IADC 2026 MIDYEAR MEETING

INTERNATIONAL SANCTIONS, EXPORT CONTROLS AND TARIFFS: THE RISKS OF RUNNING BUSINESS ON A GLOBAL SCALE

Authors: Damien Devot, Meyer Fabre Avocats, Paris, France; Jennifer Gellie, Pillsbury Winthrop Shaw Pittman LLP, Washington, D.C. USA; Gabriel Sidere, Florida Wellness Company, Bucharest, Romania; and Samantha Welch, BRG, New York, New York USA

Date: December 19, 2025

I. Introduction

In-house lawyers and counsels are increasingly confronted with the complexities of international sanctions. The impact of these measures, however, can vary significantly depending on whether they originate from the United States or the European Union. This paper aims to analyze the differences between US and EU sanctions regimes and assess their practical implications for businesses.

The paper focuses first on an overview of US sanctions in particular through the structure and functioning of the Office of Foreign Assets Control (OFAC) (Section II). It will then explore how the US deals with Export controls (Section III).

The paper then turns to the European Union, highlighting the EU approach to both sanctions and export controls, illustrating how these measures are adopted and applied in practice (Section IV).

Finally, the study considers the broader effects of these sanctions on companies and corporate compliance strategies (Section V).

II. Office of Foreign Assets Control – US Sanctions

A. Background on the US Treasury's Office of Foreign Assets Control

OFAC operates under Presidential national emergency powers and specific legislation to administer and enforce economic sanctions based on US foreign policy and national security goals. Although the US had used sanctions in a variety of cases since the War of 1812, OFAC was formally established in 1950 when China entered the Korean War and President Truman declared a national emergency to block Chinese and North Korean assets under U.S. jurisdiction. Sanctions are one tool that the US Government has at its disposal to exert influence on the international stage. Other non-military options exist, such as Section 311 of the USA PATRIOT Act, which gives Treasury the power to name jurisdictions or entities a "primary money laundering concern" and cause financial institutions subject to the USA PATRIOT Act to take action with respect to such jurisdictions, entities or transactions.

B. The OFAC Regime[1]

[1] Home | Office of Foreign Assets Control

1. Sanctioned Target Scope

OFAC administers both comprehensive, broad based jurisdictional sanctions and targeted sanctions, either sectoral or against specific individuals, entities and wallets.

Jurisdictional based sanctions include those that broadly target a country, such as those on North Korea, Iran, Cuba, and certain jurisdictions in Ukraine (i.e., Crimea, Donetsk, Luhansk).[2]

Targeted sanctions include sectoral sanctions that focus on a specific scope such as the energy or defense, or that place limits on certain financial transactions. Sectorial sanctions give the US Treasury flexibility to target and weaken specific parts of the foreign country's economy, such as oil used to fund nuclear and military spending, while permitting transactions that would be in the interest of the U.S. government to continue, such as agriculture.

The most targeted sanctions are those that target specific persons, entities or wallets, termed Specially Designated Nationals, or SDNs. SDN designations are not country specific, but include targeted narcotics traffickers, weapons proliferators, and others, as well as terrorists, a category of SDNs, Specially Designated Global Terrorists (SDGTs).[3] Entities owned by a person on the SDN List (defined as a direct or indirect ownership interest of 50 percent or more) are also blocked.

2. Application and Licensing

OFAC applies to persons, (i.e., both individuals and entities,) in the U.S., as well as U.S. persons anywhere in the world. Sanctions can have extraterritorial application.

In addition, the U.S. can impose secondary sanctions on foreign financial institutions that conduct activity that if it were in the U.S. would be prohibited. Specifically, in response to Russia using such institutions to evade sanctions, the U.S. may impose sanctions on financial institutions conducting transactions with its military and industrial base.[4]

OFAC maintains General Licenses to allow exceptions to its sanctions programs. These licenses are typically time-based, allowing for wind down of certain transactions, or specific carve outs such as allowances for humanitarian relief. Those that wish to participate in a prohibited transaction or activity that is not covered by a General License may apply to OFAC for a specific dispensation. OFAC's Best Practices for License Applicants[5] helps companies understand the information OFAC needs to process the application.

3. Strict Liability

[2] As of November 2025.
[3] Document – Executive Order 13224.
[4] SANCTIONS ADVISORY Updated Guidance for Foreign Financial Institutions on OFAC Sanctions Authorities Targeting Support to Russia's Military-Industrial Base
[5] Quick-Reference Guide: License Applications

Although a company's actions, such as whether there was a compliance program, and self-disclosure, will be considered in any enforcement action, OFAC violations generally carry strict liability.

C. Recent Developments in Sanctions

Sanctions are a rapidly evolving area, and a challenge for legal and compliance teams to keep pace and protect their firms. The following sections detail some recent developments as of November 2025.

