Dual Use items, implemented by the national authorities, includes an assessment of both the intended end use and the end-user to ensure these items are not utilized for harmful activities.

National export control regulators

The EU provides a common list of Dual Use items and general guidelines; however, the actual issuance and management of licenses are handled by national authorities. Each Member State has its own competent authority to ensure compliance with both national and EU regulations, adapting the common rules to their specific administrative and security contexts. For instance, in France, this responsibility falls to the Service des Biens à Double Usage (SBDU).

[77] "Guidance Note on Blocking Statute." *EUR*, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XC0807%2801%29&amp=&qid=1625557217449. Accessed 19 Dec. 2024. Art. 1.1

[78] "EU Enables Coordinated Export Controls by Compiling National Lists." *Trade and Economic Security*, 26 Oct. 2023, policy.trade.ec.europa.eu/news/eu-enables-coordinated-export-controls-compiling-national-lists-2023-10-26_en.

5.2.2 E.U. classification systems for export control and trade.

While trade codes do not directly determine export control requirements, they are often used alongside the EU Dual Use List to meet regulatory standards.

E.U. classification systems for export control.

In the European Union, the equivalent of the Export Control Classification Number (ECCN) is known as the EU Dual Use Classification Number**.** This classification is part of the EU's export control regime, which governs the export of Dual Use times[79]. The EU's Dual Use list is structured similarly to the U.S. Commerce Control List (CCL) and includes categories and subcategories that align with the ECCN system. For example, a Dual Use item classified under a certain ECCN in the U.S. has a corresponding entry under the same designation in the EU list.

Unlike in the U.S., in the EU not all items have an export control classification. However, there is a Catch-All clause[80] in the regulations. This Catch-All clause allows national authorities to control the (re)export of items that are not specifically listed in the EU's Dual Use control list but could potentially be used in ways that go against non-proliferation policies or other security concerns. This clause is particularly important for items that might be used for military purposes, internal repression, or the violation of human rights and international humanitarian law. Under this clause, if an exporter is informed by a competent authority that their items could be used for such purposes, they must obtain an export license even if the items are not listed as controlled Dual Use goods. This ensures that potentially dangerous items do not bypass export controls simply because they are not explicitly listed. Companies can also request that the competent authority in their Member State confirms whether the catch-all clause applies. If it does, they will need to request an export license.

E.U. classification systems for trade.

The Combined Nomenclature (CN) of the European Union, administered by the European Commission, uses the international Harmonized System (HS), administered globally by the World Customs Organization (WCO), as its foundation. The first six digits of a CN code are identical to the HS code, which is used globally to classify goods for customs purposes. The CN then adds two additional digits to provide more specific classification details required for EU import regulations. This extended coding helps determine the applicable tariff rates and import duties for goods entering the EU. Exporters in the EU must use CN codes on shipping documents to ensure compliance with customs and export control regulations. These codes also facilitate the collection of trade statistics, informing export control policies and identifying trends in controlled goods.

TARIC codes, part of the integrated Tariff of the European Union (TARIC), are used for more detailed classification and include additional digits to specify measures such as tariff quotas, anti-dumping duties, and import and export restrictions.

[79] "Exporting Dual Use Items." *Trade and Economic Security*, policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-Dual Use-items_en. Accessed 22 Dec. 2024.
[80] "Regulation - 2021/821 - En - EUR-Lex." *EUR*, eur-lex.europa.eu/eli/reg/2021/821/oj. Accessed 28 Feb. 2025. Article 4

5.2.3 Sanctions in the EU

In the EU, sanctions are described as an instrument to prevent conflict or respond to emerging or current crises, to promote peace and strengthen international security, develop, and consolidate democracy, with respect for the rule of law, human rights, and fundamental freedoms.

The policy framework used by the European Union (EU) to coordinate its foreign policy and security measures, including sanctions, is called CFSP and stands for Common Foreign and Security Policy[81].

The CFSP allows the EU to impose restrictive measures, such as travel bans, asset freezes, and trade restrictions, in response to actions that threaten international peace and security.

All restrictive measures the EU decides on are listed on the EU Sanctions Map, which provides detailed information on all the sanctions imposed by the European Union. These sanctions are grouped by country, entity, and thematic areas, and they include several types of restrictions such as financial sanctions, travel bans, trade restrictions or sectorial sanctions. Restrictive measures are imposed due to various reasons, such as human rights violations, terrorism, cyber-attacks, and the proliferation of weapons of mass destruction.

The EU implements all sanctions adopted by the UN Security Council by transposing them into EU law. This ensures that UN sanctions are uniformly applied across all EU Member States[82]. National authorities use the EU Sanctions Map[83] as a basis for implementing these measures within their jurisdictions. They may also add additional national sanctions to address specific concerns or situations.

Member States must ensure that violating EU sanctions is punishable by effective and proportionate criminal penalties, which vary depending on the offence. However, intentional violation of sanctions must give rise to a prison sentence as the maximum penalty[84]. The penalties for any breach of EU restrictive measures are dependent on the national legislation of EU Member States, however, in April of 2024, the Council adopted a law covering EU-wide minimum rules for the prosecution of violation or circumvention of EU sanctions in Member States, whereby certain actions will now be considered criminal offences in all Member States, for example helping to bypass a travel ban, trading in sanctioned goods or performing prohibited financial activities[85]. Inciting, aiding, and abetting these offences can also be penalized.

5.3 EASA regulatory requirements versus sanctions compliance

Under the European Union Aviation Safety Agency (EASA) regulations, aerospace OEMs must meet several key requirements to ensure continued airworthiness and safety. Firstly, they must provide airlines with comprehensive Instructions for Continued Airworthiness (ICA), which include maintenance

[81] *Foreign Policy: AIMS, Instruments and Achievements: Fact Sheets on the European Union: European Parliament*, www.europarl.europa.eu/factsheets/en/sheet/158/foreign-policy-aims-instruments-and-achievements. Accessed 22 Dec. 2024.
[82] *Types of Sanctions the EU Adopts - Consilium*, www.consilium.europa.eu/en/policies/sanctions-different-types. Accessed 22 Feb. 2024.
[83] "EU Sanctions Map." *EU Sanctions Map*, www.sanctionsmap.eu/#/main. Accessed 22 Dec. 2024.
[84] *Why the EU Adopts Sanctions - Consilium*, www.consilium.europa.eu/en/policies/why-sanctions. Accessed 22 Dec. 2024. Section: Violating sanctions is a crime.
[85] *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Definition of Criminal Offences and Penalties for the Violation of Union Restrictive Measures and Amending Directive (EU) 2018/1673*, European Union, 3 Apr. 2024, data.consilium.europa.eu/doc/document/PE-95-2023-INIT/en/pdf.

manuals, service bulletins, and other necessary documentation to ensure the aircraft remains airworthy throughout its operational life. OEMs are also required to provide detailed Component Maintenance Manuals (CMM) for the maintenance of individual components, including instructions for inspection, testing, repair, and overhaul. Furthermore, they must issue Airworthiness Directives (ADs) to address any identified safety issues, providing mandatory instructions for corrective actions to maintain safety. Finally, OEMs must maintain detailed records of all maintenance, modifications, and inspections performed on the aircraft, which are crucial for tracking the airworthiness status of the aircraft[86].

When sanctions against Russia were imposed in 2022, EASA published an FAQ[87] confirming that the sanctions regulations take precedence over continued airworthiness support obligations of the EU Type Certificate Holders (TCHs)[88] and other design approval holders[89], resulting in that decisions by sanctioning authorities take precedence over the Type Certificate (TC)[90] holders' obligations towards safety. This means that decisions by EU based sanctioning authorities take precedence over the OEMs' obligations towards safety.

5.4 Conclusion: Navigating tension between the U.S. and EU regulations

While there are similarities between U.S. and EU export control regulations and overlapping sanctions, the challenges arise from the differences between the regulations.
Each transaction must be evaluated against both EU and U.S. export control regulations and screened against all relevant EU and U.S. sanctions and restrictive measures lists.

5.4.1 Extraterritorial overreach of the U.S.

Despite the EU's efforts to counter the effects of U.S. legislation by means of the blocking statute to prevent the U.S. from exerting far-reaching jurisdiction concerning export control and sanctions over EU entities, these measures are often mitigated, leading to ongoing struggles in achieving efficiency. This became evident as most EU companies ceased activities in Iran[91]. The U.S. Department of Justice often negotiates heavy fines with European companies to avoid further prosecution. However, fines and penalties for violating U.S. export controls and sanctions are still being enforced.

Businesses in the EU must not only comply with EU and national regulations but also verify whether U.S. jurisdiction applies to their transactions. When exporting, this determination involves performing de minimis calculations and applying the Foreign Direct Product Rule to classify all items or gathering classification information from suppliers. Not only is the U.S. controlling all parts it considers under its

[86] "Continuing Airworthiness." *EASA*, www.easa.europa.eu/en/regulations/continuing-airworthiness. Accessed 23 Dec. 2024.
[87] "EU Restrictive Measures against Russia." *EASA*, www.easa.europa.eu/en/the-agency/faqs/eu-restrictive-measures-against-russia. Accessed 19 Dec. 2024.
[88] The TCH, or Type Certificate Holder is the holder of the Type Certificate (TC), and as such is responsible for ensuring that the aircraft design remains compliant with safety standards and regulations.
[89] In particular Article 3c (4)(a) of Regulation (EU) No 833/2014, as amended by Council Regulation (EU) 2022/328 of 25 February 2022
[90] Type Certificate (TC) is a certificate issued by a regulatory authority, such as EASA, to signify the airworthiness of an aircraft's design.
[91] "United States Extraterritoriality: European Union Sovereignty at Stake." *International Bar Association*, www.ibanet.org/article/CF85E59E-6564-4AA3-9408-3F47C6449C9D#_edn12. Accessed 18 Dec. 2024.

jurisdiction, it also controls the reexport and transfer of those items regardless of how many times it is reexported, transferred or sold.

The U.S. plays a crucial role in enforcing global sanctions, leveraging the dominance of its banks and the U.S. dollar to extend its legal reach. Companies that defy U.S. sanctions, risk exclusion from the U.S. market and potential criminal charges for their CEOs. As a result, EU-based companies often prioritize U.S. laws over EU regulations. Therefore, businesses in international markets must develop compliance and export control programs that consider sanctions from the EU, national authorities, and especially the U.S.

5.4.2 Differences regarding sanctioned parties

Both the U.S. and EU implement UN sanctions, but they can also impose their own sanctions independently to address specific national security and foreign policy objectives. Although there is commonality in the sanctioned entities, differences exist between them. For OEMs, this can lead to a dilemma when a person or entity is affected by a blocking sanction in the U.S. but not in the EU. Under EASA regulations, a minimum of safety documentation needs to be provided to airlines. However, under the U.S. sanction forbids transactions with this entity or person. This means that the OEM must determine which documentation cannot be shared with the airline due to U.S. content and therefore subject to sanctions. Consequently, the information that the OEM is allowed to share may not meet the EASA requirements for minimum safety documentation.

The effects of restrictions often reach beyond the parties identified by name on these lists. By OFAC's Fifty Percent Rule[92], blocking sanctions generally also extend to entities owned 50 percent or more in the aggregate by one or more blocked persons, whether the entity itself has been explicitly identified. In the EU (and UK), however, there are even broader ownership and control tests to determine that entities are majority-owned or controlled by blocked persons. Compliance programs need to consider these differences in regulations.

Determining the right course of action when deciding to do business can be challenging. Even though the rules may seem black and white, the analysis can be complex, and the outcome is often not clear-cut. Companies must navigate these nuances carefully to ensure compliance while meeting their operational needs and obligations.

5.4.3 Differences in classifications

The differences in export control classification systems require companies to be aware of both U.S. and EU classification systems. As illustrated below, the U.S. controls a wide range of items, while the EU primarily focuses on Dual Use items. Although there is significant commonality in the classifications of items that both systems regulate, there are also notable differences. For instance, the U.S. has moved some military items to its commercial control list, the so called "500" and "600" series, whereas similar items in the EU mostly remain on military lists.

[92]"Entities Owned by Blocked Persons (50% Rule)." *Office of Foreign Assets Control | U.S. Department of the Treasury*, ofac.treasury.gov/faqs/topic/1521. Accessed 1 Aug. 2024.

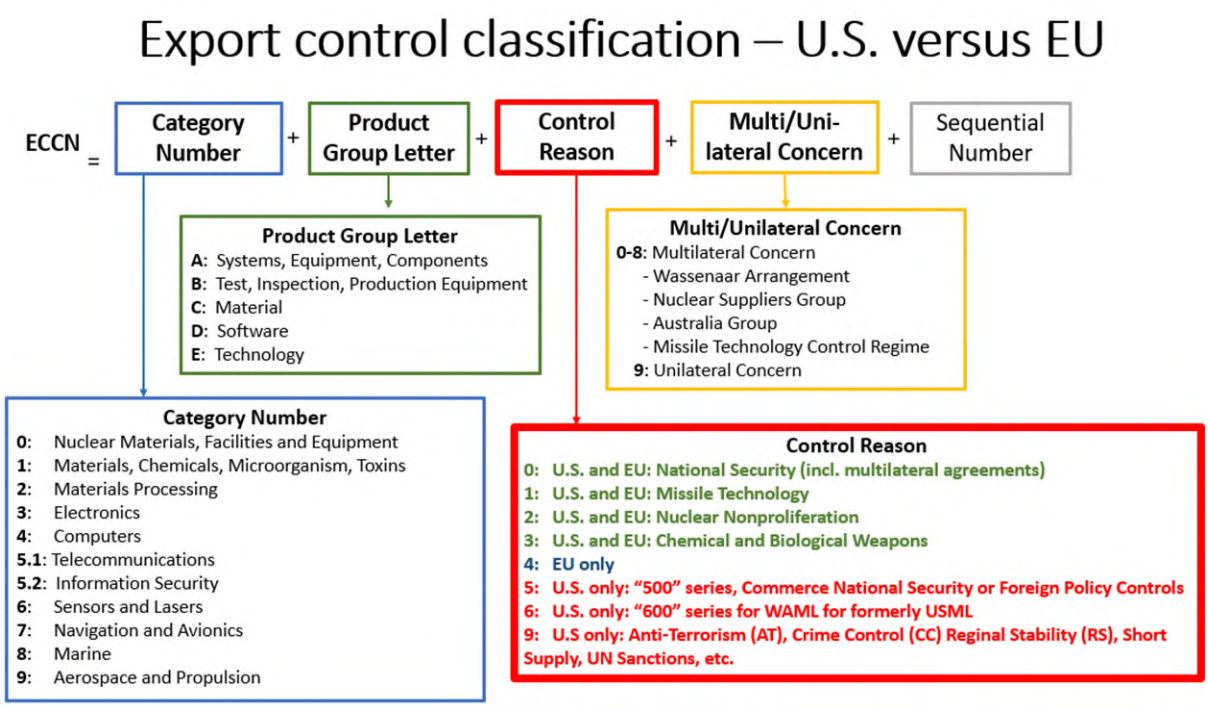


Figure 1: Export control classifications in the U.S. versus EU

When exporting, it is essential to mark each item with a control destination statement. Given that the U.S. imposes extensive export controls compared to the EU, this marking process can be complex to program into an IT system. It must account for various jurisdictions and classifications, as well as the end use, end user, and final destination.

5.4.4 Different approaches to export license determination between the EU and U.S.

Although the EU Member States and the U.S. collaborate on international export control regimes, resulting in largely harmonized lists of controlled Dual Use items, their approaches to determining export license requirements differ significantly. The EU's approach is straightforward: controlled Dual Use items require a license for exports outside the EU. It must then be determined whether a General License at the EU or national level is available, or if an individual export license is needed. Within the EU, Dual Use items generally do not require an export license, except for specific notification obligations. The EU does not use a "No license required" (NLR) designation, but export declarations with customs authorities include codes to indicate where licenses are required and available.

The U.S. approach to export controls is more detailed, considering both the reason for control of an item and its destination using the Commerce Country Chart[93] to determine if a license is required. If a license is needed, it must be checked if a License Exception is available, along with other prohibitions. While this allows for more nuanced handling of specific destinations, the EU approach is simpler and less complex for operators, which is likely why many jurisdictions adopt the EU approach when implementing or

[93] *Commerce Country Chart - Bis*, 8 Dec. 2023, www.bis.doc.gov/index.php/documents/regulations-docs/2253-supplement-no-1-to-part-738-commerce-country-chart/file. This chart helps determine if an export license is required based on the reason for control of an item and its destination.

enhancing national export controls. Conversely, no jurisdiction is known to have adopted the U.S. approach.

For EU businesses that re-export or incorporate U.S. items, both approaches must be considered, even within a single transaction.

5.4.5 Reporting violations

Reporting violations across these jurisdictions introduces another layer of complexity. In the U.S., the Office of Export Enforcement (OEE) within the Bureau of Industry and Security (BIS) is primarily responsible for investigating and prosecuting export control violations. The U.S. has a well-established system for tip-offs and voluntary self-disclosures, encouraging companies to report any suspected non-compliance[94].

