BEALE&CO

Staying Compliant

A Guide to Sanctions Law

November 2025

Contents

Purpose

In today's globalised business environment, compliance with financial sanctions has become increasingly crucial. Financial sanctions are powerful tools used by governments and international organisations to maintain international peace and security, prevent terrorism, and curb the influence of rogue states or individuals. This guide is designed to provide an accessible overview of the UK's financial sanctions regime, helping businesses understand their obligations, the risks of non-compliance, and how to ensure they operate within the law.

We have found that there is often a challenge in identifying when a particular scenario gives rise to potential issues related to sanctions. For example, there may be a prohibition on providing certain goods or services to persons connected to a particular jurisdiction. That prohibition may be engaged in situations where the person in question does not possess the nationality of that state or is not physically living in the jurisdiction concerned.

This means that businesses need to be diligent in ensuring that their activities do not infringe the rules. By providing a clear, step-by-step overview of how financial sanctions work, we aim to equip companies with the knowledge they need to navigate this complex regulatory landscape, particularly as it applies to entities engaging in cross-border trade, financial services, or dealing with designated persons and jurisdictions.

It is important to emphasise that the law of economic sanctions is fluid and dynamic with changes frequently being made. This guide is not intended to be the last word on the matter, nor to serve as legal advice.

The law is stated as of October 2025.

Paul Henty
Partner

Introduction

OVERVIEW OF ECONOMIC SANCTIONS

Financial sanctions are legal restrictions imposed by governments or international bodies such as the United Nations (UN), European Union (EU), and United Kingdom (UK) to limit or prohibit financial dealings with certain countries, individuals, or entities. These sanctions are typically implemented in response to activities such as terrorism, human rights abuses, nuclear proliferation, or violations of international law. The scope of financial sanctions varies and can include measures such as:

- **Asset Freezes:** Preventing the movement or use of assets owned or controlled by sanctioned individuals or entities.
- **Restrictions on Financial Services:** Limiting the ability of individuals or organisations to access financial services like banking, insurance, and loans.
- **Prohibitions on Making Funds Available:** Restricting businesses and individuals from providing funds or economic resources to persons subject to sanctions, or otherwise dealing in funds or economic resources on their behalf (e.g. accepting payments from a designated person).

These measures are intended to apply economic pressure on specific targets to compel them to change their behaviour or restrict their ability to carry out harmful activities.

In the UK, most sanctions measures are adopted pursuant to the Sanctions and Anti-Money Laundering Act 2019. UK measures which implement UN sanctions are typically adopted pursuant to Section 1 of the United Nations Act 1946.

The obligation to comply with UK sanctions measures extends to all UK persons and entities, including UK nationals overseas.

TYPES OF SANCTIONS

There are broadly two types of sanctions measures: financial sanctions (discussed in Section 4) and trade sanctions (discussed in Section 5).

Whereas financial sanctions are targeted against specific individuals connected with a government or regime involved in wrongdoing, trade sanctions aim to penalise a state by restricting its ability to import and/or export specified goods or services.

In the UK, the primary body responsible for enforcing financial sanctions is the Office of Financial Sanctions Implementation (OFSI), which operates under HM Treasury. OFSI enforces sanctions that include:

- **Country-based Sanctions:** For example, sanctions against Russia due to its invasion of Ukraine.
- **Thematic Sanctions:** These may target terrorists, narcotics traffickers, or those involved in serious human rights violations.
- **Sectoral Sanctions:** Often targeted at specific sectors of the economy, such as oil, gas, and defence, in sanctioned countries.

This guide aims to help you understand the different types of sanctions, how to identify whether your business is affected, and the steps you need to take to comply with them. Sanctions are not just limited to direct transactions; they also extend to third-party dealings with sanctioned individuals or countries, making compliance a crucial consideration for many businesses.

By the end of this guide, you should have a solid understanding of how to identify sanctions risks, manage compliance effectively, and mitigate the potential consequences of breaching financial sanctions regulations.

Key Enforcement Bodies

OFFICE OF FINANCIAL SANCTIONS IMPLEMENTATION (OFSI)

The Office of Financial Sanctions Implementation (OFSI), part of HM Treasury, is the UK's primary body responsible for enforcing financial sanctions. OFSI plays a critical role in ensuring that businesses, financial institutions, and individuals comply with financial sanctions in the UK. OFSI has a broad mandate, including:

- **Administering Financial Sanctions:** OFSI manages the implementation of sanctions across various sectors and works to ensure that businesses understand their obligations.
- **Issuing Guidance:** It provides detailed guidance and updates on how financial sanctions apply to specific scenarios, helping businesses navigate complex regulations.
- **Enforcing Penalties:** OFSI has the power to impose civil monetary penalties on entities that breach financial sanctions, even on a strict liability basis. This means that the intention behind a breach is irrelevant; if a breach occurs, OFSI can issue fines.
- **Licensing:** In cases where transactions or services might otherwise breach sanctions, OFSI issues licenses that permit those activities under specific conditions. For example, it can issue licenses for humanitarian aid or legal services.
- **Maintaining the Consolidated List:** OFSI regularly updates the Consolidated List of designated persons and entities that are subject to sanctions, ensuring businesses can check whether they are dealing with a sanctioned entity.