1. Sanctions Lifted on Syria[6]

In spring 2025, following the ouster of Bashar al-Assad, via Executive Order 14312, the U.S. lifted its comprehensive sanctions on Syria, and pivoted remaining sanctions to target, among others, those threatening peace, security and stability of Syria, those in the former Assad regime, those responsible for serious human rights abuses, Iranian proxies, and those illicitly producing and proliferating Captagon.[7] This was a material reversal of U.S. policy, terminating the national emergency related to Syria itself, and revoking six executive orders related to the Syrian sanctions. The revocation is intended to allow Syria to rebuild its economy by allowing transactions and investment into the country, to promote stability and peace.

2. Foreign Terrorist Organization (FTO) Designations[8]

Pursuant to Executive Order 14157, *Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists*, the Department of State named eight cartels[9] as FTOs and SDGTs. The designations are part of the Trump administrations prioritization of total elimination of cartels and transnational criminal organizations.[10] Seven of the designations were already blocked SDNs, however the added terrorist designation includes added restrictions and liability. Specifically, it is unlawful to knowingly provide "material support or resources" to these entities. The restrictions apply to not just US companies, but also non-US companies with personnel or operations in the US, non-US companies with US persons located anywhere, and any company or financial institution engaged with a US correspondent bank. Further, dealings may also subject foreign financial institutions

---

[6] Tri-Seal Advisory: Sanctions and Export Controls Relief for Syria; Providing for the Revocation of Syria Sanctions – The White House

[7] Promoting Accountability for Assad and Regional Stabilization Sanctions (PAARSS) | Office of Foreign Assets Control

[8] Federal Register :: Designating Cartels and Other Organizations as Foreign Terrorist Organizations and Specially Designated Global Terrorists

[9] Tren de Aragua (TdA), Mara Salvatrucha (MS-13), Cártel de Sinaloa, Cártel de Jalisco Nueva Generación (CJNG), Cártel del Noreste (CDN), La Nueva Familia Michoacana (LNFM), Cártel de Golfo (CDG), and Cárteles Unidos (CU).

[10] Total Elimination of Cartels and Transnational Criminal Organizations

that "knowingly conducted or facilitated any significant transaction on behalf of any person whose property and interests in property are blocked" to secondary sanctions.[11]

The FTO designations open companies to both civil and criminal liability. Particularly, U.S. nationals injured by acts of terrorism may sue for damages under the Anti-Terrorism Act if a company aids and abets such acts or conspires with an FTO or its affiliates or agents in support of such acts. On the criminal side, the government could try to attribute knowledge or actions of a specific employee to the argument that a company is providing material support to a cartel.[12]

3. Russia

In the beginning of 2025 when Attorney General Bondi dissolved Russia-focused Task Force KleptoCapture and the Kleptocracy Asset Recovery Initiative,[13] indications were that the U.S. was poised to ease sanctions on Russia. However, as peace in Ukraine remains elusive, Treasury has taken additional measures including sanctions in October 2025 on Russia's two largest oil companies, Rosneft and Lukoil, and their subsidiaries in part to "degrade the Kremlin's ability to raise revenue for its war machine."[14] President Trump campaigned in part on bringing about an end to the war in Ukraine, and is deeply vested in seeing hostilities end at least for the duration of his term. As of November 2025, it is unclear whether the sanctions, including secondary sanctions on foreign financial institutions servicing the Russian military-industrial complex, combined with other pressures like imposing tariffs on countries buying Russian oil, will be enough to bring Russia to the negotiating table, or if Ukraine will cede land to Russia in hopes of ending the conflict. Critically, it is also unclear whether the thousands of children abducted to Russia and Belarus will make their way home again.[15]

4. Iran

In February 2025, the White House issued National Security Presidential Memorandum 2/ NSPM2 directing the heads of U.S. agencies to implement measures to impose maximum pressure on Iran to curtail its nuclear ambitions and malign influence in the region. With respect to sanctions, NSPM2 directed the Secretary of the Treasury to "impose sanctions on persons for which Treasury has evidence of violation of one or more Iran-related sanctions" and to "review for modification or rescission any general license, FAQ, or other guidance that provides Iran or any of its terror proxies economic or financial relief." [16]

---

[11] IN11205.4.pdf - Designating Cartels and Other Criminal Organizations as Foreign Terrorists: Recent Developments

[12] 18 USC 2339B: Providing material support or resources to designated foreign terrorist organizations; 18 U.S. Code § 2333 - Civil remedies | U.S. Code | US Law | LII / Legal Information Institute

[13] Total Elimination of Cartels and Transnational Criminal Organizations

[14] Treasury Sanctions Major Russian Oil Companies, Calls on Moscow to Immediately Agree to Ceasefire | U.S. Department of the Treasury

[15] New Sanctions Reinforce U.S. Efforts to Ensure Justice for Ukraine's Children - United States Department of State