The EU provides a whistleblowing tool[95] for reporting sanctions breaches. From an export controls perspective, reports should be submitted to the nearest competent national authority, however, contrary to the U.S., not all EU Member States provide statutory regulations on voluntary self-disclosures. For instance, Germany does not have such regulations for material violations of export control and sanctions, but only for some minor formal mistakes.

In the EU, the role of customs authorities is pivotal in identifying export control violations. They work alongside national authorities to ensure compliance with export regulations. However, the mechanisms for reporting violations can vary significantly from one Member State to another.

5.5 Export control and sanctions compliance program implementation in aerospace OEMs

Building an export control and compliance program that adheres to both U.S. and EU regulations is a complex and demanding task. It requires a thorough understanding of the regulatory landscape, meticulous planning, and the implementation of robust internal controls. Companies must develop an Internal Compliance Program[96] (ICP) or Export Control Program[97] (ECP) to meet these stringent requirements. The EU Dual Use regulation defines internal compliance program (ICP) as “ongoing effective, appropriate and proportionate policies and procedures adopted by exporters to facilitate compliance with the provision and objectives of the regulation, including inter alia, due diligence measures assessing risks related to the export of the items to end-users and end-uses”.

Senior management's support is crucial, as it fosters a culture of compliance and ensures the allocation of necessary resources, including the appointment of a compliance officer with clearly defined authority and responsibilities.

Regular risk assessments are essential to identify potential compliance risks related to export controls and sanctions. This involves evaluating products, customers, and transactions to pinpoint vulnerable

[94] The reporting of violations under the EAR is specified in 15CFR764.4 and has been amended recently by BIS.
[95] *Eqs Integrity Line*, eusanctions.integrityline.com/frontpage. Accessed 12 Nov. 2024.
[96] “COMMISSION RECOMMENDATION (EU) 2019/1318 on Internal Compliance Programmes for Dual Use Trade Controls under Council Regulation (EC) No 428/2009.” *EUR*, 30 July 2019, eur-lex.europa.eu/eli/reco/2019/1318/oj/eng.
[97] Andrukonis, Tom. *Internal Compliance Program Elements*, www.bis.doc.gov/index.php/documents/compliance-training/export-administration-regulations-training/244-compliance-pdf/file. Accessed 15 Oct. 2024.

areas. Additionally, companies must establish processes to ensure that all exports, reexports, and transfers are properly authorized and comply with the conditions specified in obtained licenses.

The BIS specifies that export authorization aims to establish procedures, processes, and process flows to help employees make consistent and correct export decisions and consists of the following elements: jurisdiction, classification, license determination and screening.

Screening procedures must clearly define what is being screened, specify the lists to be used, and detail how the process is integrated into business operations. It should outline when screening needs to be completed, its frequency, and identify who is subject to screening. Additionally, it should specify the information required from purchasers, consignees, and other intermediaries. Special attention must be given to the end user, considering the risk of diversion during screening. The process should include methods for resolving false positives, specify the system used for screening, and describe how the screening process is audited.

Maintaining proper records of all export transactions, including licenses, shipping documents, and communications with regulatory authorities, is mandatory for the specified period as required by the relevant regulations.

Tailored training for employees involved in export activities should be provided regularly, emphasizing the importance of compliance and the potential consequences of violations. Enhanced due diligence processes to screen customers, suppliers, and other third parties against all relevant restricted party lists from both the U.S. and EU should be implemented to ensure that transactions do not involve prohibited entities or individuals.

The companies' compliance program is expected to have comprehensive internal controls, including written policies and procedures for export control and sanctions compliance, covering areas such as employee training, corrective actions, record-keeping, and internal audits to ensure ongoing compliance. Regular internal audits and monitoring should be conducted to identify and address any compliance gaps or potential violations. The program should also include procedures for reporting potential violations to regulatory authorities and making voluntary disclosures when necessary.

Both U.S. and EU Member State authorities expect that an export control program undergo regular reviews and updates to address new risks, incorporating feedback from audits, monitoring activities, and changes in the regulatory environment.

Implementing an export control and sanctions compliance program at an OEM requires a thorough understanding of how the business intersects with both EU and U.S. regulations, and IT solutions are a necessity. Aerospace OEMs generally have complex supply chains and customers on many continents, resulting in the export of items to various locations. The combination of items, tangible and intangible, with many different export control classifications, complicated by the differences in both EU and U.S. classification, and the extraterritoriality of U.S. export controls, with many "sold-to" and "ship-to" entities all needing to be screened, necessitates robust internal procedures and extensive IT systems tailored to each jurisdiction's specific requirements.

Traditionally, internal export and compliance programs are built around the requirements described from both the BIS and EU requirements and guidance.

Leveraging technology to automate aspects of export control and compliance management, such as screening and classification, can enhance efficiency and accuracy. Compliance with evolving export control and sanctions regulations can be considerable as it might touch on every aspect of the program. IT systems might have to be updated, processes, procedures, and internal controls rewritten, requiring training of the stakeholders in the company.

5.6 Summary and Conclusion

EU businesses need a comprehensive approach that covers both EU and U.S. regulations due to significant differences between the two jurisdictions. The EU's extraterritorial reach in sanctions is much less extensive than that of the U.S., which includes a general de minimis threshold and applies its regulations across borders. The EU's blocking regulation reflects its concerns about such wide extraterritorial reach; however, most companies comply with U.S. regulations out of fear of fines and being shut out of the U.S. market.

In the EU, liability for export control violations requires at least negligence, whereas the U.S. can impose civil penalties under strict liability. Media coverage of violations also differs, with the U.S. providing detailed information about companies and their violations on official websites, a practice not common in the EU.

The statute of limitations for prosecuting export control and sanctions violations differs between the U.S. and the EU. Therefore, compliance programs must account for these differences by ensuring that records are maintained for the appropriate duration in each jurisdiction. Specifically, all records with a U.S. nexus now need to be kept for 10 years to comply with the extended statute of limitations.

Despite discussions about harmonizing export control and sanctions between the EU and U.S., substantial differences in content and procedures remain.

Due to these differences, OEMs have faced significant challenges in implementing export control and compliance programs. This has necessitated IT solutions such as for export control classification, screening of end users and end uses, marking with the proper control destination statements of exported items, throughout the entire value chain, from product conception to serving the aftermarket. The IT systems, processes, procedures, and training required to comply with both EU and U.S. export control and compliance programs are critical for ensuring compliance. However, these requirements are not easily or quickly adapted to new regulations that fall outside the scope of the existing setup within the company. Once systems and procedures are in place, adapting them to rapidly changing regulations, such as those related to sanctions on Russia regarding diversion and circumvention, presents an additional significant challenge.

6 Impacts of sanctions on the OEMs

6.1 Introduction

Regulators imposed sanctions that legally required aerospace companies to halt their business activities with Russia and established a program to prevent the circumvention of these sanctions and the diversion of items to Russia. These measures were enforced through Compliance Notes issued by U.S. authorities and Sanctions Packages from the EU.

The foundation for all the EU sanction packages in response to Russia's destabilizing actions in Ukraine in 2022 can be found in the 2014 Regulations. The initial sanctions were established by Council Regulation (EU) No 833/2014[98] and Council Regulation (EU) No 269/2014[99]. These regulations complement each other, with Regulation 269/2014 focusing on targeted sanctions against individuals and entities, while Regulation 833/2014 addresses broader economic measures. The sanctions packages build upon the 2014 regulations by introducing more comprehensive measures to address the evolving situation and enhance the effectiveness of the sanctions. U.S. sanctions against Russia are organized under several key programs and legal authorities. The primary framework is established by Executive Order 14024[100], which targets harmful foreign activities of the Russian government.

Following the initial sanctions, the aerospace industry had a brief wind-down period to cease business activities. Subsequent sanctions have primarily targeted preventing diversion and circumvention. This chapter provides a high-level summary of significant measures imposed by authorities that affect the aerospace sector, particularly those aimed at enhancing the effectiveness of sanctions and preventing their evasion through diversion and circumvention, specifically as they apply to aerospace OEMs. While most sanction packages and compliance notes include measures affecting aerospace, only the most significant ones are highlighted, and sanctions in place before February 2022 and those imposed after the EU's 14th package are not covered.

By applying Giumelli's[101] theoretical framework, the predicted outcomes of these sanctions are compared with insights gathered from interviews with the OEMs, providing real-world evidence to support our theoretical predictions. Additionally, this analysis contrasts these sanctions with the typical workload in a compliance department, illustrating their unique impact on OEMs. This comparison aims to evaluate the accuracy of the theoretical predictions against the actual responses from the industry.

Finally, the overall effect to the sanctions are assessed, supported by interview findings, and provide a final summary of our conclusions.

---

[98] "Council Regulation (EU) No 833/2014 of 31 July 2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine." *EUR*, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0833. Accessed 31 July 2014.

[99] "Council Regulation (EU) No 269/2014 of 17 March 2014 Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine." *EUR*, 17 Mar. 2021, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269&qid=1731687869032.

[100] In contrast, earlier sanctions, such as those under Executive Orders 13660, 13661, 13662, and 13685, primarily focused on the crisis in Ukraine and targeted specific sectors like defense and energy.

[101] Giumelli *The role of for-profit actors in implementing targeted sanctions: The case of the European Union* pp. 123-141

6.2 Interviews and analysis

Due to the current emphasis on regulatory penalties and fines, and the need to protect the confidentiality of compliance program weaknesses, the interviews were conducted anonymously. All participants insisted on anonymity due to the sensitivity of the data and the relevance of the topic.

Export control personnel from four OEMs in leading roles were interviewed. The study included full-time professionals from the export control and sanctions departments, all of whom had over six years of experience in the aerospace export control and sanctions domain and had been in their roles since the sanctions on Russia in 2022.

All participants work for multinational companies with divisions on several continents. These companies, whose main shareholders are involved in industries such as aerospace, defense and space, cybersecurity, communication, infrastructure, automotive, and medical equipment, have complex supply chains and partnerships. The companies interviewed were mostly OEM, but also include "built to print" manufacturing for other businesses.

It is important to note that these OEMs have different situations in the marketplace. While all the companies that participated in this research are part of large conglomerates, they face very different competitive situations in the market, ranging from producing products for which demand exceeds their capacity to deliver, to having a more challenging competitive situation.

Participants expressed discomfort with being recorded. Therefore, to ensure their privacy and encourage candid responses, interviews were conducted in person or via online video meetings. Detailed notes were taken during the conversations and summarized to highlight the main themes and responses without directly attributing specific statements to individual participants. All interviewees offered to answer or clarify questions if needed afterward.

Interviews were semi-structured to ensure that the main topics were addressed, while also allowing room for 'opportunity comments,' meaning views that were not necessarily part of the interview protocol. All interviewees provided additional interesting insights and information or reiterated important points expressed earlier in the interview.

From detailed notes, all comments were sorted by topic to assess the overall impact as high, medium, or low, and to identify any major differences in how companies experienced and handled the measures. These findings are described further in this chapter.

6.3 Integrating theory and practice: evaluating sanctions and compliance programs

To bridge the gap between the theoretical framework on compliance with sanctions and the reality of their implementation, the typology proposed by Giumelli (2017) in "The Role of For-Profit Actors in Implementing Targeted Sanctions: The Case of the European Union" is used. This framework helps predict the level of implementation based on the clarity of instructions and the capacity to monitor and enforce compliance, providing an understanding of how these actors implement sanctions.

The interview analysis and conclusions will offer insights into the actual behavior of OEMs in terms of compliance, specifically addressing overcompliance, uneven compliance, and lack of compliance.

Guimelli (2017) argues that effective implementation of sanctions occurs when authorities provide detailed instructions and have a high capacity for monitoring. When monitoring capacity is high, but instructions are vague, there is a risk of overcompliance. Conversely, low monitoring capacity with detailed instructions results in compliance that varies based on the company's location. Finally, low monitoring capacity combined with vague instructions leads to a lack of compliance, with behavior largely dependent on the type of company involved. The author proposes the following four typologies of regulatory environments, and the behavior demonstrated by the companies. The typologies are:

A. Enforceable Implementation: Clear instructions and strong monitoring or enforcement; governments can specifically outline what private actors are supposed to do and monitor their behavior to enforce the regulation. The problem of compliance is not considered.
B. Implementation by Persuasion: Clear instructions but weak monitoring or enforcement; public authorities can provide detailed regulation, but monitoring cannot be properly done. The problem would be the level of compliance depends on the location of the company.
C. Enforceable Delegation of Implementation: Vague instructions but strong monitoring or enforcement; the authorities have the power to monitor the behavior of non-state actors, but clear and specific instructions cannot be provided. The expected level of compliance would be overcompliance
D. Delegation of Implementation by Persuasion: Vague instructions and weak monitoring or enforcement; private actors do not know exactly what they have to comply with, and public authorities cannot monitor what they do. Examples include instructions such as “block suspicious activities” and “no funds shall be made available indirectly or directly,” where "suspicious" and "indirectly" are not clearly defined. The problem being lack of compliance and behavior depending on the type of company.

6.4 Initial sanctions: halting aerospace exports

On 23 February 2022 the EU's "first package[102]" of restrictive measures was published, but it is the second package of 25 February that directly targeted the aviation sector, similar to the U.S. sanctions measures of 24 February 2022. The U.S. government enforced extensive export control restrictions on Russia under the EAR[103] and sanctions under the OFAC[104]. These measures include export bans on shipping certain U.S. goods, technology, and software to Russia without a license, even if previously no U.S. authorization was needed. Additionally, there is a general policy of denying such license requests, with limited exceptions, and restrictions on using U.S.-origin technology and equipment to produce items for Russia. Additionally, the Countering America's Adversaries Through Sanctions Act (CAATSA) and the Magnitsky Act also play significant roles in sanctioning Russian individuals and entities for human

[102] Asset Freeze: CIR (EU) 2022/261 of 23 Feb. 2022 implementing Regulation (EU) No 269/2014
Financial and investment restrictions: CR (EU) 2022/262 of 23 Feb. 2022 amending Regulation (EU) No 833/2014 (reflecting the adoption of CD (CFSP) 2022/264 Sectorial sanctions: CR (EU) 2022/263 of 23 Feb. 2022
[103] “U.S. Department of Commerce & Bureau of Industry and Security Russia and Belarus Rule Fact Sheet.” *U.S. Department of Commerce*, 14 Mar. 2022, www.commerce.gov/news/fact-sheets/2022/02/us-department-commerce-bureau-industry-and-security-russia-and-belarus.
[104] “Russia-Related Sanctions.” *Office of Foreign Assets Control | U.S. Department of the Treasury*, ofac.treasury.gov/sanctions-programs-and-country-information/russia-related-sanctions. Accessed 12 Oct. 2024.

rights abuses and corruption. The OFAC administers these sanctions, issuing directives and maintaining a list of sanctioned individuals and entities.

The U.S. sanctions measures from 24 February 2022, impacted all ECCNs contained in categories 3-9, which now required a license to be exported to Russia. This covers items such as navigation equipment and avionics (category 7), and aircraft components (category 9).
Two new Foreign Direct Product Rules (FDPRs)[105] significantly restrict Russia's ability to obtain U.S. and certain foreign-made aerospace items, including those with U.S. components[106]. Restrictions on Russian Military End Users (MEU) have also been expanded to cover a broader category of items and are no longer limited by the specified categories on the CCL[107]. Now, all items subject to the EAR require a license to be exported, re-exported, or transferred (in-country) to a MEA with some exceptions.

Any license granted for any Russian party, under the U.S. Dual Use regulations (EAR), was suspended as of 3 March 2022 without confirming the eligibility of using license exceptions.

For the purposes of determining U.S.-origin controlled content when making a de minimis calculation for reexports to Russia, exporters may exclude U.S. origin content controlled for Anti-Terrorism (AT) reasons and ECCN 9A991 items only if the foreign-produced item will be reexported or exported from a country (e.g., the EU countries) that has adopted similar export controls on exports, reexports, and transfers (in-country) to or within Russia, as determined by the U.S. In essence, these measures significantly restrict Russia's ability to obtain U.S. and certain foreign-made aerospace items, that include U.S. components.

The European Union also published restrictive measures in response to Russia's actions in Ukraine directly targeting the aerospace sector. In the 2nd sanctions package, effective from 26 February 2022, companies were required to implement a comprehensive export ban on goods and technology[108,] including a prohibition on Dual Use goods and technology[109], a prohibition on technical and financial assistance[110] and a prohibition on aviation and space industry goods and technology. For contracts concluded before 26 February 2022, these prohibitions would not apply until 28 March 2022.