ROLE OF OFSI IN PRACTICE

If your business engages in financial transactions, you must ensure that none of the parties involved are listed on OFSI's Consolidated List. Regularly screening customers and clients against this list is a necessary compliance step. OFSI's penalties for breaches can be substantial, up to £1 million or 50% of the breach's value.

OFFICE OF TRADE SANCTIONS IMPLEMENTATION (OTSI)

The Office of Trade Sanctions Implementation (OTSI) was introduced in 2024 to handle trade-related sanctions, primarily focusing on trade, shipping, and aviation sectors. While OFSI handles financial sanctions, OTSI's remit includes:

- **Civil Enforcement of Trade Sanctions:** OTSI has the power to impose civil penalties on companies that breach trade sanctions. Like OFSI, these penalties can be issued on a strict liability basis, meaning companies can face fines even if they were unaware of the breach.
- **Reporting Obligations:** OTSI requires companies to report any knowledge or suspicion of a breach of trade sanctions. Non-compliance with reporting requirements can lead to criminal liability.
- **Sector-Specific Focus:** OTSI handles sanctions affecting particular sectors such as shipping, aviation, and trade in goods, which often have complex and specific regulations.
- **Collaboration with HMRC:** While OTSI is responsible for civil enforcement, criminal enforcement of trade sanctions remains with HMRC for trade-related sanctions and the National Crime Agency (NCA) for shipping and aviation sanctions.

HM REVENUE & CUSTOMS (HMRC)

HMRC plays a critical role in the criminal enforcement of sanctions, especially when breaches involve trade sanctions, including those related to military goods, dual-use technologies, or goods subject to strategic export controls. HMRC investigates and prosecutes violations of trade sanctions, particularly those involving exports that could compromise national or international security.

For businesses involved in international trade, it's crucial to be aware of export controls and the role of HMRC in enforcing them. HMRC often collaborates with OTSI and OFSI to ensure that sanctions are effectively enforced across both civil and criminal domains.

DEPARTMENT FOR BUSINESS AND TRADE (FORMERLY BIS)

The Department for Business and Trade also plays an important role in enforcing sanctions, particularly through the Export Control Joint Unit (ECJU), which manages export licenses for controlled goods and technologies in accordance with the Export Control Order 2008. ECJU ensures that businesses comply with UK sanctions when exporting items that could potentially contribute to military or strategic threats in sanctioned countries.

ECJU is crucial for businesses that export military or dual-use goods, as failure to obtain the correct licenses can result in severe penalties, including imprisonment. The department also has enforcement responsibility for maritime transport sanctions, particularly involving the transport of oil and oil products.

COLLABORATIVE ENFORCEMENT

Sanctions enforcement is a collaborative effort between OFSI, OTSI, HMRC, and the Department for Business and Trade, ensuring that both financial and trade sanctions are comprehensively applied. Each body has its own remit, but they work together to ensure that businesses in the UK comply with sanctions, whether they relate to financial transactions, trade, or the provision of services.

By understanding the roles of these bodies, businesses can better navigate the sanctions regime and avoid the serious consequences of non-compliance.

UK SANCTIONS REGIMES CURRENTLY IN FORCE

By "sanctions regime", we refer to sets of sanctions rules targeted against particular states. In nearly all cases, the UK Government has introduced sets of regulations under the Sanctions and Anti-Money Laundering Act 2019. Arms embargoes have been introduced under the Export Control Order 2008.

As at October 2025, the UK has the following regimes in force:

COUNTRY/TERRITORY	CORRESPONDING REGULATIONS
Afghanistan	Afghanistan (Sanctions) (EU Exit) Regulations 2019
Armenia (arms embargo only)	Export Control Order 2008 (Schedule 4, Part 1)
Azerbaijan (arms embargo only)	Export Control Order 2008 (Schedule 4, Part 1)
Belarus	Republic of Belarus (Sanctions) (EU Exit) Regulations 2019
Bosnia and Herzegovina	Bosnia and Herzegovina (Sanctions) (EU Exit) Regulations 2020
Central African Republic	Central African Republic (Sanctions) (EU Exit) Regulations 2020
China (mainland) and Hong Kong (arms embargo only)	Export Control Order 2008 (Schedule 4, Part 1)
Democratic People's Republic of Korea (North Korea)	Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019
Democratic Republic of the Congo	Democratic Republic of the Congo (Sanctions) (EU Exit) Regulations 2021
Guinea	Guinea (Sanctions) (EU Exit) Regulations 2019
Guinea-Bissau	Guinea-Bissau (Sanctions) (EU Exit) Regulations 2019
Haiti	Haiti (Sanctions) (EU Exit) Regulations 2022
Iran	Iran (Sanctions) (Nuclear) (EU Exit) Regulations 2019 and Iran (Sanctions) (Human Rights) (EU Exit) Regulations 2019
Iraq	Iraq (Sanctions) (EU Exit) Regulations 2020
Lebanon	Lebanon (Sanctions) (EU Exit) Regulations 2019 and Lebanon (Sanctions) (Assassination of Rafiq Hariri and Others) (EU Exit) Regulations 2019
Libya	Libya (Sanctions) (EU Exit) Regulations 2020
Mali	Mali (Sanctions) (EU Exit) Regulations 2019
Myanmar	Myanmar (Sanctions) (EU Exit) Regulations 2019
Nicaragua	Nicaragua (Sanctions) (EU Exit) Regulations 2020
Russia	Russia (Sanctions) (EU Exit) Regulations 2019 (as heavily amended)
Somalia	Somalia (Sanctions) (EU Exit) Regulations 2021
South Sudan	South Sudan (Sanctions) (EU Exit) Regulations 2021
Sudan	Sudan (Sanctions) (EU Exit) Regulations 2020