[16] National Security Presidential Memorandum/NSPM-2 – The White House

In addition, Treasury was required to, among other things: issue guidance to relevant business sectors including shipping, insurance, and port operators, ensure that Iraq and the Gulf states are not used by Iran for sanctions evasion or circumvention. Throughout 2025 the administration-imposed sanctions aligned to NSPM2, targeting a geographically diverse set of parties supporting Iran, including companies in China, Hong Kong, Singapore, and the Gulf purchasing or supporting the movement of Iranian oil. In October, following the UN snapback and re-instatement of sanctions targeting Iran's nuclear program, OFAC promulgated sanctions against a number of targets within Iran's weapons and defense infrastructure.[17] Both Russia and Iran transport sanctioned oil and gas using a shadow fleet of aged tankers that use various methods to hide their illicit activities, including but not limited to, ship-to-ship transfers to comingle sanctioned oil with non-sanctioned oil, AIS spoofing, stripping names from tankers, swapping IMO numbers, causing a number of environmental and safety risks.

D. Recent Enforcement Actions

Sanctions are not industry specific, so all companies must be vigilant. In one case focused on the insurance industry, in November 2024, American Life Insurance Company (ALICO), a subsidiary of MetLife, Inc. agreed to pay $178,421 to settle potential civil liability for apparent violations of OFAC sanctions on Iran. ALICO issued group medical and life insurance policies, collected premiums, and paid claims to several schools and entities located in the United Arab Emirates and owned or controlled by the Government of Iran. ALICO processed 2,331 transactions amounting to $446,077.[18]

Another recent case brought by OFAC focused on the cryptocurrency industry. In September 2025, OFAC announced that ShapeShift AG, a digital asset exchange incorporated in Switzerland and operating from Denver, Colorado, agreed to pay $750,000 to settle potential civil liability for apparent violations of multiple sanctions programs. ShapeShift engaged in digital asset transactions on its exchange platform with users located in Cuba, Iran, Sudan, and Syria on 17,183 occasions.[19]

Finally, another example of an enforcement action involves the beverage industry. In October 2024, OFAC announced an $860,000 settlement with Vietnam Beverage Company Limited (VBCL). VBCL agreed to settle its subsidiaries' potential civil liability for 43 apparent violations of the North Korea Sanctions Regulations. According to the release, VBCL's subsidiaries caused U.S. financial institutions to process approximately $1,141,547 in payments for the sale of alcoholic beverages to North Korea.[20]

---

[17] Treasury Targets Iranian Weapons Procurement Networks Supporting Ballistic Missile and Military Aircraft Programs | U.S. Department of the Treasury

[18] download - Enforcement Release: November 14, 2024 - American Life Insurance Company Settlement with OFAC

[19] Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and ShapeShift AG | Office of Foreign Assets Control

[20] Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Vietnam Beverage Company Limited | Office of Foreign Assets Control

III. Bureau of Industry and Security – U.S. Export Controls

A. Background on the U.S. Commerce Department's Bureau of Industry and Security

1. The Bureau of Industry and Security (BIS), under the U.S. Department of Commerce, administers and enforces export controls to protect U.S. national security, foreign policy interests, and economic competitiveness.
2. Export controls regulate the transfer of sensitive goods, technology, and software to foreign destinations or persons.
3. While the U.S. has long restricted certain exports for national security reasons, BIS was formally established in 1980 to consolidate export administration and enforcement functions.
4. Export controls are a critical non-military tool for preventing the proliferation of weapons of mass destruction, safeguarding advanced technologies, and countering adversarial capabilities.

B. The Export Control Regime

1. Controlled Scope

BIS administers the Export Administration Regulations (EAR), which apply to "dual-use" items—goods, software, and technology with both civilian and military applications. Controls are based on:

i. Commerce Control List (CCL): Categorizes items by Export Control Classification Number (ECCN) and specifies reasons for control (e.g., national security, anti-terrorism, nuclear nonproliferation).
ii. Country Chart: Determines licensing requirements based on destination and reason for control.
iii. Entity List and Denied Persons List: Targets specific foreign entities and individuals involved in activities contrary to U.S. interests, such as military modernization or WMD proliferation.

Controls range from broad restrictions on entire categories of technology to highly targeted measures against specific companies or individuals. For example, advanced semiconductor manufacturing equipment may require a license for export to China, while basic consumer electronics may not.

iv. Application and Licensing - the EAR applies to:
- U.S. persons worldwide and any item subject to the EAR, including foreign-made items incorporating controlled U.S. content.
- Certain extraterritorial provisions, such as the Foreign Direct Product Rule, which extends U.S. jurisdiction to foreign-produced items derived from U.S. technology.

v. Licensing is managed through BIS's SNAP-R system. Applicants must provide detailed technical specifications, end-use statements, and end-user certifications. BIS guidance and advisory opinions help companies navigate complex licensing requirements. BIS issues:

General Licenses: Broad authorizations for low-risk transactions.
Specific Licenses: Required for sensitive exports or destinations.