[105] The first results in many additional foreign-produced items now being subject to the EAR. The second, the new Russia-Military End User (MEU) FDPR further restricts Russia's access to critical technologies and components needed for its military capabilities.
[106] *Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex*, 14 Oct. 2022, ofac.treasury.gov/media/928856/download?inline. .
[107] The Russian entities on the MEU List have all been moved to the Entity List at Supp. 2 of Part 744.
[108] Trade: CR (EU) 2022/328 of 25 Feb 2022 amending Reg. (EU) No 833/2014 – update/new Art. 2, 2a-d, 3b-c.
Ban on public funding: CR (EU) 2022/328 of 25 Feb 2022 amending Reg. (EU) No 833/2014 – new Art. 2e.
Financial investment: CR (EU) 2022/328 of 25 Feb 2022 amending Reg. (EU) No 833/2014 – amendments to Art. 5.
Financial facilities/deposit: CR (EU) 2022/328 of 25 Feb 2022 amending Reg. (EU) No 833/2014– new Articles 5b-g. Additional basis for designations: CR (EU) 2022/330 of 25 Feb 2022 amending Reg (EU) No 269/2014. Asset freeze: CIR (EU) 2022/332 of 25 Feb 2022 implementing Reg (EU) No 269/2014.Visa: CD (EU) 2022/333 of 25 Feb 2022.
[109] The direct or indirect sale, supply, transfer, or export of all Dual Use goods and technology to Russian airlines was banned. However, for contracts concluded before 26 February 2022, Member States could authorize such activities for non-military use and non-military end users if authorization requests were made before 1 May 2022. Exceptions to the Dual Use prohibition were allowed in limited circumstances, such as government-to-government exports for purely civil cooperation, intergovernmental cooperation in space programs, or for diplomatic representations.
[110] Similar to the Dual Use goods prohibition, Member States could authorize these activities for non-military end use and non-military end users if requests were made before 1 May 2022.

There was also a prohibition of aircraft and component services, such as overhaul, repair, inspection[111], replacement, modification, or defect rectification of an aircraft or component.

Package 2 forced aerospace OEMs to cease immediately all Maintenance, Repair, and Overhaul (MRO) activities, apply for European Dual Use licenses from their national authorities for the delivery of any parts and services to Russian airlines by 1 May 2022, and suspend or wind down all their contracts with Russian Airlines by 28 March 2022.

The EU's third package from 28 February 2022, included an airspace ban on any Russian registered, or non-Russian-registered aircraft owned, chartered, or controlled by Russian entities or individuals[112] from flying into, over or out of the territory of the European Union[113]. Furthermore, there were additional financial restrictions on the Central Bank of Russia, and asset freezes on senior businesspeople, oligarchs, government ministers, journalists, and senior military personnel.

OEMs reaction and perception of the initial sanctions

One of the four companies interviewed was not affected by the initial sanctions as they had already cut all direct business ties with Russia in 2014, perceiving it as too risky due to their significant involvement in military products. This division decided already in 2014 that pursuing business for their commercial applications was no longer worthwhile. Three out of four companies, however, had extensive business relations with Russian entities and all indicated that at first, they scrambled to understand the impact, but quickly realized they would need to withdraw from Russia as fast as possible. The extensive restrictions meant the export control and compliance departments communicated internally that all exports to Russia had to stop and apply export control blocks in their systems for goods, software, training and technical documentation. While it is usual business in a compliance department to update systems to block certain items or destinations for export, it had never been done on this scale before. Products ready for delivery had to be halted and reintegrated into the production process or returned to the warehouse.

The wind-down period of about four weeks to negotiate the suspension of contracts with Russian counterparts and retrieve all on-site materials, such as spare parts in exchange pools, manufacturing, and test equipment, was insufficient, resulting in losses from left-behind material and abandoned partnerships. All three companies reported that the process of retrieving material was greatly hampered by the limited availability of flights due to counter sanctions from Russia and the airspace ban from the EU and U.S. Freight forwarders became overwhelmed with the increased demand for their services and scrambled to navigate the complex logistics of moving goods in and out of sanctioned regions. Additionally, the sanctions led to increased scrutiny and regulatory hurdles at customs, adding another layer of complexity to the process of reclaiming assets. Contractually, title exchanges for on-site stock and unserviceable material already with the OEM for repair, had to be signed between Russian companies and OEMs before transport could be arranged. One company reported missing the deadline by one day, resulting in ongoing consequences from the unavailability of components. To this day, they have not managed the title exchange for the material with Russian tags in their warehouse. Two other

[111] except for pre-flight inspections.

[112] Included also or any Russian registered aircraft, any non-Russian-registered aircraft which is owned, chartered or controlled by any Russian person/entity, to land in, take off from or overfly the territory of the EU, except in emergencies.

[113] by two amending acts, published in the OJ L 77 of 28 February 2022, Council Regulation (EU) 2022/334, also amending Council Regulation (EU) 833/2014, Council Decision (CFSP) 2022/335, which amends again Decision 2014/512/CFSP.

companies believe that the Russian airlines they had to leave material with are still in reasonable condition today because they have access to a warehouse full of components.

Two companies needed to consult with outside counsel to properly halt business and suspend all contracts, where the other one had a large enough legal department to handle it internally.

Ensuring that companies were not involved with certain sanctioned financial institutions and their subsidiaries[114] affected all four to a certain extend. Specifically, one company mentioned that it was difficult to determine how and if some payments could still be received and made. Although they did not need any outside counsel, they felt there was not sufficient time, and had to call people back on weekends and pull people away from other functions and projects to determine if any transactions involved sanctioned banks and their subsidiaries and if exception or exemption could be applied. The measures affected pending payments for rendered services and goods which could no longer go through, leaving this OEM with unrecoverable debt on their balance sheets.

The three affected OEMs spent considerable time, under significant time pressure, checking the regulations and potential license requests to ensure that pending deliveries or retrieving their material from Russia was possible and compliant, and two out of three consulted with outside counsel for a proper understanding of the measures.

Effectiveness and actual implementation of the initial sanctions
The interviews indicate that initial sanctions were well understood, but for business there was the main issue of the short wind-down period. However, the instructions can be considered clear. The enforceability of the early sanctions was high, as exports to Russia could be monitored by customs. According to Giumelli (2017), when there are clear instructions and a strong ability by the authorities to enforce sanction measures, compliance is not an issue. The interviews indeed confirm compliance by the businesses interviewed.

6.4.1 Misinterpretations of technical assistance regulations.

On 21 July 2022, Council Regulation (EU) 2022/1269[115] came out stating that “In order to safeguard the technical industrial standard setting process of the International Civil Aviation Organization (ICAO)[116], Decision (CFSP) 2022/1271 allows the sharing of technical assistance with Russia in relation to aviation goods and technology in this specific framework.” However, the new exception introduced by this Council Regulation served a narrow purpose, not altering the position previously taken on the provision of the technical assistance since the beginning of the war in Ukraine: provision of technical assistance to Russian airlines was still not allowed per the applicable laws and regulations.

OEMs reaction and perception to the technical assistance regulation update
Based on interview findings, it appears that there was significant confusion among airlines and OEMs and their suppliers regarding their rights to access technical documentation. Russian airlines believed

[114] Institutions now listed as Specially Designated Nationals (SDNs), or their subsidiaries could no longer be used for transactions such as payments
[115] “Council Regulation (EU) 2022/1269 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia’s Actions Destabilising the Situation in Ukraine.” *EUR*, 12 July 2022, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1269.
[116] The International Civil Aviation Organization (ICAO) coordinates international air navigation and establishes international standards and regulations for aviation safety, security, efficiency, and environmental protection.

they had regained the right to obtain technical documentation assistance, and OEMs and their suppliers did not seem sure at first. With help from corporate offices and outside counsel the new rule was quickly clarified, and a communication was sent to Russian entities who had contacted the OEMs, repair stations, and support organizations, that basically nothing had changed.

Effectiveness and actual implementation of the technical assistance regulation update
Overall, the findings highlight the need for comprehensible regulation updates to ensure that all parties understand their rights and responsibilities under the new rule. Misunderstanding can lead to invertedly violating a regulation. In this case, it required significant time and effort from compliance personnel and legal departments to communicate internally and to Russian operators that nothing had changed.

6.5 Additional sanctions – introducing circumvention and diversion

From March 2022 to June 2023 the EU published sanctions packages 3 to 14, during which the existing restrictions were expanded, mainly by package 4, 11, 12 and 14 in which new measures were introduced to address sanctions evasions. The U.S. sanctions updates mirror in many cases the EU requirements.

6.5.1 Enforcing sanctions on oligarchs

To target Russian oligarchs and their illicit activities, the U.S. Department of Justice launched Task Force KleptoCapture[117] on March 2, 2022. This task force was established to enforce sanctions, export restrictions, and economic countermeasures against Russian oligarchs and entities in response to Russia's invasion of Ukraine. Its purpose is to ensure that corrupt Russian officials, government-aligned elites, and those aiding or concealing their unlawful conduct are held accountable. The task force also focuses on preventing the evasion of sanctions and ensuring compliance with international economic measures.

Following an Oligarch Task Force meeting on March 17, 2022, the EU introduced its 4th sanctions package against Russia. This package required EU companies to take several actions to ensure they were not aiding sanctioned individuals or entities, including conducting thorough due diligence to avoid engaging in transactions with sanctioned oligarchs.

Catching Russian oligarchs circumventing sanctions is challenging for several reasons. Oligarchs often use intricate networks of anonymous shell companies and offshore accounts to hide their assets, making it difficult to trace the true ownership, the Ultimate Business Owner (UBO), of assets. For OEMs, this is a daunting task. Although Russian oligarchs were mainly targeted because of their involvement in private aviation, they have also been known to use Russian state-owned aircraft. All these activities must be traced to ensure that no parts are being delivered to the benefit of these oligarchs through any indirect channels. The scale of this activity is unprecedented compared to any previous sanctions. If an OEM finds it has inadvertently still served oligarchs, it needs to report this to the authorities. Preparing a self-disclosure is demanding and often involves services from outside counsel.

[117] "Attorney General Merrick B. Garland Announces Launch of Task Force Kleptocapture." *Office of Public Affairs | Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture | United States Department of Justice*, 22 Mar. 2022, www.justice.gov/archives/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

OEMs reaction and perception to the KleptoCapture measure

Two out of four companies believe that the KleptoCapture measure does not apply to them. One company had not considered it at all and noted challenges in identifying the Ultimate Business Owner (UBO), remarking that not having really looked could indeed be risky. The second company reported that their client base was not affected by KleptoCapture but had considered the measure.

A third company initially did not believe they would be affected due to their limited activity in private aviation. However, they were surprised when a parent company, during their own research, reported a potential link to an oligarch for their product. Upon further investigation of the actors involved, there was a suspicion that their product was being diverted to a Russian airline. The interviewed company stated that they would not have been able to identify the link to the oligarch without the in-depth research conducted by the parent company, which was assisted by law firms. This finding did not result in a reportable event regarding KleptoCapture, but rather highlighted a general issue of diversion for which outside counsel was consulted. Consequently, all business had to be stopped, and a report was made to the relevant authority. The interviewed company expressed concerns about possibly being overcompliant by stopping all business with the operator and cited safety concerns. However, the authorities have not responded to their request for clarification.

The fourth company already included oligarchs in their enhanced due diligence processes and considered all private aviation to be high risk. Despite this, they noted that they still have a limited ability to always find the UBO, posing challenges for business operations. The company seemed to have shied away from doing business with many very rich individuals due to the financial risk in case of an accident that would result in a court case. They hinted at a recent event where a major defense company is being sued for billions after an accident[118].

Effectiveness and actual implementation of KleptoCapure

In this case the instructions can be considered as unclear, as all companies reported that it can be really hard to find the UBO and the rules for who is considered UBO are different in the U.S. and EU, the EU being more complex. While it may be evident that an oligarch could benefit from a company's product, the use of complex and opaque ownership structures to conceal their involvement makes it challenging to trace the oligarch as the ultimate beneficial owner (UBO).

Not all companies have the resources to involve third-party services to do in-country research and have to rely on publicly available information. Each company decides, based on their risk appetite what process to follow.

Referring back to Guimelli's (2017) typology, the initial situation can be described as "Enforceable Delegation of Implementation." with vague instructions but strong monitoring and enforcement by the special KleptoCapture task force. The expected level of compliance would be overcompliance.

It is worth noting that the Trump administration disbanded the Task Force KleptoCapture in February of 2025, which makes it unclear what will happen to companies who are still investigating transactions which could lead to findings that would need to be reported. Today's situation is therefore "Delegation

[118] Osborne, Tony, and Based in London. "Leonardo Sued for $2.6B by AW169 Crash Victim's Family." *Aviation Week Network*, 10 Jan. 2025, aviationweek.com/business-aviation/safety-ops-regulation/leonardo-sued-26b-aw169-crash-victims-family.

of Implementation by Persuasion" with vague instructions and weak monitoring or enforcement, the problem being lack of compliance and behavior depending on the type of company.

Based on the information provided during the interviews, it is evident that there is significant variability in how companies perceive and respond to the KleptoCapture measure. This variability can be attributed to several factors, including the clarity of the guidelines, which led companies to either consider or overlook it, underscoring the potential for companies to miss critical compliance issues. Additionally, the complexity of identifying the Ultimate Business Owner, varying levels of risk appetite, and available resources further contribute to this variability.

Overall, the conclusion is that the effectiveness of the KleptoCapture measure is hindered by unclear guidelines, differing levels of resources, and varying risk appetites among companies. This results in inconsistent compliance and potential gaps in identifying and addressing issues related to the UBO.

6.6 Integrating customs measures into sanctions controls to combat evasion.

The introduction of large-scale customs measures to address sanctions evasion was unprecedented in the sanctions against Russia. While previous sanctions included various economic and financial restrictions, the comprehensive integration of customs measures marked a significant escalation in efforts to prevent circumvention and diversion. As a result, OEMs found themselves navigating uncharted territory.

6.6.1 Tracing iron and steel origins: aerospace industry challenges

The aerospace industry experienced considerable disruption when the EU imposed a ban on the import, purchase, transport, and provision of associated services for specified iron and steel products originating from Russia in the EU's 11th package[119]. This includes products exported from or located in Russia. These restrictions took effect on 17 June 2022 for contracts concluded before 16 March 2022. Companies were required to ensure and certify that their entire supply chain was free of Russian-origin iron and steel. This involved a comprehensive due diligence process to trace the origin of iron and steel inputs used in their products. Importers had to provide evidence of compliance, such as Mill Test Certificates (MTCs), which document the origin of the steel. These certificates needed to be available for inspection by customs authorities.

OEMs reaction and perception to the tracking of iron and steel origins

Within OEMs, extensive cooperation between compliance departments, which oversee the implementation of these sanctions and export control regulations, and customs departments was essential. Customers and suppliers simultaneously asked for proof of compliance with this new regulation.

Based on the interview findings, it is clear that the EU's sanctions on Russian-origin iron and steel had a significant impact and caused considerable disruption and delays. All interviewed were displeased with the communication by the authorities. Only end of September 2023 customs offices released a statement and early October the EU published guidelines confirming that the Mill Test Certificate" (MTC) is sufficient proof of the origin of steel inputs, but that in the absence of this certificate, any alternative

[119] Council Regulation (EU) 2022/428 of 15 March 2022 amending Regulation (EU) No 833/2014 - new Article 3g.

proof may be presented to the controlling customs office, such as a quality certificates or suppliers' declaration.

From mid-June to the end of September, OEMs faced significant challenges in implementing the measure by obtaining the required Mill Test Certificates (MTCs). This measure initially caused confusion and delays as suppliers struggled to provide the necessary documentation. OEMs found themselves caught between suppliers and customers, all demanding certifications. This situation led to intense cooperation with procurement departments to identify which companies sold parts within the targeted HS codes and to obtain the required certificates. Delays were common as shipments could not be accepted into warehouses without the MTCs. In some cases, shipments were put aside awaiting certificates, and when this took too long, companies had to accept regular declarations instead to avoid massive disruptions.

Over time, it became clear that obtaining all the MTCs was impractical. Companies began accepting corporate declarations or confirmations that shipments were free of Russian steel or iron, even before this was confirmed to be acceptable by customs authorities and the EU. Interviewed companies with several business units in EU countries also noted that customs authorities reacted differently; in one country, shipments were blocked due to paperwork issues, while in another, the same paperwork was accepted.

Effectiveness and actual implementation of the tracking of iron and steel origins
The guidance on the sanctions was initially unclear, and companies were unsure what MTCs even meant. As the guidance evolved, it became more practical, allowing companies to provide their own declarations to their customers, which helped mitigate further delays. Despite these efforts, there was still uncertainty about how to ensure compliance and confidence in the process.

Eventually companies ended up with a workable situation with clear instructions, meaning a statement or certificate from the supplier was acceptable. Customs offices have a strong monitoring or enforcement ability, although they seem to have different strategies to follow up on this. The combination of strong enforcement with clear instructions the expected outcome according to Guimelli (2017) is that the problem of compliance is not considered.

The interviews confirm that companies have made significant efforts to comply with the regulations. However, there is a pervasive sense of doubt among these companies regarding the effectiveness and validity of their compliance measures. Many feel that, beyond the initial buyer of steel and iron, it is challenging to ensure the accuracy of the certifications. This raises the question: Was the effort and expense born by business, truly worth it for the authorities?