COUNTRY/TERRITORY	CORRESPONDING REGULATIONS
Syria	Syria (Sanctions) (EU Exit) Regulations 2019 and Syria (Sanctions) (Cultural Property) (EU Exit) Regulations 2020
Venezuela	Venezuela (Sanctions) (EU Exit) Regulations 2019
Yemen	Yemen (Sanctions) (EU Exit) Regulations 2020
Zimbabwe	Zimbabwe (Sanctions) (EU Exit) Regulations 2019

The UK also has in force several thematic sanctions regimes, which aim to prevent certain types of criminal activity on an international scale. Those in force as at October 2025 are set out below:

THEME	CORRESPONDING REGULATIONS
Chemical Weapons	Chemical Weapons (Sanctions) (EU Exit) Regulations 2019
Counter-Terrorism	Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019
Counter-Terrorism (International)	Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019
Cyber	Cyber (Sanctions) (EU Exit) Regulations 2020
Global Anti-Corruption	Global Anti-Corruption Sanctions Regulations 2021
Global Human Rights	Global Human Rights Sanctions Regulations 2020
Global Irregular Migration and Trafficking in Persons	Global Irregular Migration and Trafficking in Persons (Sanctions) Regulations 2023
ISIL (Da'esh) and Al-Qaida	ISIL (Da'esh) and Al-Qaida (Sanctions) (EU Exit) Regulations 2019
Unauthorised Drilling Activities	Unauthorised Drilling Activities in the Eastern Mediterranean (Sanctions) (EU Exit) Regulations 2020

Understanding Financial Sanctions

FINANCIAL SANCTIONS - WHO IS A "DESIGNATED PERSON"?

Sanctions are generally targeted towards a state which is involved in actions considered to offend human rights or the international legal order. Financial sanctions are restrictions imposed specifically against individuals or organisations who are considered to be closely connected to that state, generally restraining their ability to access or use assets or funds within the jurisdiction which has imposed the sanctions. Other restrictions imposed on particular individuals or entities may not be, strictly speaking, of a financial nature.

The relevant Secretary of State is empowered under sanctions legislation to identify persons or entities against whom sanctions measures are to be applied (referred to as designated persons). The list will often include the Ministries of the Government of the country concerned, the Ministers and senior offices of that Government and other public officials involved in wrongdoing (e.g. Iranian scientists working on the nuclear proliferation program or the Russian judicial officials involved in the detention and inhumane treatment of Sergei Magnitsky).

Prominent businesses and businesspersons and family members of Government officials will also frequently find themselves targeted – which has previously led to fiercely fought legal challenges. Bank Mellat successfully contested its designation in connection with the EU's Iranian sanctions regime, arguing that it had no connection with the nuclear program those sanctions sought to target.

It is important to note that where a person or entity is designated, any entity under the direct or indirect control of that person is also subject to prohibitions. Superficially, the trigger point is ownership of 51% or more of the shares in the relevant entity (see Regulation 7 of the Russia (Sanctions) (EU Exit) Regulations 2019).

Working out whether or not an entity is under their ownership or control can be complicated. Other shareholders may be expected to act under the instructions of the designated person (e.g. employees or family members). That factor should be considered before concluding that the designated person does not exercise control over the entity. Other relationships may be obscured by complex offshore structures.

It is also important to note that for compliance purposes, a UK person has an obligation not to deal as soon as there is "reasonable cause to suspect" that the other party may be a designated person. This is a lower bar than actual knowledge and may be met where certain red flags are present.

TYPES OF FINANCIAL SANCTIONS

Financial sanctions encompass a variety of restrictions that governments and international bodies use to influence behaviour, protect national security, and uphold international law.