2. Strict Liability vs. Knowledge/Willfulness

i. Export control violations under the EAR generally carry strict liability for civil penalties. In other words, intent is not required for enforcement.
ii. Companies can face penalties even if violations were inadvertent.
iii. However, criminal liability applies when violations are knowing and willful, such as deliberate attempts to evade licensing requirements or falsify documentation.
iv. Criminal penalties can include substantial fines and imprisonment (up to 20 years per count under the Export Control Reform Act).
v. Mitigating factors, such as voluntary self-disclosure and robust compliance programs, can reduce penalties, but willful misconduct significantly increases exposure.

C. Recent Developments in Export Controls

Export controls evolve rapidly in response to geopolitical and technological changes. Below are notable developments as of November 2025:

1. Semiconductor Restrictions on China

In October 2025, BIS expanded controls on advanced semiconductor manufacturing equipment and AI-related chips to China, citing national security concerns. The rules broadened the Foreign Direct Product Rule and added new entities to the Entity List, significantly impacting global supply chains.

2. BIS Affiliates ("50%") Rule and Suspension

In September 2025, BIS issued the Affiliates Rule, extending export restrictions to any entity 50% or more owned (directly or indirectly, individually or in aggregate) by parties on the Entity List, Military End User List, or certain OFAC SDN programs. This rule mirrors OFAC's 50% Rule for sanctions, closing a loophole that allowed listed entities to route transactions through majority-owned subsidiaries. However, on November 10, 2025, BIS announced a one-year suspension of the Affiliates Rule as part of U.S.–China trade negotiations[21]. The suspension runs through November 9, 2026, but BIS has confirmed the rule will likely return unless extended or repealed. Companies should use this period to map ownership structures and prepare compliance programs for reinstatement.

i. Russia

[21] BIS Affiliates Rule Suspension – Federal Register

Following continued hostilities in Ukraine, BIS tightened controls on items that could support Russia's military-industrial base. New rules restricted exports of industrial software, advanced machine tools, and aerospace components. BIS also imposed foreign direct product restrictions on companies supplying Russia through third countries.

ii. Iran

In February 2025, BIS implemented measures under NSPM2 to restrict exports of dual-use items that could enhance Iran's missile and drone capabilities. This included revoking certain license exceptions and adding Iranian procurement networks to the Entity List.

3. Recent Enforcement Actions

Export control enforcement spans industries from technology to logistics. Two notable cases:

1. Cadence Design Systems Settlement (July 2025)

Cadence agreed to pay $95 million in civil penalties to BIS and nearly $118 million in criminal penalties under a DOJ plea agreement, totaling over $140 million, for knowingly exporting Electronic Design Automation (EDA) software and semiconductor design technology to Chinese military end-users, including the National University of Defense Technology (NUDT). The violations involved 56 unauthorized exports valued at $45 million and deliberate concealment of links to Entity List parties[22].

2. AI Chip Diversion Arrests (November 2025)

Four individuals (two U.S. citizens and two Chinese nationals) were arrested for conspiring to illegally export Nvidia A100 GPUs and other advanced AI chips to China via Malaysia and Thailand. The scheme involved falsified paperwork, shell companies, and $3.9 million in wire transfers. Charges include conspiracy to violate the Export Control Reform Act and money laundering, each carrying up to 20 years in prison[23].

[22] Cadence Settlement Press Release – Department of Justice
[23] AI Chip Diversion Press Release – Department of Justice

IV. From an EU Perspective

A. Differences/ considerations in sanctions

1. Adoption and legal framework of EU sanctions

Sanctions constitute a central instrument of the European Union's Common Foreign and Security Policy (CFSP). Their primary purpose is not punitive, but corrective: they are designed to influence the conduct or policies of targeted states, entities, or individuals in line with the EU's foreign policy objectives.[24]

In this context, the EU systematically implements sanctions adopted by the United Nations Security Council by transposing them into EU law. In many cases, it goes further by reinforcing UN sanctions through additional or more stringent restrictive measures.[25]

Beyond UN-mandated sanctions, the EU also retains the ability to adopt restrictive measures autonomously.[26] These sanctions are established through Council decisions adopted under the CFSP framework, following a proposal by the High Representative of the Union for Foreign Affairs and Security Policy. The proposed measures are examined by several preparatory bodies within the Council, including regional working groups, the Group of Advisers on External Relations, the Political and Security Committee where appropriate, and ultimately the Permanent Representatives Committee (Coreper II). The adoption of sanctions requires unanimity among Member States.

When sanctions include economic or financial measures such as asset freezes or restrictions on financial transactions they must be implemented through a Council regulation, which ensures their direct applicability within the EU legal order. Once published in the Official Journal of the European Union, these measures become binding across the EU and apply not only within EU territory, but also to EU nationals worldwide, EU-incorporated companies, and vessels or aircraft under Member State jurisdiction.