6.6.2 Strengthening sanctions with the CHPI List

In February 2024, the EU along with the U.S., U.K. and Japan, introduced the Common High Priority Items (CHPI) list[120 & 121]. This list was developed to identify items that Russia seeks to procure for its weapons programs. This 11th EU package and U.S. update by BIS was detailed in their policy guidance and included a new anti-circumvention tool, the CHPI list, designed to restrict the sale, supply, transfer,

[120] "Common High Priority List." *Russia Export Controls – List of Common High-Priority Items*, BIS, 23 Feb. 2024, www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items.
[121] *List of Common High Priority Items, Feb. 2024,* https://finance.ec.europa.eu/system/files/2023-09/list-common-high-priority-items_en.pdf.

or export of specified sanctioned goods and technology to third countries considered at high risk of facilitating circumvention.

The CHPI list includes prohibited Dual Use goods, and any technology items used in Russian military systems. With this list, customs and enforcement agencies in the EU and partner countries can target diversion and anti-circumvention actions by monitoring these items. The CHPI list is updated regularly based on discoveries in Russian military systems on the battlefield in the Ukraine.

The BIS extended its controls on items beyond those regulated by the EAR by 50 Harmonized Tariff System (HTS) and the E.U. now controlling non-listed items by imposing that companies monitor the equivalent Common Nomenclature (CN) codes, expanding the total to encompass 22 two-digit HTS and CN chapters resulting in more items now being restricted as CHPI items, necessitate licenses and requiring enhanced vigilance by businesses. As a consequence, items subject to the EAR in the U.S. need to be screened for diversion and anticircumvention for specific HTS codes, where before items subject to the EAR were only controlled based on export classifications, such as EAR99 or the ECCNs.

OEMs reaction and perception to the CHPI list

The answers from the interviewees show that the companies had different levels of concern and hence different levels of difficulty complying to this measure. This can be explained by the number of HS codes affected and their client base. All companies interviewed did not find much useful explanation in the regulation and guidance, other than having to implement this. For the companies most affected, two out of four, implementing a system to monitor the CHPI has proven to be very challenging due to the large number of customers in “transshipment” countries and the lack of readily available standards for normal sales volumes. While it is possible to estimate how much one customer would buy to support their activities, standards first need to be developed and then included in an automated system that flags unusual purchases. An additional difficulty in finding unusual patterns, arises from customers ordering parts through different channels, often identifying the item as purchased for stock, therefore not traceable to an aircraft. Brokers, MROs, and airlines also order for stock from various warehouses worldwide, making it difficult to consolidate all the information into a single picture. Customers can also order from different divisions and distribution centers. Consolidated sales data is available, but not in the form it can easily be used for diversion tracking. One company reported doing manual checks for entities in the third countries, or the so-called transshipment countries, until reports from a more automated method would be available. The system should have already been ready, however it is more difficult than anticipated and the focus cannot only be on sanctions on Russia as other tasks have already been shifted to the right.

One of the OEMs interviewed decided not to use their SAP GTS system, which can handle both HS and export classifications, as it was deemed not the best solution for this task. If more measures like this appear in the future, they might have to resort to SAP GTS anyway, but for now, they block certain destinations for specific HS codes differently and have a manual monitoring process in place.

Comments from the OEMs included that it is obvious that measures like the CHPI are here to stay and that authorities will be trying to control the supply chains of Common High Priority Items (CHPIs) as an integral part of sanctions. There are third-party services now that compare international trade data with supply network analysis to help trace the flows of these products through other countries. However, these services are considered expensive and require IT work, going beyond "best efforts." It is also clear that authorities will increasingly use trade data to discover undesired trade flows.

Effectiveness and actual implementation of the CHPI list

By controlling exports using HTC and CN codes, which are traditionally used for imports, the authorities have introduced a new tool. However, IT systems managing export control transactions are designed to control exports based on end destination and ECCN, not HTC and CN codes. This has thrown businesses for a loop, leaving them uncertain about compliance requirements. The instructions were considered vague, and companies are skeptical about the authorities' ability to detect non-compliance effectively, leading to what can be considered weak monitoring by the authorities. According to Guimelli (2017), there will be varying levels of compliance and behavior depending on the type of company.

The interviews confirmed that company behavior varied, with all four companies taking the measure seriously and attempting to comply as best as they could. However, they were unsure if their implemented or ongoing measures would be sufficient.

6.6.3 Targeting Iran's missile and UAV components

In the fall of 2024, the U.S. introduced a stricter Foreign Direct Product Rule (FDPR), which now subjects items exported to Iran to U.S. export control regulations, even if they were not previously controlled. Consequently, exports of items that fall under the FDPR for Iran, even if companies have U.S. export licenses, are now restricted under U.S. export controls. However, items exported from many European countries are exempt from these controls. This new FDPR demonstrates the U.S.'s stricter stance on controlling exports to Iran, adding a new layer of controls for companies still exporting to Iran.

In response to Iran's support for Russia's invasion of Ukraine, the EU introduced a new framework for restrictive measures in July 2023, amended in May 2024, targeting Iran's[122] military support to Syria and Russia. This regime bans the export of components from the EU to Iran that are used in the construction and production of missiles and Unmanned Aerial Vehicles (UAVs)[123]. The prohibition is managed by restricting the export of items classified under specific Common Nomenclature (CN) codes. In some cases, only certain parts of the items within a CN code are prohibited, based on their technical capabilities.

Although not many OEMs were still exporting to Iran due to the requirement for U.S. licenses from OFAC and BIS, those companies that did have the licenses faced additional burdens. The more restrictive U.S. Foreign Direct Product Rule and the EU requirement based on CN codes necessitated detailed analysis.

OEMs reaction and perception to additional requirements for exports to Iran

Only one OEM interviewed was impacted by this measure. The measure was considered particularly challenging because exports are traditionally managed by ECCNs, and license conditions are mainly based on ECCNs. Automating the verification of CN codes is difficult, especially for items under CN codes preceded by an “ex,” which are only allowed to be exported if they exclude certain technical capabilities. This necessitated verifications with the engineering department to determine if the part was excluded or could still be exported, resulting in manual reconciliation of orders and compliance status. Parts

[122] “Council Regulation (EU) 2024/1338 Amending Regulation (EU) 2023/1529 Concerning Restrictive Measures in View of Iran’s Military Support of Russia’s War of Aggression against Ukraine.” *EU*, 14 May 2024, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1338.

[123] *EU Sanctions against Iran - Consilium*, 20 July 2023, www.consilium.europa.eu/en/policies/sanctions-against-iran/.

exported with an "ex" in front of the CN code were held up in customs for weeks, requiring extensive communication of the technical details of the part to the customs department.

Effectiveness and actual implementation additional requirements for exports to Iran
There is no alternative but to be fully compliant. This is a case of clear instructions and strong monitoring, as customs checks all shipments to Iran. Although it places an extra burden on the exporting company to check and document transactions, and to communicate with customs officers and customers to explain shipment delays, full compliance is achieved.

6.7 Red Flag analysis for sanctions compliance

On 7 September 2023, the European Commission issued guidance to help EU operators prevent the circumvention of Russia sanctions. Articles 10 and 12 of EU Regulation 833/2014, along with the European Commission's FAQs (FAQ n°6, p.153)[124], and Section 228 of the U.S. CAATSA, mandate companies to implement robust measures to prevent sanctions evasion.

These additional due diligence requirements preventing diversion and circumvention export's schemes of spare parts, services, or aircraft to Russia and actions required to comply with the "Best Efforts" obligations under Article 8a of Council Regulation 833/2014 and related guidance.

Key points included due diligence steps for operators to avoid exposure to sanctions circumvention, general recommendations for maintaining compliance, strategies to prevent goods from being diverted to Russia or Belarus via third countries, such as including clauses in contracts with third-country partners that prohibit re-exports to these nations, banking and finance guidance, and a list of Red Flags[125] related to business partners and customers.

As part of the Red Flags, exporters must ensure that items listed in the relevant annexes, such as the CHPI, are not reexported to Russia. This involves staying updated on the annexes, which are regularly expanded, conducting enhanced due diligence on customers and end-users, obtaining end-user certifications, and monitoring order quantities for CHPI to prevent diversion to Russia.

OEMs need to maintain a list of entities in countries prone to diversion and circumvention and check transactions for abnormal patterns. These additional due diligence requirements aim to prevent the diversion and circumvention of exports of spare parts, services, or aircraft to Russia and comply with the "Best Efforts" obligations under Article 8a of Council Regulation 833/2014 and related guidance.

OEMs must fulfill their obligations under international regulatory frameworks to mitigate the risk of sanctions circumvention. OEMs now need to conduct extensive due diligence on third parties to ensure they are not indirectly dealing with sanctioned entities. This involves verifying ownership structures, beneficial ownership, and potential links to sanctioned individuals or entities. Although third-party checking has always been part of any compliance program, there is now additional requirement, such as

[124] *Guidance for EU Operators; Implementing Enhanced Due Diligence to Shield against Russia Sanctions Circumvention*, European Commission, finance.ec.europa.eu/document/download/3c86c9a8-f09e-4092-ab8c-a9e678df1494_en?filename=guidance-eu-operators-russia-sanctions-circumvention_en.pdf. Accessed 25 May 2024.
[125] A list of warning signs related to business partners and customers that may indicate potential circumvention.

to check companies established after the introduction of the sanctions to verify if they were set up with the specific goal of circumventing these sanctions.

OEMs reaction and perception to Red Flag analysis

Three out of four OEMs reported significant impacts from this requirement due to their products and customer base. They all noted the challenge of determining if their efforts were sufficient and mentioned that while many regulations have similar requirements, the current pace of changes is unprecedented, making it difficult to stay updated. This has resulted in numerous internal meetings across various functions and brainstorming sessions to ensure the correct and consistent interpretation of the sanctions measures.

OEMs reacted to this extensive Red Flag requirements by updating compliance plans with specific instructions, ongoing risk assessments, developing new queries in their IT systems, and training customer-facing and order administration personnel as well as compliance employees to recognize Red Flags. Constant adaptations are made based on on-going risk assessments.

The Red Flags related to the regular Know Your Customer (KYC) process and screening were deemed acceptable, although third-party oversight remains unpredictable, and absolute certainty is unattainable. Customers who were supported three years ago may no longer be supported today. As one interviewee remarked: “Ensuring consistent accuracy in third-party oversight is challenging due to inherent risk in compliance”.

Red Flags concerning monitoring (such as the CHPI codes) were found much harder to implement. While a single Red Flag can sometimes be sufficient, it usually involves a combination of factors, making it impossible to be on high alert everywhere at all times. The standards for sufficient monitoring are considered unclear and the FAQ has not been found very helpful. IT solutions for all the Red Flags are not feasible. The data we need is often spread across different systems. For companies with multiple divisions serving the same customer base, compiling all this data to identify diversion and circumvention trends is a massive task.

Compliance is complicated by the lack of standardized guidelines for what constitutes normal business practices. Monitoring the CHPI list is particularly challenging without standards for normal order quantities, making it difficult to identify trends that might indicate the diversion of parts. Businesses are primarily focused on selling and often lack mechanisms to flag unusual orders. Developing standards to identify potential diversions requires extensive knowledge about clients' operations, requiring multiple input from different departments.

Current IT systems aren't designed to monitor and track parts based on CN codes. Upgrading or implementing new systems to handle this level of detail is both costly and time-consuming. When it comes to monitoring exports and integrating standards into the IT system, first it needs to be established what constitutes a normal order quantity for items per customer. Given the complex supply chain and the involvement of brokers and MROs who don't necessarily order for specific aircraft, identifying unusual or suspicious orders that might indicate attempts to circumvent sanctions is deemed challenging to impossible.

To adapt compliance programs accordingly, the companies continuously monitor these changes, which requires dedicated compliance teams, legal expertise, and ongoing training for employees. All agreed

that the timeframe to implement such extensive requirements was insufficient. They found that these factors combined make compliance with diversion and circumvention requirements a complex and resource-intensive task.

Effectiveness and actual implementation of the Red Flag analysis

OEMs clearly indicated that the instructions are vague, leaving them uncertain about what to comply with and how to do so. They have primarily focused on strengthening their existing compliance measures and based on ongoing risk assessments, have added IT solutions where possible, although many of these solutions are still not fully implemented and operational.

Given the complexity and multitude of factors involved, it is challenging for authorities to monitor whether businesses' compliance efforts are sufficient. If businesses themselves struggle to establish clear standards, it becomes equally difficult for authorities to evaluate the overall compliance programs and their handling of all the red flags. This ambiguity and the evolving nature of regulations make it hard for both businesses and authorities to ensure consistent and effective compliance.

6.8 The "No-Russia" clause and DTP codes

No-Russia Clause

On December 18, 2023, the EU introduced its 12th package[126] of Russian sanctions, including a new "No Russia" clause. Article 12g of the Regulation requires EU companies to prohibit the re-exportation to Russia or for use in Russia of sensitive goods and technology (such as aircraft and their parts) when selling to third countries, except for "partner countries"[127]. This clause requires EU exporters to include wording in certain contracts that prohibits the re-export of goods to Russia and provides for adequate remedies in case of a breach. The aim is to prevent the circumvention of EU export bans by ensuring that goods exported to third countries are not re-exported to Russia and to this means the EU guidance suggests wording with the requirements of Article 12g. The same mechanism exists for exports to Belarus since 29 June 2024, when the EU adopted additional sanctions which mirror the measures that have been imposed on Russia, the "No Belarus" clause[128]. The aviation goods for the aerospace OEMs concerned, are those listed in Annex XI and Annex XL, the so called CHPI[129].

Failure to comply with EU or U.S. sanctions can lead to serious consequences. In the EU, there is strict scrutiny of contracts, with minimum penalties for violations set by Directive (EU) 2024/1226, effective from May 19, 2024. The EU is taking a firm stance on anti-circumvention, expecting additional compliance steps under Articles 12g and 8g (No Russia and No Belarus clauses), beyond the general aviation sanctions in Article 3c.

[126] by adding Article 12g to CR (EU) 833/2014, set out in Council Regulation (EU) 2023/2878, effective December 19, 2023. Further amendments were made on June 24, 2024, via Regulation (EU) 2024/1745.

[127] The "No-Russia clause" applies to all contracts with non-EU or non-partner country counterparts. Partner countries include Australia, Canada, Iceland, Japan, Liechtenstein, New Zealand, Norway, South Korea, Switzerland, the UK, and the USA.

[128] The "No Belarus" clause requirements, pursuant to article 8g of Regulation (EU) 2024/1865 (Article 8g), apply only to contracts entered into from 1 July 2024, with no retroactive application.

[129] The Common High Priority Items, or CHPI, is a subset of items already prohibited for export to Russia, but which have been identified by the G7 as posing the highest risks of re-export from third countries for use by the Russian military.

The scope of Article 12g[130] is such that contracts concluded from December 19, 2023, onwards (the date that Council Regulation (EU) 2023/2878 came into force) must include the "No-Russia clause." Contracts concluded prior to Council Regulation (EU) 2023/2878 coming into force benefit from a one-year transition period (or until the contracts' expiry, whichever is earliest). All pre-existing contracts must therefore have a "No-Russia clause" in place from December 20, 2024.
The "No-Russia clause" required OEMs to amend existing contracts, as well as standard and specific terms and conditions, to include this clause. Although the "No-Russia clause" refers only to a relatively narrow set of items considered to be at highest risk of diversion to Russia, it applies to many contracts for aerospace OEMs, who had to consider whether the products under their sales contracts fall within the restricted goods listed in Article 12g.

In December of 2024 a new FAQ regarding the No-Russia clause clarified that only operators in the EU are involved and if the delivery obligations are only to be performed within the EU, there is no obligation to include the No-Russia clause. However, in aerospace there are a lot of drop-shipments happening for Aircraft on Ground (AOG)[131] reasons. This makes it very hard to predict if there are contracts, for which deliveries normally take place in the EU, need to be updated anyway in case of a drop-shipment to a new address outside of the EU. On December 18, 2024, it was further clarified in the FAQ[132], that a general clause prohibiting the re-exportation to countries subject to EU restrictive measures can be sufficient if the other requirements in Art. 12g are met, i.e. adequate remedies are indicated.

DTP codes
On October 19th, 2024, all EU Customs offices announced that, effective October 21, 2024, a specific tariff code, known as Specific Tariff Provisions (DTP code[133]), must be provided in each Member State's customs declaration tool to represent the status of the No Russia/No Belarus Clause. This requirement was introduced without prior notice. Shipments of certain Common Nomenclature (CN) codes would be blocked without this code.