The types of sanctions that businesses need to understand include:

1. **Asset Freezes:** One of the most common forms of financial sanctions. An asset freeze prevents individuals or entities from accessing or using their financial assets. Businesses must ensure that they do not deal with or transfer any assets belonging to a sanctioned person or entity. For example, if a company has funds held by a UK bank that belongs to a sanctioned individual, those funds will be frozen, and the company cannot make any transactions involving them.
2. **Prohibition on Financial Services:** This form of sanction restricts the ability of businesses to provide or receive financial services from designated persons or entities. It could involve limits on banking, insurance, or any type of financial support that might indirectly benefit a sanctioned individual or country.
3. **Prohibitions on Making Funds Available:** In addition to prohibiting transactions with sanctioned entities, financial sanctions often extend to restrictions on making any kind of funds available to or receiving funds from them. Dealing with funds belonging to a designated person is also prohibited. This is designed to ensure that sanctioned individuals or entities cannot gain access to financial support through indirect means, such as third-party arrangements.
4. **Prohibitions on Making Economic Resources Available:** Beyond funds, it is also prohibited to provide economic resources to or receive economic resources from a designated person, or otherwise deal in such resources belonging to a designated person. The definition of economic resources is broad and engenders anything of value which could be exchanged for funds. This can include tangible (e.g. property) and intangible property (e.g. intellectual property) and assets.
5. **Travel Bans:** States commonly ban designated persons from entering their territory. For example, after Russia imposed a travel ban on the late US Senator John McCain, he sarcastically quipped: "*There goes my beach holiday in Siberia!*"

Comparatively, trade sanctions are directed against states, restraining their ability to import and export goods and services. In more recent times, extensive trade sanctions have been imposed on Russia and Belarus in response to Russia's invasion of Ukraine in 2022.

Financial sanctions measures are backed up by anti-circumvention provisions which prohibit parties from putting in place arrangements to evade the prohibition (e.g. Regulation 19 of the Russia (Sanctions) (EU Exit) Regulations 2019, Regulation 16 of the Venezuela (Sanctions) (EU Exit) Regulations 2019).

WHO IS REQUIRED TO COMPLY WITH UK FINANCIAL SANCTIONS?

The rules in UK sanctions apply to UK nationals and businesses regardless of where they operate. This includes any business that:

- Operates within the UK.
- Engages in business with UK financial institutions or entities.
- Conducts transactions involving UK citizens, regardless of location.

Financial sanctions also apply to UK-registered companies operating internationally, meaning that a UK business must comply with sanctions even when trading overseas. Furthermore, non-UK businesses dealing with UK entities or assets in the UK are also subject to sanctions regulations.

It is important to emphasise that some jurisdictions are more aggressive in applying their sanctions rules to non-nationals, situated outside the jurisdiction. For example, the United States applies its sanctions on an 'extraterritorial' basis through the Office of Foreign Assets Control (OFAC). This means that even non-US companies and individuals can be exposed to liability if their activities involve US persons, US goods or technology, or US dollar transactions cleared through the US financial system. As a result, businesses with any US nexus must take particular care to assess not only UK and EU obligations, but also potential US exposure. In terms of the territorial application of sanctions rules, the approach of the European Union is closer to that of the UK. Both primarily bind persons and entities within their jurisdiction - that is, EU nationals, entities incorporated within the EU, and activities taking place on EU territory. Unlike the United States, the EU does not generally assert extraterritorial jurisdiction over non-EU persons who are wholly outside its territory, although EU sanctions may still catch foreign subsidiaries of EU companies, or dealings that have a sufficient nexus with the EU (such as payments routed through an EU bank). Switzerland adopts a similar approach, aligning closely with EU practice, and has historically implemented EU sanctions into Swiss law with limited modifications.

DUE DILIGENCE AND SCREENING OBLIGATIONS

To comply with financial sanctions, businesses must conduct thorough due diligence to identify whether they are dealing with designated persons or entities. This involves checking the OFSI Consolidated List, which contains the names of individuals, groups, and companies subject to financial sanctions. Businesses should implement regular screening procedures, especially in industries with higher exposure to international transactions.

- **Customer Due Diligence:** This process involves verifying the identity of customers and ensuring they are not listed as sanctioned entities.
- **Transaction Screening:** Ongoing screening is essential, as new individuals and entities can be added to sanctions lists at any time. Businesses must ensure their transactions do not breach sanctions regulations as lists are updated.
- **Supplier and Third-Party Screening:** Beyond direct customers, businesses should screen suppliers and third-party service providers to ensure they are not inadvertently facilitating transactions with sanctioned entities.

THIRD-PARTY RISKS

Financial sanctions are not limited to direct transactions with designated persons. They also apply to situations where businesses could indirectly benefit or provide support to sanctioned individuals or entities. For example, if a business's client is not listed on the sanctions list but is owned or controlled by a sanctioned person, dealing with that client could still violate financial sanctions laws.

This creates significant risks for businesses operating in high-risk jurisdictions or those with complex supply chains. Effective risk management requires businesses to not only know their immediate counterparties but also the broader ownership structures and control mechanisms that could expose them to sanctions risks.

By understanding these key concepts in financial sanctions compliance, businesses can protect themselves from the significant financial and reputational risks associated with non-compliance.

Key Concepts in Financial Sanctions Compliance

DESIGNATED PERSONS AND ENTITIES

At the heart of any financial sanctions regime are designated persons and entities: individuals, groups, or organisations that have been specifically identified as subject to restrictions due to their involvement in activities such as terrorism, human rights abuse, threat to international peace and security, or from their connection with a state involved in same.