EU sanctions are subject to continuous review to ensure that they remain proportionate and effective. Listed individuals and entities have access to procedural safeguards, including the right to request a review of their listing by the Council and to challenge the legality of the measures before the General Court of the European Union.[27]

2. Scope and targets of EU sanctions[28]

---

[24] https://www.consilium.europa.eu/fr/policies/why-sanctions/

[25] https://www.consilium.europa.eu/fr/policies/sanctions-different-types/

[26] https://www.consilium.europa.eu/fr/policies/sanctions-adoption-review-procedure/

[27] https://www.consilium.europa.eu/fr/policies/sanctions-adoption-review-procedure/; The challenge of legality will be done under the conditions laid down in the second paragraph of Article 275 and the fourth and sixth paragraphs of Article 263 of the Treaty on the Functioning of the European Union.

[28] https://www.consilium.europa.eu/fr/policies/sanctions-different-types/

EU sanctions can be aimed at a wide range of actors including governments of non-EU countries, entities providing the means to carry out targeted policies, group or organizations such as terrorist groups and individuals.

Individuals and entities subject to sanction shall be informed of the measures taken against them either personally by mail if their address is known or by means of a notice published by the Council in the C series of the Official Journal of the European Union.

To keep track the EU continuously publishes a list to keep track of the latest EU sanctions: https://data.europa.eu/apps/eusanctionstracker/

3. Best practices in sanctions' implementation

Recognizing the complexity of sanctions enforcement, the EU published an updated set of "Best Practices" in July 2024.[29] These guidelines aim to promote consistency and effectiveness in the implementation of sanctions across Member States. They are intended for national authorities, financial institutions, and other stakeholders involved in sanctions compliance.

The Best Practices provide detailed operational guidance on key issues such as the identification and designation of sanctioned persons, the handling of cases of mistaken identity, and procedures for de-listing requests. They also address the practical management of financial restrictions, including asset freezes, and clarify the administrative and legal responsibilities of national authorities.

4. Recent developments

i. Russia[30]

, The EU has adopted an unprecedented number of restrictive measures since Russia's invasion of Ukraine on February 24, 2022, building on sanctions already imposed following the annexation of Crimea in 2014. These measures encompass economic and financial sanctions, individual listings, diplomatic restrictions, and visa measures.[31]

On October 23, 2025, the European Union adopted a 19th package of sanctions against Russia.[32]

These include measures in the energy sector such as a ban on the purchase, import and transfer directly or indirectly of Russian LNG, a tightening of restrictions against Rosneft and Gazpromneft, the designation in Annex XLII of 117 ships in the ghost fleet, bringing the total number of ships sanctioned by the EU to 557 and a ban on providing reinsurance services to these vessels. 47 new entities have been listed as prohibited to have transactions related to dual-sue items.

[29] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/fr/pdf

[30] https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/russie-en-lien-avec-la-violation-par-la-russie-de-la-souverainete-et-de-l-integrite-territoriale-de-l-ukraine

[31] https://www.consilium.europa.eu/fr/policies/sanctions-against-russia-explained/

[32] https://ec.europa.eu/commission/presscorner/detail/fr/ip_25_2491

There has also been an extension of the existing export ban on products such as metals, oxides and alloys used in the manufacture of military systems as well as an extension of the existing Import Ban to all acyclic hydrocarbons.

ii. Iran[33]

The Joint Comprehensive Plan of Action (JCPOA), adopted on July 14, 2016, established a framework under which a significant number of UN sanctions against Iran were suspended in return for commitments to guarantee the peaceful nature of Iran's nuclear programme[34]. On this basis, the European Union, through Regulation 2015/1861 of 18 October 2015, which entered into force on 16 January 2016, lifted the economic sanctions then in place against Iran relating to its nuclear programme.

On September 29, 2025, the UN sanctions against Iran for its nuclear program were reinstated according to the "snapback" procedure that was provided by the JCPOA after France, Germany and the United Kingdom formally notified the UN Security Council of Iran's failure to comply with its obligations towards the International Atomic Energy Agency. Under the snapback procedure, this notification triggered a 30-day consultation period aimed at reaching a diplomatic resolution.

During this period, the UN Security Council had to vote if necessary on the continuation the period of suspension of sanctions. In the absence of a vote, the suspension of UN sanctions against Iran for its nuclear programme was to end automatically.

It is in this context that on August 28, 2025, France, Germany and Great Britain, in a joint letter addressed to the President of the UN Security Council, hat they considered Iran to be in serious breach of the JCPOA and confirmed their decision to initiate the snapback process. No agreement was found.

On this basis the European Union, by Regulation 2025/1975 reactivated the sanctions which had been lifted in 2015.

5. The difficulty of articulation between EU and US sanctions

i. The EU blocking statute and extraterritorial sanctions[35]

A recurring challenge for European citizens and businesses arises from the extraterritorial application of unilateral sanctions from third countries, such as the United States. The EU considers that such extraterritorial application is contrary to international law and has adopted Regulation 2271/96, better known as the "blocking statute", to protect EU citizens and companies from their effect. Since 2018, the Blocking Statute has applied notably to US sanctions against Iran and Cuba.