The new mandatory customs declaration for all exports outside the EU requires confirmation that the contract under which the item is being exported either includes a "No-Russia/No-Belarus clause" or was signed before December 19, 2023, when this EU sanctions requirement came into effect. If signed before December 19, 2023, exports were allowed until December 31, 2024. However, starting January 1, 2025, this transition period for including the no-Russia/Belarus clause in pre-existing contracts ended. This meant that the exception for contracts signed before December 19, 2023, no longer applied, so OEMs

[130] The first clause of Article 12g(1) states: 'When selling, supplying, transferring or exporting to a third country, with the exception of partner countries listed in Annex VIII to this Regulation, goods or technology as listed in Annexes XI, XX and XXXV to this Regulation, common high priority items as listed in Annex XL to this Regulation, or firearms and ammunition as listed in Annex I to Regulation (EU) No 258/2012, exporters shall, as of 20 March 2024, contractually prohibit re-exportation to Russia and re-exportation for use in Russia.'
[131] In aerospace, AOG (Aircraft on Ground) refers to an aircraft that can't fly due to technical issues or maintenance needs. This situation is urgent, often requiring expedited shipping of spare parts and emergency maintenance to get the aircraft back in service quickly.
[132] *"No Re-Export to Russia" Clause, European Commission, 22 Feb. 2025, finance.ec.europa.eu/publications/no-re-export-russia-clause_en. No. 11*
[133] Update of the note on the implementation of CR (EU) 2024/1745 of June 24, 2024, amending Regulation (EU) 833/2014 (Russia) and CR (EU) 2024/1865 (Belarus) of June 29, 2024, amending Regulation (EC) No 765/2006. Initially published in July 2024, these notes were updated to create new specific tariff provisions related to Article 12g of Regulation (EU) 2024/1745 (Russia) and Article 8g of Regulation (EU) 2024/1865 (Belarus).

had to ensure that the “No-Russia” clause was implemented in all pre-existing contracts. There is no similar U.S. requirement to amend contracts to refer specifically to Russia.

Any false customs declaration, such as falsely stating that the no-Russia clause is included when it is not, will be considered a serious offense. Penalties for such offenses vary by Member State but are designed to be efficient, proportionate, and dissuasive. They can include substantial fines, administrative sanctions, and in some cases, criminal penalties[134].

OEMs were abruptly confronted with an unexpected and unannounced update to customs requirements, necessitating the inclusion of these new specific tariff codes related to the implementation of the No Russia/No Belarus clause. The DTP requirement leaves no room for interpretation or a risk-based approach.

The requirement to include new tariff codes in customs declarations for items specified as CHPI forces exporters to comply strictly with Articles 12g/8g (No Russia, No Belarus clauses) of the related contract or transaction.

If an export is subject to the No Russia/No Belarus clause, and the OEM cannot confirm that the contract includes a 12g/8g clause, it cannot clear customs in good faith. This shifts the obligation from making legitimate best efforts to ensuring absolute compliance with the 12g requirement. According to EU Member States' customs laws, a false declaration (e.g., claiming a 12g/8g clause exists when it does not) is a criminal offense punishable by a fine. Each Member State sets its own fines; for example, in France, the fine can be as high as three times the value of the item, which can be considerable given the high value of many aerospace items (systems, components, aircraft).

OEMs reaction and perception to the No-Russia Clause and DTP requirement

The new contractual requirement to integrate the No-Russia clause into contracts, placed a significant new burden on OEMs, leading to a considerable workload and requiring significant effort from multiple departments. All four OEMs interviewed were very impacted because of their customer base and the products they sell, however did not take the same approach. The regulations and FAQs were seen by the OEMs as unclear and frequently changed, causing rework and confusion.

One company decided against directly updating contract clauses. Instead, they integrated the No-Russia Clause into their SAP system, incorporating it into quotations, order confirmations, and invoices, as all transactions are processed through SAP. To avoid the risk of reopening contracts, they chose to manage it within SAP with an updated notification. This blanket inclusion, however, led to overcompliance in some cases where the No-Russia Clause was not necessary, however this OEM’s interpretation of the No-Russia clause, could be considered as not sufficient by authorities. While they took the decision to greatly simplify the implementation of the No-Russia clause, their corporate office was in contact with the European Commission and the national ministry responsible for customs to lobby for the

[134] *Report from the Commission on the Assessment of Customs Infringements and Penalties in Member States*, 6 Jan. 2023, www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&WordsInText=3658*&DocumentLanguage=EN.

requirement to be fulfilled when there is an End-User Statement, End User Certificate, or Non-Transfer Certificate signed by the client for contracts with an export authorization in place.

Actually, all four OEMs noted that their parent companies or corporate offices were lobbying for the rules to be more workable. The European Commission, in October of 2024 gathered information through a survey[135] on the implementation, impact and potential extension of the No-Russia clause. Although no feedback regarding the results has been available on-line, in December 2024, the EU clarified in their FAQ that a notification or statement was sufficient. Until then, the regulation required contract amendments.

Three out of the four companies that consulted with outside counsel on the implementation received conflicting advice. One was advised to open up contracts to insert the clauses, another one to update the Terms & Conditions (T&Cs) with customer acknowledgements, and one was advised to send out a notification only. This confusion occurred before the FAQ was updated in December 2024, which clarified that a notification or statement was sufficient.

For companies updating contracts as initially required by the regulations, there was a considerable workload and internal coordination needed. They first had to identify which contracts needed amendments, compare the relevant annexes to the items in the contracts, check the contract dates to establish a priority list for implementation, and then update the contracts. The unpredictable nature of drop shipments added to the challenge. When a contract is with a company in a partner country, a contract clause is not required. However, if there is a drop shipment to a non-partner country, the DTP code must reflect that the No-Russia clause requirement was fulfilled.

The implementation of the DTP codes also had a very high impact on OEMs, who were given only a weekend's notice to comply. This led to scrambling to assemble a team to handle the flow manually, resulting in delivery delays.

One company reported that it took two weeks to check all lists and three months to implement an automated solution, pulling specialists away from other projects. Another company reported that implementing the DTP codes remains a manual process due to the complexity of contracts and the limitations of their ERP systems. This manual approach increases the risk of mistakes, such as order administrators inadvertently accepting incorrect terms and conditions.

Companies trying to automate the tariff codes into their customs declarations were confronted by the fact that in the relevant annexes, some CN codes are preceded by "ex." When a CN code is marked with "ex," it indicates that not all goods under that CN code are subject to the prohibition, but only a subset. This subset corresponds to the description in the table, title, subtitle of the annex, or the relevant article in the regulation. Automation for CN preceded by "ex" has not been achieved yet, and therefore the specific part numbers are blocked and must be released manually as long as the system cannot account for the specific product descriptions to determine compliance accurately. Another issue encountered was inconsistencies or mistakes in the CN codes in the annex which required verification with customs, and affected the automation, resulting in blocked transactions.

Until the FAQ update of December 2024, companies were at risk, not only for a fine but also the impact of being unable to deliver items to customers and suppliers if the No Russia/No Belarus clause is not

[135] *Eusurvey*, ec.europa.eu/eusurvey/runner/article-12-g-feedback. Accessed 26 Feb. 2025.

secured or has been refused. Given that many countries do not adhere to the notion of sanctions on Russia, this put deliveries to entities in these countries at risk. Once it was permitted to use a notification instead of renegotiating the contract to include the No-Russia clause, the situation was unblocked.

OEMs also remarked that companies outside the EU and not exporting from the EU do not have to comply with this requirement and therefore have a competitive advantage.

Effectiveness and actual implementation of the No-Russia Clause and DTP requirement

Overall, the interviews reveal that the European Commission lacks in understanding of business operations. The inconsistent handling of DTP codes have made compliance a burdensome and error-prone process. Corporate offices lobbied the European Commission and national ministries to clarify the No-Russia Clause requirements, which may have led to the requirement being diluted to a notification in December 2024.

The evolving nature of the sanctions and the short time to implement some of the requirements, such as the DTP codes on the customs declaration with only three days between announcement and implementation, suggest that authorities face challenges with the practical aspects of the sanctions.

Initially, OEMs struggled to implement the No-Russia Clause in contracts as per the regulation. OEMs which had implemented the No-Russia clause requirement by updating their contracts, instead of blanket notifications or integration into SAP, in a way, suffered from trying to do it right. Over time, the instructions evolved, allowing companies to comply more effectively. While the initial instructions were vague in the sense that companies could not comply without risking massive stops of deliveries to parties who would not sign, the DTP code measure provided authorities with strong monitoring and enforcement capabilities, which, according to Guimelli (2017), would lead to overcompliance. However, the regulation changed, likely based on companies feedback to the Commission and to avoid massive disruptions in supply chains.

With the No-Russia requirement now diluted to a notification, the authorities' ability to monitor diversion and circumvention via DTP codes is questionable. Third parties in countries that had no intention of signing the No-Russia Clause (such as entities in China, India, South Africa, and elsewhere) now receive a notification advising them not to transfer products to Russia. Although the instructions on how to implement the No-Russia Clause are now clear and feasible for businesses, and the authorities' ability to enforce this via DTP codes is high, proper monitoring remains challenging. Authorities can check if the No-Russia requirement was fulfilled but ensuring that the notified party is not transferring goods is weaker with a notification than with a signed contract.

6.9 "Best Effort" obligation

Having already implemented its most impactful measures (banning the export of aerospace items and introducing anticircumvention measures), the EU adopted its 14th sanctions package on June 24, 2024[136]. It includes tighter restrictions and enforcement of these anti-circumvention efforts, with a wider

[136] *COUNCIL DECISION (CFSP) 2024/1738 Amending Decision 2014/145/CFSP Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine*, 24 June 2024, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401738.

scope and a best effort obligation on EU parents to prevent their third country subsidiaries from undermining sanctions or circumvent restrictions and expanding restrictions on individuals and entities such as Chinese, UAE and Indian companies.

On 22 November 2024, Frequently Asked Questions (FAQs) was published to clarify the "best effort" obligation[137] determined by Art. 8a Reg. (EU) 833/2014 regarding subsidiaries and Joint Ventures of EU companies. The EU also published FAQ and guidance to clarify some of the terminology used in the regulations, such as best efforts, circumvention and undermining[138].

The "best efforts" requirements, introduced in June 2024, are clarified in the FAQs. For economic operators, these efforts depend on their specific circumstances and should encompass all necessary and appropriate actions, limited to what is feasible for the EU operator, considering factors such as the sector of operation and the country of establishment. Specifically, these efforts can include internal policies, controls, and procedures for risk management and mitigation. For the sale of certain high-priority goods (e.g., battlefield goods), EU operators must identify, assess, and mitigate the risks of re-exportation to Russia. These assessments must be documented and kept up to date. For subsidiaries established outside the EU that are owned or controlled by EU businesses, best efforts must be undertaken to ensure they do not participate in activities that undermine the restrictive measures provided for in the Russia and Belarus Regulations. This will require a risk assessment and potentially an adjustment of the compliance program of the OEM.

The concept of "circumvention" now also includes participating in activities that aim to circumvent prohibitions, even if the participant does not deliberately seek that outcome but is aware that their participation may lead to it and accepts that possibility.

Other additions under this package include third-country entities and the expansion of the No-Russia clause to Intellectual Property rights. If an EU operator owns or controls an entity in a third country, the EU operator must ensure that the entity implements these requirements, provided that the legislation of the third country allows it. EU operators must include a clause in their contracts with third-country parties prohibiting the re-exportation to, or use in, Russia of their transferred IP rights (e.g., know-how).

A further addition is that, according to Article 12g §4 of the EU reg 833/2014 paragraph 4 of Article 12g exporters are required to inform their national competent authorities as soon as they become aware of a breach or circumvention of the “No-Russia” clause.

OEMs reaction and perception of the Best Effort obligation

Other than checking if the No-Russia clause needs to be added to contracts for Intellectual Property, the OEMs interviewed seem to consider this “more of the same” and commented that they are already continuously adjusting processes to try to stay ahead of regulatory changes, as future sanctions packages may be even more stringent. Their risk assessments has a direct focus to the highest-risk areas, but it's

[137] “Article 8A of Council Regulation (EU) No 83.” *FAQ on Sanctions against Russia, Best Effort Obligation*, 22 Nov. 2024, finance.ec.europa.eu/document/download/65560de8-a13a-4a58-a87c-ddd27b14e6c1_en?filename=faqs-sanctions-russia-best-efforts-obligation_en.pdf.

[138] Undermining in the context of Council Regulation (EU) No 833/2014 refers to actions that weaken or circumvent the restrictive measures imposed by the regulation. Specifically, it involves any activities that attempt to bypass or evade the sanctions, thereby diminishing their effectiveness. This can include indirect or deceptive practices aimed at continuing prohibited activities despite the sanctions.

impossible to achieve 100% oversight on third-party circumvention. Comments received about the clarity for the Best Effort obligation were very similar to the comments for the Red Flag analysis, and generally it was seen as not changing anything.

Effectiveness and actual implementation of the Best Effort obligation

OEMS did not really know what to do with the Best Effort obligation, so therefore consider them vague instructions. Authorities do not have much to monitoring or enforcement the Best Effort obligation with, and the problem is then, according to Guimelli (2017), lack of compliance and behavior depending on the type of company.

6.10 Additional screening and vigilance requirements

Since the sanctions against Russia began, a significant number of entities and individuals have been added to restricted lists. In 2023 alone, the U.S. added approximately 2,500 persons to the Specially Designated Nationals and Blocked Persons (SDN) list, including 1,621 entities and 879 individuals[139].

By April 2024, OFAC has designated more than 4,500 individuals, entities, vessels, and aircraft as Specially Designated Nationals. Of these, OFAC has issued more than 4,100 sanctions designations pursuant to E.O. 14024 since the start of Russia's expanded invasion of Ukraine in February 2022[140].

Between February 22, 2022, and January 11, 2024, territories and organizations worldwide imposed over 16,000 restrictions on individuals from Russia and roughly 9,300 list-based sanctions on entities[141].

Denied party screening of entities and individuals.

Many companies have outsourced their screening processes, either partially or wholly, to third-party service providers who compile comprehensive lists of blocked entities and handle the clearing of false positives. A false positive occurs when an individual or entity is flagged as a match to a listed entity, but upon further verification, it is found not to be the case. Since the sanctions against Russia, the number of listed entities has surged, leading to an increase in false positives and, consequently, higher costs for screening services. When handled internally, this also adds to the workload of compliance teams.

Denied party screening of aircraft.

Another example of added vigilance is on aircraft suspected of entering Russia in violation of the EAR. General Prohibition 10 (GP10) prohibits any action with respect to such aircraft, wherever located. The GP10 prohibition under EAR is one of the ten general prohibitions that govern the export, reexport, and transfer of items subject to the EAR. It basically states that if you know or have reason to know that an item is being exported or used in violation of the EAR, you are prohibited from engaging in any of the listed activities with that item. Therefore, before servicing any aircraft, to avoid an export violation, the

[139] Scarpino, Rowan, and Jocelyn Trainer. "Sanctions by the Numbers: 2023 Year in Review." *CNAS.Org*, 27 June 2024, www.cnas.org/publications/reports/sanctions-by-the-numbers-2023-year-in-review.
[140] Welt, Cory. *U.S. Sanctions on Russia: Legal Authorities and Related Actions*, 26 Apr. 2024, crsreports.congress.gov/product/pdf/R/R48052/4.
[141] Statista Research Department. *Sanctions Imposed on Russia by Target 2024 | Statista*, 28 Jan. 2025, www.statista.com/statistics/1293531/western-sanctions-imposed-on-russia-by-target/.

supplier needs to check the flight history to verify that the aircraft was not flying into Russia, without the required authorization from the EAR.

As aircraft also appear on denied party lists, companies are required to keep their systems updated with these aircraft. If a customer places an order for a part or service for an aircraft on the SDN list, the order must be blocked and investigated. A complication in maintaining these lists is that the SDN list identifies aircraft by their registration number, while the aerospace industry places orders using the Manufacturer Serial Number (MSN)[142].

OEMs reaction and perception of additional screening and vigilance requirements

OEMs have become more conservative in their screening processes, taking no risks and often refusing business if there is any doubt. Potential customers suspected of requesting parts and services for diversion to Russia are placed on internal blacklists and blocked in the system. These findings are not reported to authorities, as they have not resulted in transactions that could be diverted. All these OEMs maintain their own lists of blocked entities, which extend beyond restricted, denied, and sanctioned parties.

Screening lists are purchased from third-party services and managed through home-grown systems, linked to SAP, or handled by third-party software, depending on the company. The sanctions on Russia have increased the number of false positives, adding to the workload but still manageable by the same team. In one case, the increased workload of clearing false positives led a service provider to renegotiate rates.

Enhanced Know Your Customer (KYC) processes have been implemented, with shorter intervals for KYC renewals in transshipment countries and other sensitive regions. Screening of Manufacturer Serial Numbers (MSNs) is challenging because IT systems identify aircraft by MSN, while authorities use registration numbers. OEMs have become demanding in screening for MSNs, insisting on accurate information, which adds to lead times on orders.