These names are included in the OFSI Consolidated List, which is regularly updated to reflect new additions and removals. Businesses must ensure they are familiar with this list and have processes in place to screen clients, suppliers, and partners.

The Consolidated List includes individuals and entities targeted by the UK, as well as those covered under UN, EU, and US sanctions regimes where applicable. This list spans across multiple sectors, and failing to account for these designations can lead to significant penalties for non-compliance.

In the UK, designated persons may challenge their designation under section 23 SAMLA 2018 by request for review and, if necessary, by appeal to the High Court (or Court of Session in Scotland). Any proceedings must be commenced as a judicial review on the basis of one or more public law grounds (e.g. illegality, irrationality or procedural impropriety). For example, an entity that has been listed may argue that it has no connection with a particular regime or conduct, or that it is being singled out for irrational or unfair treatment (see *Bank Mellat v HM Treasury* [2013] UKSC 39, [2014] AC 700, [2013] 3 WLR 179).

In other cases, claimants have successfully argued that certain sanctions Orders made by Ministers have gone beyond what can reasonably be considered "necessary or expedient" under the parent legislation. In *Ahmed and Others v HM Treasury* [2010] UKSC 2, the Court agreed that an Order which denied designated persons the right to effective judicial review of the measure would be *ultra vires*.

Human rights considerations are also important. Sanctions measures must not interfere disproportionately or unlawfully with the property rights of individuals, these being protected under Article 1, Protocol 1 of the European Convention on Human Rights. In *Bank Mellat v HM Treasury* [2015] EWHC 1258 (Comm)), Flaux J held that in such an event, a designated person may be entitled to damages under ss 7 and 8 of the Human Rights Act 1998, which could include loss of future profits provided that these losses had been caused by the unlawful action.

SANCTIONED JURISDICTIONS

In addition to specific persons and entities, financial sanctions also apply to entire jurisdictions - countries that are subject to sanctions due to activities such as nuclear proliferation, terrorism, or military aggression. Countries like Russia, North Korea, Iran, and Syria are currently subject to broad-based sanctions, affecting sectors like finance, energy, and defence.

Sanctions can vary in scope, with some targeting entire economies, while others may focus on specific sectors or industries. For example, sectoral sanctions on Russia target areas such as banking, energy, and defence, limiting investment and trade in those sectors without imposing a complete embargo.

For businesses operating internationally, it is crucial to understand which jurisdictions are subject to sanctions and the specific restrictions imposed. **Due diligence** is essential when dealing with entities or individuals from sanctioned countries, as even indirect dealings with these parties could expose a business to risk.

DUE DILIGENCE AND SCREENING

To ensure compliance with sanctions regulations, businesses are required to carry out due diligence procedures. This includes conducting comprehensive checks on clients, suppliers, and any third parties with which they engage. The purpose of due diligence is to ensure that businesses do not inadvertently violate sanctions by dealing with designated persons or sanctioned jurisdictions.

1. **Client Screening:** Regular screening of clients against the OFSI Consolidated List and any relevant international sanctions lists (such as OFAC's list for the US) is essential to ensure compliance. Businesses should use automated systems that screen clients in real-time, as sanctions lists are frequently updated.
2. **Transaction Monitoring:** Beyond initial client screening, businesses need to monitor transactions to ensure that no funds are being moved to or from sanctioned persons or countries. This is especially important in sectors such as banking, insurance, and export services, where transactions can be complex and involve multiple intermediaries.
3. **Risk Assessment:** Businesses should conduct a thorough risk assessment to identify areas where they may be exposed to sanctions risks, such as dealing with high-risk jurisdictions or industries. A well-structured risk assessment allows a business to tailor its compliance efforts, focusing on areas where the likelihood of sanctions breaches is higher

When carrying out due diligence, lists are an invaluable resource and are usually the first port of call for ascertaining whether a particular person or entity is subject to financial sanctions. This will usually entail a prohibition on dealing with that person or entity – directly or indirectly – unless a licence to do so is obtained from the relevant regulator.

However, it is important that lists not be the only source consulted:

- **spelling variances:** when transliterated from languages with non-Latin alphabets, different transliterations can lead to a risk of false negatives when carrying out searches; and
- **sanctions lists do not purport to be exhaustive:** for example, entities under the control or ownership of a designated person are subject to the same sanction as the designated person, even though they may not be listed.

There have been judgments where the UK courts have been required to determine whether or not a particular corporate entity is under the direct or indirect control of a designated person. For example, in *Mints & ors v PJSC National Bank Trust & anor* [2023] EWCA 1332 and *Hellard & Ors v OJSC Rossiysky Kredit Bank & Ors* [2024] EWHC 1783, the High Court has considered the circumstances in which an entity can be considered under the control of a designated person for the purposes of Regulation 7 of the Russia (Sanctions) (EU Exit) Regulations 2019 (as amended).