[33] https://www.consilium.europa.eu/fr/policies/sanctions-against-iran/
[34] Resolution 2231 (2015) of July 20, 2015
[35] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021DC0535

The regulation prohibits European actors from complying with certain foreign sanctions and limits cooperation with the authorities or courts of the third country in question in the application of such sanctions.

The regulation also provides for a compensation mechanism if they are convicted in the third country and allows under strict conditions for the European Commission to authorize compliance.

ii. Practical illustration

These tensions were the basis of one of our own case. It was an an action for annulment of a €34 million international arbitral award arising from a dispute between a French company and a Middle Eastern quais-public entity. The dispute raised complex issues concerning the interaction between the EU, UN and US sanctions.

The contract had been terminated after the opposing party was allegedly unable to obtain bank guarantees denominated in US dollars, as no bank was willing to issue such guarantees for the Middle Eastern country concerned. The arbitral tribunal dismissed the claimant's claims, prompting the latter to seek annulment of the award before the Paris Court of Appeal.

The claimant argued that US, UN and EU sanctions against Iran imposed embargoes and prohibited dollar-denominated transactions, making performance of the contract impossible. It claimed that these sanctions, as mandatory rules forming part of international public policy, had been ignored by the arbitral tribunal, rendering the award contrary to French international public policy.

The core issue was therefore the applicability of EU, UN and US sanctions to the arbitral award, a legally complex matter given the scarcity of case law at the time and the overlapping nature of the sanctions.

The client countered that no breach of EU sanctions was established, that UN Security Council resolutions have no direct effect in France without EU or national implementation, and that US sanctions were inapplicable, as US law could not be considered part of international public policy in this case.

French courts ultimately held that US sanctions did not form part of French international public policy and that the arbitral award did not violate applicable international sanctions regimes. The courts emphasized the importance of assessing sanctions in light of their temporal and material scope, concluding that neither EU nor UN sanctions were applicable to the underlying contract. This decision was confirmed by the *Cour de Cassation*.

B. Differences/ considerations in export controls

1. Purpose and scope

The EU sanctions regime and the EU framework governing dual-use export controls framework constitute two distinct policy instruments. They differ in their legal

foundation, objectives and decision-making processes, even-though they pursue complementary foreign and security policy goals.

The European Union regulates the export of dual-use items, namely goods, software and technologies that can be employed both for civilian and military purposes. The objective of these controls is to mitigate the risks associated with the diversion of sensitive technologies for military build-up, terrorism, or the proliferation of weapons of mass destruction, while presenting the free-flow of civilian trade.

EU law adopts a broad definition of dual-use items which encompass not only tangible goods but also intangible elements such as software, technology, brokering services and technical assistance.

2. Legal Basis[36]

The EU export control framework is governed by Regulation (EU) 2021/821, which has been in force since 9 September 2021. Adopted on the basis of Article 207 of the Treaty on the Functioning of the European Union. It replaced Regulation (EC) No 428/2009 in order to modernize the existing framework and take into account evolving security risks, rapid technological innovation and changes in global trade patterns.

The regulation aims to strengthen cooperation between Member States, guidance given to exporters and introduces controls regarding cybersurveillance technologies.

Annex I to Regulation (EU) 2021/821, lists more than 1,800 dual-use items requiring export authorization[37]. The list is structured into ten categories, including nuclear materials, linked special materials, material treatments, electronics, calculators, telecommunications, sensors and lasers, navigation and avionics, marine technologies, and aerospace and propulsion systems.

Annex I is based on internationally agreed control lists derived from multilateral export control regimes such as the Wassenaar Arrangement, the Nuclear Suppliers Group and the Missile Technology Control Regime.

To take into account changes agreed in 2024 under these texts, the regulation was updated on September 8, 2025,[38] by Commission Delegated Regulation (EU) 2025/2003. These changes address controls related among else to quantum technology, semiconductor manufacturing and testing equipment and advanced computing integrated circuits, coating for high-temperature applications, additive manufacturing machines, peptide synthetisers.

[36] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821
[37] https://circabc.europa.eu/ui/group/654251c7-f897-4098-afc3-6eb39477797e/library/19eee88d-8b29-40a0-9e02-a662ecafaf6e/details?download=true
[38] https://eur-lex.europa.eu/eli/reg_del/2025/2003/oj/eng

3. Licensing

Regulation (EU) 2021/821 establishes several types of export authorizations such as EU General Export Authorizations (EUGEAs), National General Export Authorizations, individual licenses, global licenses (delivered by national authorities) and authorizations for large-scale projects.

An authorization may also be required for the export of dual-use items not listed in Annex I if the exporter has been informed by the competent authority that the items in question are or may be intended, in their entirety or in part to biological weapons, military use in countries in which a weapons embargo has been imposed, components of military goods already exported in member state of the EU without the necessary approval.