All four interviewed OEMs reported that screening, due diligence, and strengthened End User Statements (EUS) since the sanctions on Russia have resulted in more blocked entities. While there is concern about being too conservative, the risk of engaging with an entity that could cause difficulties is deemed unacceptable. If potential customers have hits that cannot be easily cleared or are hesitant to sign an End User Statement (EUS), they are added to the blacklist and blocked. This rigorous stance on screening could lead to overcompliance, but the high demand for products means not all customers need to be accepted.

Two out of four OEMs noted that banks are also more conservative in their screening and will no longer accept payments from either third-party payers or the customers themselves, even if neither the third-party payer nor the customer is a restricted party. This has led to extensive communication and exchanges between OEMs and banks to resolve issues and release blocked funds.

[142] In aerospace, MSN stands for Manufacturer Serial Number. This unique identifier, assigned by the OEM to a specific aircraft, is crucial for tracking, documentation, maintenance records, and regulatory compliance.

Effectiveness and actual implementation of additional screening and vigilance requirements

The additional vigilance requirements that extend beyond the denied party screening process are linked to the best-efforts obligation and red flag analysis, making them somewhat vague. However, authorities have limited ability to monitor the behavior of OEMs. According to Guimelli (2017), the expected level of compliance varies by company. For the OEMs interviewed, it was evident that they are risk-averse and tend to lean towards overcompliance.

6.11 Extended violation limitations and recordkeeping requirements.

In April 2024, new U.S. legislation extended the limitations period for violations for OFAC sanctions under the Trading with the Enemy Act (TWEA) or the International Emergency Economic Powers Act (IEEPA) from five years to ten years. This extension applies to any violation not already time-barred at the time of enactment, meaning it does not apply to violations that occurred before April 24, 2019. OFAC clarified that it can now bring enforcement actions for civil violations of IEEPA- or TWEA-based sanctions prohibitions within ten years of the latest date of the violation if such date was after April 24, 2019.

In September, OFAC issued an interim final regulation to extend recordkeeping requirements from five years to ten years, effective March 12, 2025. The regulation mandates that every person engaging in any transaction subject to the provisions of this chapter must keep a full and accurate record of each transaction for at least ten years, regardless of whether the transaction is effected pursuant to a license or otherwise[143].

The Impact of the OFAC recordkeeping requirements is that relevant transactions need to be safeguarded for at least ten years, which means that internal recordkeeping procedures need to be modified from five to ten years, employee training on maintaining records needs to be updated and provided, and potentially changes to data management systems are necessary. There is also the extended scope of data whereby the data recorded needs to be "full and accurate record for each transaction", which means that companies have to ensure that the whole sequence of each business transaction is kept, including communication related to compliance and documentation such as customer certifications and End User Statements. The U.S. DOJ, BIS and the OFAC issued a joint compliance note focused on cracking down on third-party intermediaries used to evade Russia-related sanctions and export controls enforcement.[144]

Given the extended investigation period, businesses are at a higher risk of facing enforcement actions if their records are incomplete or not properly maintained. By extending the statute of limitations, the liability associated with a risky transaction is effectively doubled. Consequently, it is more crucial than ever to thoroughly screen business relationships for denied parties, implement meticulous OFAC compliance processes, establish comprehensive data management practices, and conduct regular audits.

[143] "Reporting, Procedures and Penalties." *Federal Register*, 13 Sept. 2024, www.federalregister.gov/documents/2024/09/13/2024-20674/reporting-procedures-and-penalties.
[144] *Cracking down on Third-Party Intermediaries Used To ...*, 3 Mar. 2023, www.justice.gov/file/1571551/download.

Effectiveness and actual implementation of the extended record keeping requirements for extended violation limitations

This high-impact change has not yet been implemented. Two companies noted they never discard export records but need to ensure all related analyses, like emails and memos, are retained. Procedures and contracts with third-party compliance suppliers for screening and archiving may need updates. All OEMs are still assessing necessary process updates, but there is time to implement changes as the 10-year retention period starts from 2019.

Effectiveness and actual implementation of the extended record keeping requirements for extended violation limitations

The level of compliance will vary by company. While the instructions to businesses are clear, enforcement by authorities is nearly impossible. If a business fails to maintain records for 10 years, authorities will remain unaware unless the company is investigated.

6.12 Overall business impact and strategy

High impact and intense workload
All four OEMs interviewed rated the impact of the restrictive measures on Russia as high to very high, citing the unprecedented volume and complexity of the regulations. These measures significantly affected all OEMs, requiring extensive team cooperation to stay updated. The constantly changing regulations have been challenging, demanding considerable time and effort to understand and implement new measures. Dedicated task forces were established to manage these changes. Training and additional screening have been necessary to ensure compliance, with some companies also fearing and trying to anticipate future regulatory changes and the need for further IT solutions. A concern is that national authorities within Europe will increasingly add specific requirements and export controls on top of the existing EU framework, leading to inconsistencies in regulations. The OEMs suspect that sanctions regulators will increase scrutiny, for example on Indian and Chinese companies that continue to operate in Russia without significant reputational pressure to withdraw. China and India remain important markets for these OEMs.

Both understanding and implementation of the regulations involved considerable internal communication, internally and with corporate offices, many meetings, and regularly the use of outside counsel. However, the effectiveness of this counsel has varied. When comparing the advice received from outside counsel with that from partners, sister companies, or corporate guidance, it was often found to be conflicting.

The OEMs reported having IT systems with varying degrees of readiness, but in all cases, the impact has been substantial resulting in extensive cooperation between departments such as legal, customs, commercial, customer support, IT, and logistics. Compliance departments, including export control & compliance and customs, have had to prioritize sanctions on Russia, often at the expense of other projects. Three out of four OEMs indicated that significant delays occurred in other important control and compliance initiatives. Additionally, two out of four OEMs indicated that budgets had to be redirected for IT and outside counsel.

Impact of varied reactions from authorities
Companies with business units in different EU countries noted that customs authorities reacted differently to the sanctions. In some countries, shipments were blocked due to paperwork issues, while in others, the same paperwork was accepted.

There are serious concerns about the slow response or lack of response of authorities after notifying them of suspected violations based on Red Flags and stopping business, which has had significant safety implications. Companies are unsure if their measures were too drastic, as they have led to the loss of access to documentation, parts, and training. It was also noted that customers who were blocked due to sanctions are likely lost forever, as the damaged business relationships may drive them to competitors.

OEMs who had to leave material behind in Russia felt misunderstood initially, as there was no feasible way to retrieve the materials in time. This situation negatively impacted the effectiveness of the sanctions. To date, resolving open issues, such as material in western warehouses for which titles were not exchanged against the left-behind material in Russia, remains very difficult and administratively intensive. It requires extensive knowledge of the regulations and, in some cases, assistance from outside counsel.

Risk assessment and strategy
Companies were unable to anticipate all measures, but when given sufficient heads-up, they adapted by implementing stricter compliance based on risk assessments. This resulted in blocking more potential new customers and transactions. As one interviewee mentioned, they were "very likely being more compliant than needed." Additionally, 3 out of 4 companies indicated that they are turning away more business than they would have three years ago, deeming the risk unacceptable and therefore being quite rigorous in refusing customer orders.

In some cases, OEMs anticipated that the regulations would become more reasonable over time and acted accordingly, and thus for a while were not fully compliant. This expectation is evident in measures such as the certification of the supply chain for Russian Iron and Steel, as well as the implementation of the No-Russia Clause and DTP codes. Companies sometimes felt they had no other option but to anticipate these changes, as the existing regulations were impossible to implement without major disruptions or exposing their business to unacceptable risks.

Banks have become more conservative, not only blocking more payments from customers in regions exposed to sanctions, even if the customers themselves are not subject to sanctions, but also in general. This has made it difficult for some OEMs active in certain markets to receive payments, as banks' due diligence processes have become stricter. As a result, these hesitant banks are factored into the OEMs' risk assessments, since conducting business is futile if payments cannot be secured. This has led to certain customers having difficult access to their products and services, even if the customer is not subject to sanctions.

Two out of four OEMs have noted that increased compliance requirements from their suppliers, often other OEMs, are causing some customers to lose support from these suppliers. This lack of support leads to operational issues for airlines, which in turn affects other OEMs. The interlinked nature of the supply chain means that when suppliers, due to their risk assessments, decide not to work with certain operators, it negatively impacts tier-one suppliers and airframers. Consequently, airlines often seek assistance in convincing these suppliers to resume support or attempt to obtain parts and services

through higher-tier OEMs. This situation is causing significant internal work and coordination with suppliers, and solutions have not always been found yet.

None of the OEMs interviewed were directly involved in discussions with authorities, but their parent companies or corporate offices were in contact with regulators to request extensions, better explanations, or alternative implementations. The updated FAQ of December 2024 on the No-Russia Clause reflects these efforts, as it helped prevent major supply chain disruptions in January 2025.

On a positive note, the OEMs reported that the industry has become more united, sharing information and sometimes collaborating against the authorities, as well as cooperating with them on sanction implementations. Companies have become more vocal, seeking better cooperation and uniform enforcement of diversion measures. However, the constant shifting of priorities and the risk of alienating customers due to drastic measures remain significant challenges.

7 Conclusions and recommendations

This chapter summarizes the research findings, addresses the main research question and sub-questions, discusses the business relevance, and evaluates the business relevance of the research. It outlines the limitations, offers recommendations based on the findings, and suggests areas for further research.

7.1 Conclusions

By the 14th package of EU sanctions against Russia, the aerospace industry had to identify the relevant measures out of 496 of pages of regulations and 45 annexes to Regulation (EU) 833/2014. These regulations are accompanied by 424 pages of consolidated FAQs of the European Commission.

As the regulatory environment is determined by the clarity of instructions provided by the regulations adopted by public authorities and by the monitoring and enforcing capacities of these authorities, we must first assess whether the instructions of the sanctions on Russia are clear.

The fact that there was a need for 424 pages to answer frequently asked questions, leads to the conclusion that there must have been much confusion on the understanding and implementation of the sanctions. This is underscored by the consultant and law firms' communications on the topic, as also by the interviews conducted with four major aerospace OEMs.

Estimating the demand for consulting services to navigate Russian sanctions is challenging. However, the surge in advertising and newsletters from consulting and law firms highlights the significant focus on these sanctions. Companies and consultants frequently emphasize the difficulties in understanding and implementing these regulations. Discussions on LinkedIn and other platforms by consultants, law firms, and experts underscore the vagueness of the regulations, further illustrating the challenges businesses face. All four OEMs confirm that understanding and implementing these regulations has been a major resource drain.

The enforcement capacities of U.S. authorities regarding sanctions on Russia are generally considered to be high. Particularly, the OFAC has robust mechanisms in place to monitor and enforce compliance with sanctions, utilizing extensive resources, sophisticated tracking systems, and a strong legal framework to impose penalties on violators. Additionally, the U.S. had[145] launched initiatives like Task Force KleptoCapture to specifically target and hold accountable those who attempt to evade sanctions. Frequent updates and expansions of sanctions, along with coordination with international partners, further enhance enforcement capabilities. The extension of the statute of limitations for violations from five to ten years underscores their commitment to ensuring compliance with the sanctions on Russia.

[145] In February 2025, the Trump administration dismantled the KleptoCapture Task Force, which was originally established to seize the assets of Russian oligarchs as a punitive measure for Russia's invasion of Ukraine.
Despite the disbanding, ongoing cases against Russian oligarchs will continue, but the centralized management of these efforts has ended. The European Union is expected to maintain pressure on Russian oligarchs, which could have significant consequences for businesses operating in the region.

In line with Guimelli's (2017) findings, it is evident that the EU's lack of a robust monitoring structure poses significant challenges. While the EU's enforcement mechanisms encompass monitoring compliance, imposing penalties for violations, and coordinating with Member States to ensure uniform application of sanctions, the effectiveness of these measures can vary among Member States.

Overall, while the EU may face more challenges in enforcing sanctions compared to the U.S., the aerospace sector is also subject to the extraterritorial reach of U.S. regulations. Given the U.S.'s strong enforcement and monitoring capabilities, this leads to the conclusion that the overall enforcement ability of authorities in this context is medium to high.

Based on vague instructions and enforcement and monitoring capabilities of the authorities, we would conclude that the typology suggested by Guimelli (2017) ends up being: "Enforceable Delegation of Implementation". With vague instructions but strong monitoring/enforcement, the expected level of compliance would be overcompliance.

The key findings from the interviews on handling the circumvention and diversion regulations are sorted by topic:

1. **Complexity and evolving nature of regulations**: The sanctions were highly complex and continuously evolving, making it difficult for companies to keep up with the changes and implement the necessary measures effectively.
2. **Unclear guidelines**: The lack of clear and specific guidelines from authorities made it difficult for companies to know exactly what was required of them. This led to confusion and inconsistent implementation of the measures.
3. **Resource-intensive**: Implementing these processes required significant resources, including time, money, and personnel. There was extensive cooperation internally, with parent companies, corporate offices and assistance of outside counsel, to stay current with the continuous updates on the sanctions and to address new risk and regulatory changes. Companies had to divert resources from other important projects to focus on compliance, which was not always cost-effective, and introduced delays and risk in other areas where delays were experienced.
4. **Operational disruptions**: The need for extensive internal coordination and the implementation of new IT solutions led to operational disruptions. The short timeframes for compliance, such as the sudden requirement for DTP codes, added to these challenges. There is also a cascading effects of stringent compliance measures by lower or higher tier-suppliers within the aviation supply chain, causing additional work and disruptions.
5. **Overcompliance and undercompliance**: The vague instructions and high enforcement capabilities of authorities led to overcompliance in many cases. Companies became more conservative in their screening processes, often refusing business if there was any doubt about compliance, which resulted in lost business opportunities. Where there were vague instructions and the ability of the authorities are limited, companies reported not having met the deadlines and still looking for improvements in their own monitoring, possibly indicating undercompliance in these areas.

To answer the main research question, first the supporting questions will be answered.

The first supporting question was: **What measures do aerospace OEMs take to comply with the diversion and circumvention aspects of the sanctions on Russia?**

Aerospace OEMs have implemented several measures to comply with the diversion and circumvention aspects of the sanctions on Russia. They have strengthened their due diligence processes, including enhanced screening of customers, suppliers, and transactions against restricted party lists, and verifying ownership structures, beneficial ownership, and potential links to sanctioned individuals or entities. The inclusion of the "No-Russia Clause" in contracts to prohibit the re-exportation of goods to Russia has been achieved, partly due to updated regulations accommodating business needs. However, proper implementation of monitoring per Red Flags is still not fully realized, as IT solutions and standards for normal order quantities are still being developed. OEMs provide regular trainings to exposed personnel communicate about the risk of diversion and circumvention within the organization to maximize the understanding and compliance with the regulations. OEMs have updated and developed their IT systems to automate aspects of compliance management as much as possible, although challenges remain in fully integrating the requirements.

The second supporting question was: **Does the implementation of sanctions on Russia result in overcompliance or undercompliance in other areas?**

The implementation of diversion and circumvention measures in the sanctions on Russia, has generally resulted in more overcompliance rather than undercompliance. Some of the overcompliance is the result from strict implementation of IT solutions. Due to stringent risk assessments and low risk appetite of the OEMs, sometimes amplified by suppliers in the supply chain also taking decisions to halt business with common customers, certain operators and customers no longer are served.
Companies have become more conservative in their screening processes, refusing business if there is any doubt about compliance. This cautious approach has led to the blocking of more potential new customers and transactions, sometimes beyond what is legally required. In case of high demand for products, it allows companies to be selective, but this also means that some legitimate business opportunities are lost. There are potentially undesirable consequences for the customers who do not have access to necessary documentation and spare part services, as the risk of engaging with an entity that could cause difficulties is deemed unacceptable because of a rigorous stance on compliance. Furthermore, this overcompliance has also resulted in significant operational disruptions and increased workloads for compliance teams.

The main question for this research was: **“Is it reasonably and realistically possible to effectively implement enhanced due diligence processes to identify and mitigate the risk of circumvention and diversion of aerospace items to Russia, in a way that meets the authorities’ requirements, considering the legal obligations to prevent such activities without the obligation of result, while maintaining operational continuity in a cost-effective manner?”**

Hereby, “reasonably and realistically: was defined as: “Implementing enhanced due diligence processes that are feasible within the current operational and financial constraints, while effectively mitigating the risk of sanctions circumvention and diversion, and meeting the legal requirements set by authorities.”

Based on the findings in Chapter 6, it appears that while implementing enhanced due diligence processes to identify and mitigate the risk of circumvention and diversion of aerospace items to Russia was possible, it was not entirely reasonable or realistic given the circumstances. The continuous updates and the need for extensive internal coordination have made it difficult to maintain operational continuity in a cost-effective manner. Additionally, policymakers faced significant challenges in precisely calibrating

the sanctions' impact. This has resulted in a "learning by doing" process, with businesses bearing the brunt of the consequences.

Companies have taken considerable measures to comply, investing significant resources in updating compliance programs, implementing IT solutions, and enhancing their due diligence, often by contracting outside counsel. However, the feasibility and effectiveness of these efforts are significantly challenged by the complexity and evolving nature of the sanctions.