INDIRECT EXPOSURE TO SANCTIONS

One of the biggest risks for businesses is indirect exposure to sanctions. This occurs when a business deals with a third party that is not directly subject to sanctions but is owned or controlled by a designated person or entity. For example, a company may be dealing with a supplier that is not sanctioned, but if that supplier is majority-owned by a designated entity, any transactions with that supplier could still be considered a breach of sanctions.

To manage this risk, businesses need to extend their due diligence efforts to include ownership structures and beneficial ownership details. Understanding who ultimately controls or benefits from a third-party relationship is critical to avoiding indirect exposure to sanctions violations.

SECTORIAL SANCTIONS AND THEIR IMPACT

Certain sectors are particularly vulnerable to sanctions, especially in industries such as energy, defence, and finance. Sectoral sanctions do not impose blanket restrictions but instead target specific activities within a sector. For example:

- **Energy Sector:** Sanctions may restrict investment in energy infrastructure projects or prohibit the sale of certain equipment used for oil exploration.
- **Financial Sector:** Sectoral sanctions may limit access to certain financial services, such as loan financing or securities trading, for entities linked to sanctioned regimes.

Understanding the scope of sectoral sanctions is essential for businesses operating in these industries. Sectoral sanctions require businesses to carefully assess their exposure and ensure they are not inadvertently supporting activities that breach sanctions regulations.

THIRD-PARTY DUE DILIGENCE

The risks associated with third-party transactions cannot be overstated. Businesses must have robust systems in place to vet any third parties they work with, including suppliers, subcontractors, and customers. Third-party due diligence should include:

- **Ownership and Control Checks:** Ensure that the third party is not owned or controlled by a designated person or entity.
- **Transaction Vetting:** Regularly review the nature of transactions with third parties to ensure compliance.
- **Ongoing Monitoring:** Third parties should be subject to continuous monitoring to ensure they have not been newly designated under any sanctions regime.

By implementing these key concepts and incorporating them into a robust compliance framework, businesses can significantly reduce their risk of violating financial sanctions and facing the substantial penalties that follow.

In the next section, we will discuss the licenses and exemptions that may apply to businesses navigating the complex world of financial sanctions.

Trade Sanctions

Trade sanctions are prohibitions on the export or import of goods or services to a particular state. This may entail a blanket prohibition on all or most trade with a targeted country.

At its most extreme, trade sanctions can take the form of a general trade embargo against the target state. This occurred in the UK with the passage of the Trading with the Enemy Act 1939, which prohibited all forms of trade with Germany.

These days, export and import bans tend to focus on particular industries which are of strategic importance or high-value to a particular state. For example, following the Russian invasion of Ukraine in 2022, the UK, USA and EU have prohibited the import of Russian oil, in an attempt to place a stranglehold on an important income source for the Russian regime.

The different types of trade sanctions can include:

- **Sectoral Sanctions:** These target specific sectors of a country's economy. For instance, the oil, gas, and defence industries are frequently subject to sanctions, particularly in countries like Russia or Iran. Following the annexation of Crimea in 2014, the EU banned the provision of energy related equipment to the Crimea region. Sectoral sanctions often prohibit investment in or dealings with certain companies in these sectors.
- **Import Restrictions:** Restricting the purchase of goods from a target country, often used to limit its revenue.
- **Targeted Sanctions:** More specific measures that include prohibitions on specific individuals, companies, or sectors, sometimes combined with asset freezes and travel bans.
- **Tariffs:** Taxes on imported goods, which can be imposed as a sanction to increase costs and make imports less attractive. Recently, for example, the US Government has imposed punitive tariffs on India in response to that country's refineries importing Russian oil.
- **Quotas:** Limits on the quantity of specific goods that can be imported into a country.

Since 2022, a raft of trade sanctions has been targeted against Russia, these being set out in Chapter 4 of the Russia (Sanctions) (EU Exit) Regulations 2019. Effectively, these have placed a ban on the direct or indirect provision of certain goods or services to "persons connected to Russia", a term defined under Reg 21(2) of the Russia (Sanctions) (EU Exit) Regulations 2019. There are also a number of import bans (e.g. in relation to oil and oil products of Russian origin (Regulation 46Z4).

The prohibition on exporting sectoral sanctions to Russia enacted as Chapter 4N and it's corresponding Schedule 3IA have been inserted in an amendment to the Russia Regulations, the Russia (Sanctions) (EU Exit) (Amendment) Regulations 2025, and has had significant impact on many of our clients. This provides that even where a counterparty is not itself designated, supplying, transferring or making available certain listed software or related technology to that counterparty may be prohibited if it is ultimately intended for use by a person connected to Russia. This could also extend to scenarios such as employees residing within Russia making use of the company's business enterprise software, for example accounting or enterprise resource planning tools, that fall within the scope of the restrictions. Careful mapping of the software's end use, end user and any potential re-transfer is essential to avoid breaching these trade sanctions.

Licenses and Exemptions

LICENSING REGIMES

While financial sanctions are designed to limit or prevent certain transactions with designated persons and entities, there are situations in which businesses may apply for licences that allow them to carry out activities that would otherwise be prohibited. A licence is a legal authorisation granted by the relevant sanctions authority.