Exporters seeking authorization are required to submit detailed information relating to the goods concerned, the country of destination, the end-user and the intended end-use. They must also comply with post-licensing obligations, notably the maintenance of detailed export records for a minimum period of five years.

In assessing license applications, Member States are required to consider a range of factors, including the EU's international commitments, applicable EU and UN sanctions, foreign and security policy considerations, and the risk of diversion to unauthorized end-users or uses.

C. An EU Practitioner's Perspective: Sanctions in Practice and Lessons from Complex Advisory Matters

From an EU perspective, sanctions compliance is rarely an abstract exercise. In my experience advising financial institutions and corporates, EU sanctions issues most often arise in situations where long-standing commercial arrangements collide with rapidly evolving geopolitical measures, and where the legal framework leaves little room for purely mechanical answers. The EU regime is built on broad prohibitions, functional concepts, and decentralized enforcement, which together create a compliance environment that requires careful legal judgment, early engagement with authorities, and a clear understanding of how economic value is assessed in practice.

Two advisory matters illustrate recurring themes that continue to shape EU sanctions risk: one involving independent bank guarantees linked to Syria-related sanctions, and another involving commercial operations affected by the EU's Ukraine restrictive measures. While fact-specific, both matters reveal structural characteristics of EU sanctions that remain highly relevant today.

1. Economic Reality Over Legal Form

One of the most consistent lessons from EU sanctions advisory work is that the regime focuses on economic reality rather than contractual form. EU regulations prohibit not only the transfer of funds, but also the making available of "economic resources,"

directly or indirectly, to designated persons or entities. In practice, this means that instruments which may appear contingent, technical, or administrative can nonetheless fall squarely within the scope of prohibitions if they preserve or enable economic benefit.

This issue arose acutely in the Syria-related advisory matter involving independent bank guarantees issued in support of obligations ultimately benefiting a sanctioned Syrian refinery and a designated Syrian bank. Although the guarantees themselves were contingent and payment had not yet occurred, their renewal was assessed as likely constituting the making available of funds or economic resources under EU law, because the guarantees maintained economic value for designated entities and could be drawn upon to obtain financial benefit. The legal analysis did not turn on whether funds moved immediately, but on whether the arrangement kept value within reach of a sanctioned party.

This approach is consistent with the jurisprudence of the Court of Justice of the European Union, which has repeatedly emphasized that the purpose of EU restrictive measures is to deny access to economic resources in a broad and preventive sense. For clients, the practical implication is that instruments such as guarantees, counter-guarantees, letters of credit, or similar commitments cannot be treated as neutral simply because they are indirect or contingent. If they enable economic enjoyment, they attract sanctions risk.

2. Indirect Benefit and the Limits of Structural Distance

A second recurring challenge in EU sanctions compliance is the concept of indirect benefit. EU regulations expressly prohibit making funds or economic resources available "directly or indirectly," a formulation that is intentionally expansive. In practice, this often undermines assumptions that distance in the contractual chain provides insulation from sanctions exposure.

In the Crimea-related advisory matter concerning trans-shipment operations through the port of Feodosia, the client did not have a direct contractual relationship with the designated entity operating the terminal. Instead, services were provided through an intermediary service provider. Nonetheless, the analysis focused on whether payments made under upstream contracts could ultimately benefit a designated entity, and whether goods stored or handled through the terminal could be considered economic resources "held or controlled" by that entity within the meaning of EU law

The absence of a direct contractual link did not resolve the issue. What mattered was whether value flowed, even indirectly, to a listed entity. This required a granular assessment of contractual rights, control over goods, and the practical ability of the designated entity to dispose of or benefit from the assets in question. For clients, this illustrates that EU sanctions risk must be assessed across the entire economic chain, not merely at the level of immediate counterparties.

3. Pre-Existing Contracts and the Narrow Scope of Derogations

Clients frequently assume that pre-sanctions contracts are insulated from later restrictive measures. In the EU context, that assumption is rarely safe. While EU

regulations contain derogations for obligations arising from contracts concluded before designation, these exceptions are narrowly framed, conditional, and often subject to authorisation by national competent authorities.

In both advisory matters, pre-existing contractual arrangements played a central role. In the Crimea-related case, continued performance was potentially permissible only to the extent that payments qualified as amounts "due" under contracts concluded prior to designation, and even then, confirmation from competent authorities was strongly recommended to mitigate enforcement risk.

Similarly, in the Syria guarantees matter, the fact that guarantees had been issued before the full expansion of the sanctions regime did not justify their renewal or modification without regulatory clearance.

The key lesson is that grandfathering under EU sanctions is not automatic. Each derogation must be analysed against the precise wording of the regulation, and clients must be prepared to demonstrate strict compliance with its conditions. Where ambiguity exists, reliance on informal assumptions rather than formal authorisation materially increases risk.