Vague instructions with high enforcement capabilities of authorities have led to overcompliance in some areas, and where instructions are vague and the capability of the authorities to enforce the measures is low, companies might be undercompliant.

In summary, while the implementation of the measures was feasible, it came at a significant cost to the companies involved. Compliance was mostly achievable but not entirely reasonable or realistic due to the high complexity, frequent updates, and unclear guidelines. These factors resulted in unreasonable resource demands, operational disruptions, and potential loss of future business.

7.2 Business relevance and recommendations

The significance of these findings cannot be overstated for businesses engaged in export controls and compliance with international sanctions.

Navigating the web of sanctions has always required a meticulous approach to ensure adherence to legal requirements and avoid potential penalties. Amid ongoing geopolitical tensions and anticipated further actions, diversion and circumvention control may become integral components of many more global sanctions regimes. This evolving scenario underscores the need for continuous adaptation and vigilance from both business and authorities. Additionally, there is a risk that other jurisdictions, such as China or Canada, will implement similar measures, further complicating compliance efforts for businesses.

Businesses should prioritize staying vigilant and proactive in adapting their compliance frameworks to the evolving landscape of international sanctions. To achieve this, it is crucial to invest in technological innovation and adaptation. By addressing the challenges in automating compliance processes, companies can develop more advanced IT tools that enhance compliance efficiency and effectiveness. This proactive approach will not only ensure adherence to regulations but also provide a competitive edge through improved operational integrity and risk management.

This research also highlighted that OEMs in the supply chain lack information about which other suppliers have blocked a common customer for compliance reasons and that this information is not available from the authorities. To protect the supply chain and obtain clearer answers from authorities regarding the legitimacy of blocking decisions, companies could share information amongst each other and cooperate contact the authorities. However, business must be cautious to avoid accusations of tortious interference.

Giumelli (2017, p.127) argues that when enacting legislation, authorities must possess at least as much knowledge as private actors to provide specific and actionable guidelines. The extensive volume of restrictive measures against Russia, along with the challenges OEMs faced in understanding and implementing them, underscores the need for enhanced cooperation and coordination between

sanctioning authorities and businesses. To address these challenges, businesses could leverage trade organizations, including international trade organizations where applicable, to address the varying approaches in different Member States. This would enable businesses to voice their concerns and ensure their perspectives are considered more effectively.

The competitive position of businesses is threatened by regulations that are overly stringent. Compliance is important, but getting it right is just as crucial for the authorities as it is for businesses to comply. Regulations must be practical and executable, and businesses need to be consulted before regulations are implemented to ensure they can keep up with the requirements. A collaborative approach will help in creating a balanced regulatory environment where compliance is achievable and sustainable. Enhanced coordination among EU Member States with input from business should lead to the establishment of clearer guidelines which are pivotal in reducing the administrative burden on companies.

Moreover, compliance can serve as both a competitive advantage and a competitive disadvantage. On one hand, businesses that effectively navigate and adhere to sanctions can build a reputation for reliability and trustworthiness, potentially attracting more customers and partners who value legal and ethical operations. On the other hand, the resources and efforts required to maintain compliance can be substantial, potentially putting smaller businesses or those with fewer resources at a disadvantage compared to larger, more established companies.

As one interviewee summarized: “Every day, entities are added to the blocked lists, indicating that authorities are indeed catching companies and individuals circumventing the sanctions. But was it worth the pain for business?”

Therefore, striking the right balance in compliance efforts, making them reasonable and realistic, is essential for maintaining competitiveness in the market.

7.3 Limitations and contributions

It is important to consider several limitations of this study. Firstly, given the current relevance of the topic and the potentially severe consequences of non-compliance, it was challenging to find export control and compliance employees in leading roles willing to participate in the interviews. Despite the interviews being completely anonymous and the companies unidentifiable, the results may still present a more favorable picture of their compliance than reality. Therefore, the outcomes of this research might differ if repeated after the sanctions are lifted and the focus shifts away from them.

Furthermore, although the interviews reflect real-world challenges and experiences related to compliance with export controls and sanctions, we cannot determine to what extent decisions on implementation are motivated solely by adherence to restrictive measures on Russia. Not all companies have the same market position. Where supply exceeds demand, a company's risk assessment will be influenced by the need to remain in certain markets. Conversely, when a company has more demand for its products than it can produce, it can afford to be more risk-averse, discarding entities only remotely associated with sanctions. In other words, we cannot ascertain whether a company's decision to refuse business is truly driven by compliance with export controls and sanctions, or if these measures are used as an excuse to avoid business in regions with lower margins.

Finally, due to time constraints and the availability of participants, this research gathered information from only four interviewees. Although these interviewees represent significant aerospace OEMs, the validity of their responses could not be cross-checked with their direct peers. Additional interviews or a survey could have provided a deeper understanding and may have offered insights into alternative recommendations.

This research provides a descriptive insight into the difficulties experienced by OEMS and the specific regulations and circumstances that may contribute to these difficulties. The same holds true for the validity of the recommendations. These are derived from the analysis of the interviews. However, to verify whether these recommendations are indeed valid and effective solutions for the research question, further testing is needed. To determine whether OEMs could benefit from these recommendations, additional interviews, and surveys by the relevant authorities, could be done.

7.4 Recommendations for future research

The imposition of sanctions on Russia has introduced complex regulatory challenges, particularly in the aerospace industry. The diversion and circumvention requirements imposed by these sanctions necessitate thorough examination to understand their unintended consequences. This section outlines key areas for further investigation to ensure that sanctions do not inadvertently compromise aviation safety. Additionally, it explores a broader research objective: determining whether authorities would write better sanctions by first consulting with businesses.

Balancing sanctions and safety: A call for improved coordination

The diversion and circumvention requirements imposed by these sanctions have significant implications for aviation safety, which need to be thoroughly examined. Future research should investigate the unintended consequences of sanctions, particularly concerning the safety of non-sanctioned airlines and their passengers.

In the case of the sanctions against Russia, the complexity of monitoring compliance actions and their operational impact is evident. If there is proof or strong suspicion of a breach of sanctions on Russia, such as through the no-Russia clause due to diversion, the OEM is obliged to halt all services to the airline and notify the relevant authority. This results in the airline losing access to parts, services, and documentation, which are essential for safe operations. In theory, the airline should cease operations without access to operational and maintenance documentation. However, national authorities for continuous airworthiness outside Europe or the U.S. might grant exemptions or remain unaware of the lack of minimum documentation and services, inadvertently compromising passenger security.

Communication and notification issues further complicate the situation. The European authority notified by the OEM of the breach may not relay this information to EASA or FAA, nor add the airline to the blocked entity list. Other OEMs may remain unaware and continue providing items and services to the airline, risking further diversion. The OEM that first identified the issue may hesitate to notify other OEMs due to fear of a lawsuit for tortious interference. Passengers in countries where authorities do not ground the aircraft are unaware that the airline operates without mandatory manuals, potentially boarding in unsafe conditions.

The unintended consequences of sanctions on Russia, particularly concerning aviation safety, highlight the need for further research into the responsibilities and communication practices among Original Equipment Manufacturers (OEMs) and regulatory authorities.

Suggestions for future research:

1. **Responsibilities and Communication:**
    - What responsibility do OEMs have to notify each other to protect the supply chain from unnecessary fines? Might this lead to increased lawsuits for tortious interference?
    - Should authorities inform all relevant parties (OEMs, MROs, leasing companies, etc.) about findings to ensure comprehensive awareness?
2. **Safety Concerns and Sanctions:**
    - How can the safety concerns related to sanctions be resolved? While sanctions on Russia take precedence over the obligation for minimum safety documentation, it is unlikely the intent was to expose passengers in non-Russian countries to risk due to an airline's diversion activities.
    - In the event of a serious incident or accident resulting from such a situation, who would be liable? From a legal perspective, the answer to this question appears complex because the terms “minimum safety requirements” are not explicitly defined in the relevant regulations or publications.
3. **International Compliance Challenges:**
    - How can an OEM resolve the specific issues in the case of entities/countries not targeted by EU sanctions but subject to similar sanctions imposed by third countries, such as the United States, regarding the obligation to provide safety documentation?

By addressing these questions, future research can provide valuable insights into the unintended consequences of sanctions on aviation safety and propose strategies for mitigating these risks.

Collaborative Frameworks for Effective Sanctions Implementation

Considering the intricate challenges of interpretation and implementation of sanctions, it becomes imperative to explore how authorities can better harmonize their efforts with businesses to mitigate these risks effectively. Enhanced communication such as collaborative frameworks and early consultations with the industry, may lead to more robust regulatory approaches that both maintain continuity in the businesses and adhere to sanctions

Authorities should first consult with businesses to understand how they interpret the sanctions and assess whether the desired measures can be implemented. Given the high volume of business transactions, companies will aim to automate processes as much as possible. This necessitates that authorities have a thorough understanding of the automation options available in major ERP systems. Additionally, authorities might consider consulting with the main ERP system providers to ensure the feasibility and effectiveness of the proposed measures.

List of references

Books, journal articles and publications

Beeson, Mark, Adjunct professor. "Sanctions Rarely Work, but Are They the Least Worst Option?" *University of Technology Sydney*, 12 Feb. 2024, https://www.uts.edu.au/news/business-law/sanctions-rarely-work-are-they-least-worst-option.

CNAS. *When Do Economic Sanctions Work Best*. https://www.cnas.org/publications/commentary/when-do-economic-sanctions-work-best

Giumelli, Francesco. "The role of for-profit actors in implementing targeted sanctions: The case of the European Union." *Security Privatization*, 1 Oct. 2017, pp. 123–141, https://doi.org/10.1007/978-3-319-63010-6_6.

Onderco, M, and F Giumelli . *States, Firms, and Security: How Private Actors Implement Sanctions, Lessons Learned from the Netherlands — the University of Groningen Research Portal*, research.rug.nl/en/publications/states-firms-and-security-how-private-actors-implement-sanctions-.

Verdier, Pierre-Hugues. "Sanctions Overcompliance: What, Why, and Does It Matter?" *SSRN*, 18 June 2023, ssrn.com/abstract=4476520.

Website content authorities

Bureau of Industry and Security. *Commerce Control List (CCL)*, https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

Bureau of Industry and Security. *Commerce Country Chart - Bis*, 8 Dec. 2023, https://www.bis.doc.gov/index.php/documents/regulations-docs/2253-supplement-no-1-to-part-738-commerce-country-chart/file.

Bureau of Industry and Security. *Russia Export Controls – List of Common High Priority Items*, BIS, 23 Feb. 2024, https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items.

Bureau of Industry and Security. *Entity List*, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

Bureau of Industry and Security. *Foreign Direct Product Rules*, www.bis.gov/foreign-direct-product-rules.

Bureau of Industry and Security. *Guidance on Reexports*, https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions

Bureau of Industry and Security. *Internal Compliance Program Elements*, https://www.bis.doc.gov/index.php/documents/compliance-training/export-administration-regulations-training/244-compliance-pdf/file

Bureau of Industry and Security. *Part 736 - General Prohibitions*, https://www.bis.doc.gov/index.php/documents/regulation-docs/413-part-736-general-prohibitions/file

Bureau of Industry and Security. *§ 734.3 Items Subject to the EAR.*, https://www.bis.gov/ear/title-15/subtitle-b/chapter-vii/subchapter-c/part-734/ss-7343-items-subject-ear

Department of Commerce, et al. *Cracking down on Third-Party Intermediaries Used To ...*, 3 Mar. 2023, https://www.justice.gov/nsd/media/1277536/dl?inline=

Department of Justice. "United Technologies Subsidiary Pleads Guilty to Criminal Charges for Helping China Develop New Attack Helicopter." *Office of Public Affairs*, 28 June 2012, https://www.justice.gov/archives/opa/pr/united-technologies-subsidiary-pleads-guilty-criminal-charges-helping-china-develop-new

EASA. "Continuing Airworthiness." *EASA*, www.easa.europa.eu/en/regulations/continuing-airworthiness. Accessed 23 Dec. 2024.

EASA. "EU Restrictive Measures against Russia." *EASA*, https://www.easa.europa.eu/en/the-agency/faqs/eu-restrictive-measures-against-russia

Electronic Code of Federal Regulations (eCFR). *The Federal Register*, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.9

Electronic Code of Federal Regulations (eCFR). *The Federal Register*, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736

Electronic Code of Federal Regulations (eCFR). *The Federal Register*, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-736/section-736.2

Electronic Code of Federal Regulations (eCFR). *The Federal Register*, www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-740/appendix-Supplement No. 1 to Part 740.

European Commission. *FAQ on Sanctions against Russia, Best Effort Obligation, Article 8A of Council Regulation (EU) No 83*, 22 Nov. 2024, finance.ec.europa.eu/document/download/65560de8-a13a-4a58-a87c-ddd27b14e6c1_en?filename=faqs-sanctions-russia-best-efforts-obligation_en.pdf.

European Commission. *Eqs Integrity Line*, eusanctions.integrityline.com/frontpage.

European Commission. *EU Enables Coordinated Export Controls by Compiling National Lists*, 26 Oct. 2023, policy.trade.ec.europa.eu/news/eu-enables-coordinated-export-controls-compiling-national-lists-2023-10-26_en.

European Commission. *EU Survey*, ec.europa.eu/eusurvey/runner/article-12-g-feedback.

European Commission. *Exporting Dual Use Items*, policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-Dual Use-items_en.

European Commission. *Guidance for EU Operators; Implementing Enhanced Due Diligence to Shield against Russia Sanctions Circumvention*, finance.ec.europa.eu/document/download/3c86c9a8-f09e-4092-ab8c-a9e678df1494_en?filename=guidance-eu-operators-russia-sanctions-circumvention_en.pdf.

European Commission. *List of Common High Priority Items (Version of February 2024)*, finance.ec.europa.eu/system/files/2023-09/list-common-high-priority-items_en.pdf. Accessed 12 Feb. 2025.

European Commission. *"No Re-Export to Russia" Clause*, 22 Feb. 2025, finance.ec.europa.eu/publications/no-re-export-russia-clause_en.

European Council. *COUNCIL DECISION (CFSP) 2024/1738 Amending Decision 2014/145/CFSP Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine*, 24 June 2024, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401738.

European Council. *Council Decision (CFSP) 2024/1738 of 24 June 2024 ...*, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401738.

European Council. *EU Sanctions against Iran - Consilium*, 20 July 2023, https://www.consilium.europa.eu/en/policies/sanctions-against-iran/

European Council. *EU Sanctions against Russia Explained - Consilium*, https://www.consilium.europa.eu/en/policies/sanctions-against-russia-explained/

European Council. *Iran: Eu Adopts New Restrictive Measures for Military Support To ...*, https://www.consilium.europa.eu/en/press/press-releases/2023/07/20/iran-eu-adopts-new-restrictive-measures-for-military-support-to-syria-and-russia-s-war-of-aggression-against-ukraine/

European Council. *Types of Sanctions the EU Adopts - Consilium*, https://www.consilium.europa.eu/en/policies/sanctions-different-types/

European Council. *Why the EU Adopts Sanctions - Consilium*, www.consilium.europa.eu/en/policies/why-sanctions.

European Parlement. *Foreign Policy: AIMS, Instruments and Achievements: Fact Sheets on the European Union: European Parliament*, www.europarl.europa.eu/factsheets/en/sheet/158/foreign-policy-aims-instruments-and-achievements. Accessed 22 Dec. 2024.

European Union. "COMMISSION RECOMMENDATION (EU) 2019/1318 on Internal Compliance Programmes for Dual Use Trade Controls under Council Regulation (EC) No 428/2009." *EUR*, 30 July 2019, eur-lex.europa.eu/eli/reco/2019/1318/oj/eng.

European Union. "Council Regulation (EU) 2022/1269 Amending Regulation (EU) No 833/2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine." *EUR*, 12 July 2022, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1269.

European Union. "Council Regulation (EU) 2024/1338 Amending Regulation (EU) 2023/1529 Concerning Restrictive Measures in View of Iran's Military Support of Russia's War of Aggression against Ukraine." *EU*, 14 May 2024, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1338.

European Union. "Council Regulation (EU) No 269/2014 of 17 March 2014 Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine." *EUR*, 17 Mar. 2021, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0269&qid=1731687869032.

European Union. "Council Regulation (EU) No 833/2014 of 31 July 2014 Concerning Restrictive Measures in View of Russia's Actions Destabilising the Situation in Ukraine." *EUR-Lex*, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0833.

European Union. *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Definition of Criminal Offences and Penalties for the Violation of Union Restrictive Measures and Amending Directive (EU) 2018/1673*, 3 Apr. 2024, data.consilium.europa.eu/doc/document/PE-95-2023-INIT/en/pdf.

European Union. "EU Sanctions Map." *EU Sanctions Map*, https://www.sanctionsmap.eu/#/main

European Union. *Guidance Note on Blocking Statute*, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018XC0807%2801%29&amp=&qid=1625557217449.