Whilst in the UK, this is typically OFSI (which permits certain transactions or services to take place without breaching financial sanctions regulations), on other occasions other regulators may need to be approached. OTSI is in charge of issuing licences to provide trade sanctioned services (services which under sanctions law cannot be provided to a person connected to a particular sanctioned country). The Export Control Joint Unit is in charge of issuing export licences.

Licences are typically granted for specific transactions or activities and come with clear terms and conditions. It is the responsibility of the business or individual applying for the license to ensure they remain in compliance with its conditions.

A licence can only be issued on the basis of a specific ground laid down in the parent legislation. For example, Schedule 5 of the Russia (Sanctions) (EU Exit) Regulations 2019 provides twenty separate grounds for issuing licences to authorise activities that would otherwise be prohibited under those Regulations.

Available grounds include:

- covering expenses such as food, rent and medicines (referred to as basic needs);
- reasonable professional legal fees or reasonable expenses associated with the provision of legal services;
- prior obligations (if the obligation/contract started before the sanction was imposed);
- covering the payment of fees/service charges for routine holding or maintenance of frozen funds or economic resources;
- implementation/satisfaction of a judicial, administrative or arbitral decision or lien;
- post-designation judicial decisions (for non-UN designated persons only);
- extraordinary expenses, where considered appropriate;
- extraordinary situations, where considered appropriate (only for non-UN listed persons);
- humanitarian assistance;
- diplomatic missions;
- insolvency;
- divestment; or
- extraordinary situations.

OFSI has attempted to make clear that 'extraordinary situations' are not intended to operate as a "catch-all", enabling all applications, however this has not prevented applicants from trying to rely on it that way.

Specific licenses are often issued for:

- **Humanitarian Aid:** Many financial sanctions regimes include exceptions for the provision of humanitarian aid, such as food, medical supplies, or disaster relief. For example, even though a country may be under sanctions, an organisation providing humanitarian assistance may obtain a licence to operate in that region.
- **Authorising the performance of a contract entered into before the prohibition was imposed:** A non-sanctioned company may be awaiting payment for goods already delivered to a person who has since become designated under a sanctions regime. A licence may be required to authorise payment for the performance in order to avoid unfairness.
- **Legal services:** Legal practitioners may require a licence to provide legal representation to a designated person or entity, particularly when payment for those services involves frozen assets. A licence ensures that the lawyer can be paid without breaching sanctions laws. As noted below, a General Licence has been issued under the Russia rules for this purpose, but other sanctions rules do not benefit from similar general licences.
- **Cultural or Religious Transactions:** Licences may be granted for the transfer of funds for cultural, religious, or educational purposes, ensuring that these transactions do not support prohibited activities.

GENERAL AND SPECIFIC LICENCES

There are broadly two types of licences: general and specific. General licences permit, subject to conditions, parties to engage in certain categories of transactions which would otherwise be prohibited under the sanctions rules.

Some examples of general licences currently in force are set out below:

GENERAL LICENCE	CODE/DATE	JURISDICTION/REGIME	SUMMARY OF AUTHORISED ACTIVITY	PRACTICAL RELEVANCE
Legal Services	INT/2025/6160920 (28 April 2025)	Russia	Permits the provision and payment of legal services to or for designated persons, subject to defined conditions.	Enables law firms and clients to continue legal representation and access to justice.
Arbitration Costs	INT/2025/5787748 (28 Mar 2025)	Russia	Allows payment of arbitration fees and related costs involving designated persons.	Ensures dispute resolution can proceed despite asset freezes.
Interim Basic Necessities for Designated Persons	INT/2025/5632740 (14 Jan 2025)	Multiple	Authorises limited payments from frozen accounts to meet essential living expenses of designated individuals.	Demonstrates the humanitarian principle underpinning sanctions law.
Oil Price Cap	INT/2024/4423849 (16 Feb 2024; amended Jul 2025)	Russia	Permits transport, insurance and related services for Russian oil sold at or below the G7 price cap.	Maintains global energy stability while restricting Russian revenue.
Humanitarian Activity	INT/2025/5810196 (Syria) / INT/2022/1947936 (Russia)	Syria/Russia	Permits activities necessary to deliver humanitarian aid, including financial transactions and logistical support.	Ensures sanctions do not obstruct humanitarian operations.

APPLICATION PROCESS

Where an applicant wishes to engage in an action which would be prohibited under the sanctions rules, but no General Licence is available, they are required to apply for a specific licence.

To obtain a licence, a business must submit an application to OFSI and/or the relevant UK or overseas authority, detailing the nature of the transaction or service and why it qualifies for an exemption.

OFSI assesses the application based on:

- **Risk of Circumvention:** OFSI will consider whether granting the licence might enable the designated person to access resources that support their prohibited activities.
- **Humanitarian Impact:** For humanitarian licences, OFSI weighs the benefits of allowing the transaction against the objectives of the sanctions.
- **Compliance with Sanctions Regime:** OFSI will ensure that the licence fits within the broader sanctions regime and does not undermine the enforcement of financial sanctions.