4. The Central Role of National Competent Authorities

Unlike more centralized sanctions regimes, EU sanctions are implemented and enforced primarily at the Member State level. National competent authorities play a critical role not only in granting authorizations, but also in shaping the practical application of restrictive measures.

In both matters, early engagement with competent authorities was a central component of risk management. Seeking guidance or confirmation did not merely clarify the legal position; it also provided a documented basis for good-faith compliance. EU law explicitly recognizes that actions taken in good faith, without knowledge or reasonable cause to suspect a breach, can mitigate or eliminate liability. However, that protection is far more robust when the client has proactively engaged with regulators rather than acted unilaterally.

From a practical standpoint, silence or delay tends to increase exposure. Documented interaction with authorities, even where the answer is restrictive, often provides the safest path forward in legally sensitive situations.

5. Sanctions Risk Beyond Compliance: Contractual and Operational Consequences

Finally, EU sanctions issues rarely remain confined to regulatory analysis. They frequently cascade into contractual disputes, operational disruptions, and broader risk considerations. In the Crimea-related matter, the potential freezing of assets and disruption of services raised force majeure questions under downstream contracts and exposed the client to claims for non-performance. In the Syria guarantees matter, sanctions compliance decisions had to be weighed against potential contractual liability, reputational risk, and banking licence exposure.

These experiences underscore that effective EU sanctions advice must be multidisciplinary. Legal analysis of restrictive measures must be integrated with

contract management, operational planning, and governance decisions. Treating sanctions as a purely compliance-driven issue, isolated from the business context, often leads to incomplete risk assessment.

6. Concluding Observations

From an EU advisory perspective, sanctions compliance is defined by breadth, ambiguity, and practical judgment. The recurring themes across complex matters are clear: EU sanctions prioritize substance over form, capture indirect economic benefit, constrain reliance on pre-existing contracts, and place significant emphasis on engagement with national authorities. For decision-makers, the challenge is not merely to identify prohibitions, but to understand how economic value is perceived and regulated under EU law.

As EU sanctions continue to expand in scope and sophistication, these practical lessons remain highly relevant. Sanctions are no longer peripheral regulatory constraints; they are core governance and risk issues, requiring informed judgment and early, structured engagement to manage effectively.

V. Practical (how this impacts companies)

A. Managing global operations (Preventing a violation)

The larger and more geographically diverse a company is, the harder it is to protect from sanctions and export controls exposure, but companies can take steps now to protect themselves.

A well designed risk or threat assessment can help identify vulnerabilities that may require additional attention, such as training and controls testing. Areas such as third party oversight and merger and acquisition processes may be higher risk and require more resources. Additionally geographies or business lines exposed to greater sanctions or export control risks, or with significantly divergent laws will likely require the strongest controls to ensure the U.S. is ringfenced from any exposure.

Depending on volumes of customers, transactions, third parties, deals, or other events that need to be reviewed, manual processing may not be enough to manage case volume or identify patterns of activity that would indicate a potential issue.

Testing and assurance processes are critical to make sure that what you think is happening in your compliance and risk management program actually is.

Finally a note about the Board and senior leadership. They have an obligation to oversee risk management for the company. They are depending on the control functions to give them the information they need to discharge those responsibilities. Key risk indicators and both quantitative and qualitative reporting to those with decision making authority on a regular cadence is critical.

B. Disclosures and Reporting

1. Evaluation of Corporate Compliance Programs[39]

The Department of Justice distributed guidance that details the criteria it considers when determining whether to bring an action against a company. The criteria are based on both the compliance program the company had in place at the time the event took place, as well as the culture of compliance and the actions taken once misconduct was identified.

The guidance includes:

a. *Whether the corporation's compliance program was well designed* – including whether it is based on a risk assessment, policies and procedures, training and communications, and an anonymous or confidential reporting and investigations process, whether it provides for due diligence in critical areas such as third party relationships and mergers and acquisitions.
b. *Whether the corporation's compliance program was adequately resourced and empowered to function effectively* – including a commitment by both senior and middle management, second line of defense resources have autonomy and functions are adequately staffed, and whether compensation and incentives align to a culture of compliance.
c. *Whether the compliance program works in practice* – including ongoing testing and review, that the investigation process is responsive and well scoped, and that there is a thorough analysis of any misconduct to enhance the program as necessary.

2. OFAC Enforcement Guidance[40]

Like DOJ, OFAC also considers the company's actions when determining enforcement penalties. Among other things, OFAC considers whether the company had a compliance program aligned to OFAC's guidance, if the violation was self-disclosed, if it was egregious or represented a pattern of activity, and the timing of the violation in relation to the imposition of sanctions. Further, OFAC looks at whether the company cooperated with OFAC during its investigation of the violation, and what remedial measures were taken once the violative conduct was identified.

[39] https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl
[40] eCFR :: Appendix A to Part 501, Title 31 -- Economic Sanctions Enforcement Guidelines.