European Union. *Règlement - 2021/821 - En - EUR-Lex*, eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32021R0821.

Office of Foreign Asset Control. *Impact of Sanctions and Export Controls on Russia's Military-Industrial Complex*, 14 Oct. 2022, ofac.treasury.gov/media/928856/download?inline.

Office of Foreign Assets Control. *Airbus Agrees to Pay over $3.9 Billion in Global Penalties to Resolve Foreign Bribery and Itar Case*, 6 Feb. 2025, https://www.justice.gov/archives/opa/pr/airbus-agrees-pay-over-39-billion-global-penalties-resolve-foreign-bribery-and-itar-case

Office of Foreign Assets Control. *Attorney General Merrick B. Garland Announces Launch of Task Force Kleptocapture*, 22 Mar. 2022, https://www.justice.gov/archives/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture

Office of Foreign Assets Control. *Entities Owned by Blocked Persons (50% Rule)*, ofac.treasury.gov/faqs/topic/1521.

Office of Foreign Assets Control. *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*, ofac.treasury.gov/media/37751/download?inline=.

Office of Foreign Assets Control. *OFAC Guidance on Extension of Statute of Limitations*, ofac.treasury.gov/recent-actions/20240722.

Office of Foreign Assets Control. "Reporting, Procedures and Penalties, 31 CFR Part 501." *Federal Register*, 13 Sept. 2024, https://www.federalregister.gov/documents/2024/09/13/2024-20674/reporting-procedures-and-penalties

Office of Foreign Assets Control. *Russia-Related Sanctions*, ofac.treasury.gov/sanctions-programs-and-country-information/russia-related-sanctions.

Office of Foreign Assets Control. *Specially Designated Nationals (SDNs) and the SDN List*, ofac.treasury.gov/faqs/18.

U.S. Department of Commerce. *Bureau of Industry and Security*, www.commerce.gov/bureaus-and-offices/bis. Accessed 12 Sept. 2024.

U.S. Department of Commerce. *U.S. Department of Commerce & Bureau of Industry and Security Russia and Belarus Rule Fact Sheet*, 14 Mar. 2022, https://www.commerce.gov/news/fact-sheets/2022/02/us-department-commerce-bureau-industry-and-security-russia-and-belarus

U.S. Department of State Directorate of Defense Trade Controls. *ITAR & Export Controls*, https://www.pmddtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_itar_landing

Website content other

Aviacionline. "Magical Mistery Tour: An Airbus A320 and Three A330s of a Shady African Airline Flew to Minsk; ¿to End up in Russia?" *Aviacionline*, 21 Aug. 2024, https://www.aviacionline.com/magical-mistery-tour-an-airbus-a320-and-three-a330s-of-a-shady-african-airline-flew-to-minsk-to-end-up-in-russia?utm_content=cmp-true#google_vignette.

Aviation Week, "Russia's S7 Develops Engine Blade Capabilities." *Aviation Week Network*, 4 Oct. 2024, https://www.aviationweek.com/air-transport/airlines-lessors/russias-s7-develops-engine-blade-capabilities.

Baghirov, Orkhan. “Armenia’s Role in Helping Russia Circumvent Sanctions.” *Jamestown*, 25 May 2023, https://www.jamestown.org/program/armenias-role-in-helping-russia-circumvent-sanctions/.

Beeson, Marc, Adjunct professor. “Sanctions Rarely Work, but Are They Still the Least Worst Option?” *The Conversation*, 6 Feb. 2024, https://theconversation.com/sanctions-rarely-work-but-are-they-still-the-least-worst-option-199494

Bodell, Luke. “GE Aerospace: Aviation Supply Challenges Will Continue in 2025.” *Simple Flying*, 22 June 2024, https://www.simpleflying.com/ge-aerospace-supply-challenges-2025/.

Boffey, Daniel. “Moscow Importing Western Aircraft Tyres despite Ban, Says Ukraine Agency.” *The Guardian*, Guardian News and Media, 12 Sept. 2024, https://www.theguardian.com/business/2024/sep/12/moscow-importing-western-aircraft-tyres-despite-ban-says-ukraine-agency?CMP=Share_iOSApp_Other.

Chang, Felix K. “India’s Neutrality and Strategic Relations with China, Russia, and the West.” *Foreign Policy Research Institute*, 25 Apr. 2022, https://www.fpri.org/article/2022/04/indian-foreign-policy-and-the-russian-ukrainian-war/.

Congressional Research Service. *Product Details R45618*, https://www.crsreports.congress.gov/product/details?prodcode=R45618. Accessed 20 Oct. 2024.

Disalvatore, James. “To Keep Flying, Russian Airlines Hunt and Scavenge for Spare Parts.” *Kharon*, 23 May 2025, www.kharon.com/brief/to-keep-flying-russian-airlines-hunt-and-scavenge-for-spare-parts.

Gallo, Ernest. “Among Conflicts and Sanctions: Kazakhstan’s Role in Navigating Peace and Resolving Crises.” *The Geopolitics*, 29 Sept. 2023, https://www.thegeopolitics.com/among-conflicts-and-sanctions-kazakhstans-role-in-navigating-peace-and-resolving-crises/.

Jack, Victor. “How Turkey Became Putin’s ‘pit Stop’ for Selling Camouflaged Fuel to the EU.” *POLITICO*, POLITICO, 19 June 2024, https://www.politico.eu/article/how-turkey-become-vladimir-putin-pit-stop-sell-camouflage-fuel-eu/.

James, Olivier. “En Russie, l’étonnant Maintien En Vol de Centaines d’airbus et de Boeing.” *Www.Usinenouvelle.Com*, L’Usine Nouvelle, 16 Sept. 2024, https://www.usinenouvelle.com/article/en-russie-l-etonnant-maintien-en-vol-de-centaines-d-airbus-et-de-boeing.N2217848

Juliano, Laura, et al. “Fixing Aerospace’s Supply Chain for Casting and Forging.” *BCG Global*, BCG Global, 17 July 2024, https://www.bcg.com/publications/2024/fixing-aerospaces-supply-chain-for-casting-and-forging

Kefalogiannis, Manolis. “Parliamentary Question: Turkey’s Refusal to Go along with Sanctions on Russia and Its Transformation into a Russian ‘Transit Hub’: E-003495/2022: European Parliament.” *E*, 25 Oct. 2022, https://www.europarl.europa.eu/doceo/document/E-9-2022-003495_EN.html

Loxton, Emma, et al. “Addressing Continued Turbulence: The Commercial-Aerospace Supply Chain.” *McKinsey & Company*, McKinsey & Company, 3 Apr. 2024, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/addressing-continued-turbulence-the-commercial-aerospace-supply-chain

Matthews, Chris, et al. “British Firms among Companies to Have Exported Aircraft Parts That Reached Russia.” *The Guardian*, Guardian News and Media, 20 Feb. 2025, https://www.theguardian.com/business/2025/feb/20/british-firms-among-those-that-exported-aircraft-parts-which-reached-russia

NASA. *Aerospace Supply Chain and Manufacturing - NASA ...*, 4 Feb. 2020, https://www.nari.arc.nasa.gov/sites/default/files/attachments/1-pk-feb4-5-SupplyChainManagement.pdf.

Nasr, Vali R, et al. “Do Sanctions Actually Work? Experts Evaluate the Efficacy of This Widely Used Foreign Policy Tool.” *Johns Hopkins in Washington, D.C.*, 15 May 2024, https://washingtondc.jhu.edu/news/do-sanctions-actually-work-experts-evaluate-the-efficacy-of-this-widely-used-foreign-policy-tool/.

Nikoladze, Maia. “How Is China Mitigating the Effects of Sanctions on Russia?.” *Atlantic Council*, 14 June 2023, https://www.atlanticcouncil.org/blogs/econographics/how-is-china-mitigating-the-effects-of-sanctions-on-russia/

Osborne, Tony. “Leonardo Sued for $2.6B by AW169 Crash Victim’s Family.” *Aviation Week Network*, 10 Jan. 2025, https://www.aviationweek.com/business-aviation/safety-ops-regulation/leonardo-sued-26b-aw169-crash-victims-family.

Pambukhchyan, Anna. “Armenia’s Exports to Russia Raise Concerns over Sanctions Circumvention.” *Euractiv*, 13 Feb. 2025, https://www.euractiv.com/section/armenia/news/armenias-exports-to-russia-raise-concerns-over-sanctions-circumvention/

Pitti, Fabrice. “The Latest in Aerospace: An Industry Grounded.” *Dow Jones*, 8 Nov. 2022, https://www.dowjones.com/professional/risk/resources/risk-blog/aerospace-industry-grounded

Putz, Catherine. “As Focus on Sanctions Evasion in Kyrgyzstan Intensifies, Government Promises Action.” – *The Diplomat*, The Diplomat, 21 July 2023, https://www.thediplomat.com/2023/07/as-focus-on-sanctions-evasion-in-kyrgyzstan-intensifies-government-promises-action/.

Ribakova, Elina. *The U.S. Technology Fueling Russia’s War in Ukraine: How and Why*, 27 Feb. 2024, https://www.piie.com/sites/default/files/2024-02/ribakova2024-02-27testimony.pdf

RTX. “SEC Filing.” *RTX*, 17 July 2023, investors.rtx.com/node/40741/html.

Russell, Edward. “Airbus A320neo Pratt Engine Issues to Ground 650 Planes next Year.” *Airline Weekly*, 12 Oct. 2023, https://www.airlineweekly.skift.com/2023/09/airbus-a320neo-pratt-engine-issues-to-ground-650-planes-next-year/.

Scarpino, Rowan, and Jocelyn Trainer. “Sanctions by the Numbers: 2023 Year in Review.” *CNAS.Org*, 27 June 2024, https://www.cnas.org/publications/reports/sanctions-by-the-numbers-2023-year-in-review

Statista Research Department. *Sanctions Imposed on Russia by Target 2024 | Statista*, 28 Jan. 2025, https://www.statista.com/statistics/1293531/western-sanctions-imposed-on-russia-by-target/

Stępień, Beata, et al. “The impact of external pressure on companies’ responses to sanctions – an international comparative study.” *European Journal on Criminal Policy and Research*, vol. 30, no. 2, 7 Mar. 2024, pp. 1–26, https://link.springer.com/article/10.1007/s10610-024-09576-y

Stewarts. “The Russian Aviation Litigation.” *Stewartslaw*, 3 Feb. 2025, www.stewartslaw.com/news/the-russian-aviation-litigation/.

The Moscow Times. “Half of Russia’s Airbus A320neo Fleet Grounded amid Engine Problems, Sanctions – Kommersant.” *The Moscow Times*, 21 Nov. 2024, https://www.themoscowtimes.com/2024/11/21/half-of-russias-airbus-a320neo-fleet-grounded-amid-engine-problems-sanctions-kommersant-a87087

Tokar, Dylan. “RTX Sets aside $1.24 Billion to Resolve Government Probes.” *The Wall Street Journal*, 25 July 2024, https://www.wsj.com/articles/rtx-sets-aside-1-24-billion-to-resolve-government-probes-d91a0aaf.

Vanderfort, Richard. “RTX to Pay $200 Million over Export Control Violations.” *The Wall Street Journal*, 30 Aug. 2024, https://www.wsj.com/articles/rtx-to-pay-200-million-over-export-control-violations-46d653b1

Welt, Cory. *U.S. Sanctions on Russia: Legal Authorities and Related Actions*, Congressional Research Service, 26 Apr. 2024, https://www.crsreports.congress.gov/product/pdf/R/R48052.

Williams, Julie, et al. “United States Extraterritoriality: European Union Sovereignty at Stake.” *International Bar Association*, www.ibanet.org/article/cf85e59e-6564-4aa3-9408-3f47c6449c9d. Accessed 30 Mar. 2025.

Woods, Eric. “Russia’s Aerospace Catastrophe: How Export Controls and Sanctions Will Affect Russia.” *CNS Trade Compliance*, 22 Mar. 2022, https://www.sites.middlebury.edu/tradecompliance/2022/03/22/russias-aerospace-catastrophe-how-export-controls-and-sanctions-will-affect-russia/.

Zhumagulova, Kamshat, and Rahimbek Abdrahmanov. “How Kazakhstan Helps Russia Bypass Western Sanctions.” *The Diplomat*, 25 Oct. 2023, https://www.thediplomat.com/2023/10/how-kazakhstan-helps-russia-bypass-western-sanctions/.

Annex 1: Interviews

Interview protocol

The interviews were semi-structured and conducted in the interviewee's native language to facilitate conversation and minimize misunderstandings. Each interview began with an introduction explaining the general goal of the interview, not included in the interview questionnaire below. Two interviewees were known to the researcher and two interviewees had little or no prior relationship with the researcher.
A standard set of questions was used for each interview, though the order varied. The interviews started by general questions about the business, company structure, and specifically the organization of the export control function within the company as well as the interviewee's experience in this function.
Follow-up questions were sometimes asked after the interview, as all interviewees offered to answer further questions or clarify situations if needed.
The topics addressed and questions asked during the interviews are listed below.

Interview topics and questions

Interview questions that align with the research questions on sanctions and compliance challenges for Original Equipment Manufacturers (OEMs) in the aerospace industry:

1. **Your company and interviewee:**
   a) OEM type, head office or subsidiary, only commercial airline products or other as well?
   b) How is your export department organized and who does it fall under (Finance, Legal, other)?
   c) Experience? Experience in team? Use of Corporate of Outside Counsel for legal help?
2. **Impact of sanctions:**
   a) How have the recent sanctions on Russia affected your company's operations in the aerospace industry?
      i. Have you got assets stranded in Russia - possibility for orderly withdrawal?
      ii. How have you managed staying up to date with both the EU packages and the U.S. updates? Have you been able to filter out the relevant updates in a timely manner?
      iii. How have the sanctions packages and updates changed your export control department and other departments (customs, logistics, contracts)
      iv. How have the sanctions on Russia affected your need and budget for outside counsel? Were there any sanctions in particular that have demanded special attention? Have you been happy with outside counsel, able to understand your business and provide relevant answers and solutions (not just legal opinions about criminal liability etc.)?
   b) Can you describe any specific challenges your company has faced due to these sanctions?
3. **Compliance strategies:**
   a) What strategies has your company implemented to comply with the sanctions and prevent diversion and circumvention?
      i. Certification of supply chain for **Russian iron and steel**
      ii. **HS (CN codes)** – monitoring of unusual activity
      iii. **No-Russia Clause** and implementation of **DTP** codes in the EU – was it possible, what did it take, can you estimate the effort?
      iv. OFAC – change to statute of limitations for civil and criminal violation of the IEEPA and TWEA from 5 to 10 years (applies to Cuba, Iran, Russia). Have you been able to update the **record keeping** requirements accordingly? Any other issues, concerns with this?

v. **Screening** and KYC and KYS process: have you been able to consider the risk of diversion and circumvention when screening?
vi. **Task Force KleptoCapture** - Have your exports been affected, have you spent a lot of time investigating? If so, was it to the expense of other projects, programs, tasks?

b) How effective have these strategies been in ensuring compliance?

4. **Regulatory challenges**:
   a) What are the main regulatory challenges your company faces in adapting to the complex sanctions landscape of the European Union and the United States?
   b) How does your company handle the differences and contradictions in U.S. and EU regulations?
   c) Have you had to report any diversion violations to authorities? Any fall-out from this?
5. **Risk management**:
   a) How does your company assess and manage the risks associated with non-compliance?
   b) What measures are in place to mitigate these risks?
6. **Technological solutions**:
   a) Has your company adopted any technological solutions to enhance compliance with sanctions?
   b) If so, can you provide examples of they been implemented and their impact?
7. **Collaboration and support**:
   a) How does your company collaborate with other industry participants to ensure compliance with sanctions?
   b) What kind of support or resources would be beneficial to improve compliance efforts?
8. **Resource allocation**:
   a) How many resources (e.g., financial, human, technological) has your company had to allocate to comply with the sanctions on Russia?
   b) Can you provide examples of specific areas where additional resources were necessary?
9. **Overcompliance and non-compliance**:
   a) In which areas do you believe your company may have become overcompliant?
   b) Are there any areas where your company might not have been compliant enough? What were the reasons for this?
   c) Can you provide examples of situations where overcompliance or non-compliance occurred and the impact it had on your operations?
10. **Handling mixed regulations and ambiguity in implementations:**
    a) How has your company handled the authorities' regulations that now mix customs codes with export controls?
    b) Have you had to update your systems to accommodate these changes, or are there a lot of manual checks involved?
    a) Have you encountered any ambiguity in implementing the sanctions due to unclear requirements?
    b) Did this ambiguity leave room for interpretation that caused extra work afterwards?
11. **Identifying diversion and circumvention**:
    a) Has your company identified any instances of diversion and circumvention of the sanctions?
    b) What do you think are the chances of accurately identifying such instances?
12. **Business consequences:**
    a) Did you lose any business opportunities, or do you expect that you will lose any future business because of these sanctions and how it has affected the relationship between your company and the client?