Once a licence is granted, the applicant must strictly comply with all conditions. Failure to do so can result in the license being revoked and possible penalties for non-compliance.

An applicant must make clear the specific regime to which its application relates. It must base its application on one or more of the specific available grounds for licensing available under the relevant legislation. In the context of Russia, the grounds are set out in Schedule 5 of the Russia (Sanctions) (EU Exit) Regulations 2019.

An applicant unhappy with the outcome of the process may seek a judicial review of the decision. However, the Administrative Courts are likely to afford a wide margin of appreciation to the issuing authority in carrying out its licensing functions.

It is important not to do anything which would contravene the sanctions rules until the licence has been issued and the relevant actions duly authorised.

OIL PRICE CAP EXEMPTION

One specific license regime relates to the oil price cap exemption in the sanctions against Russia. Under Chapter 4I and 4IA of the Russia (Sanctions) (EU Exit) Regulations 2019, it is not only prohibited to import oil products of Russian origin but also services such as shipping to third countries, insurance, and financing where these services are provided for the transportation of Russian oil.

Shipping of such products to third countries may be allowed if the oil has been purchased at or below a price cap set by the UK and its allies. The purpose of this price cap is to limit the revenue Russia can generate from its oil exports, while ensuring that oil continues to flow to global markets, preventing price spikes and minimising fall-out to countries in the developing world.

Businesses involved in transporting Russian oil must be aware of the price cap and comply with its terms. Failure to do so could result in penalties for breaching sanctions.

GUIDANCE ON EXEMPTIONS

OFSI provides detailed guidance on exemptions to help businesses understand when they might qualify for a licence or when they can legally carry out certain activities without breaching sanctions. Some common exemptions include:

- **Payments for Legal Fees:** Designated persons may use frozen assets to pay for legal representation, provided they obtain a licence.
- **Basic Needs:** Certain payments may be allowed from frozen accounts to cover basic living expenses, such as food, rent, or utilities, though these must be licensed.
- **Medical and Humanitarian Goods:** There are broad exemptions for the provision of humanitarian and medical goods to countries under sanctions, as long as the goods do not support prohibited activities.

REPORTING AND RECORD-KEEPING OBLIGATIONS

Once a licence is granted, businesses are subject to reporting and record-keeping obligations. These obligations ensure that the relevant authorities can monitor compliance with the terms of the license. Businesses must:

- keep detailed records of all transactions related to the licence;
- ensure required notifications are made punctually, as and when required by the terms of the licence;
- submit regular reports to the issuing authority detailing how the license has been used; and
- notify the issuing authority immediately of any changes in the circumstances under which the license was granted.

CHALLENGES IN OBTAINING LICENSES

While the licensing regime is a crucial tool for enabling certain transactions, obtaining a licence can be challenging. Applications must be comprehensive and well-documented, and the decision-making process can be lengthy. In some cases, the sensitive nature of the transaction or the risks involved may lead to an application being rejected. As such, businesses must ensure they thoroughly prepare their applications and understand the terms under which a licence can be issued.

CONCLUSION

Licences and exemptions play a vital role in navigating financial sanctions, enabling businesses to continue necessary operations while remaining compliant with the law. However, it is crucial that businesses fully understand the conditions under which licenses are granted, strictly adhere to the reporting requirements, and ensure that all activities fall within the boundaries of the license. By doing so, they can mitigate the risks of inadvertently breaching financial sanctions and facing significant penalties.

In the next section, we will explore the obligations and penalties for businesses operating under the financial sanctions regime.

Obligations and Reporting

REPORTING OBLIGATIONS

Under UK financial sanctions law, "relevant firms" have strict reporting obligations to ensure full compliance with the sanctions regime. "Relevant firms" include (among others) providers of legal or accountancy services, financial institutions and estate agents.

The primary obligations include:

1. **Reporting Frozen Assets:** If a business holds or controls assets that belong to a designated person or entity, it must immediately report these assets to OFSI. This includes both tangible assets (such as property) and financial assets (such as bank accounts or securities). Reports must include detailed information about the assets and their value.
2. **Suspected Breaches:** If a business suspects that a transaction or relationship may be in violation of financial sanctions, it is obligated to report this suspicion to OFSI as soon as possible. This could involve, for example, discovering that a client or counterparty is on the sanctions list after a transaction has already been initiated.
3. **Reporting Suspicious Activity:** Financial institutions, including banks and payment processors, are required to report any transactions that may involve sanctioned persons or activities. This requirement often intersects with **anti-money laundering (AML)** obligations, where businesses are required to monitor transactions and raise alerts if they suspect foul play.

PENALTIES FOR NON-COMPLIANCE

Failure to comply with the UK's sanctions regime can lead to significant civil and criminal penalties. Enforcement is shared between:

- **The Office of Financial Sanctions Implementation (OFSI)** within HM Treasury, responsible for financial sanctions; and
- **The Office of Trade Sanctions Implementation (OTSI)** within the Department for Business and Trade (DBT), responsible for trade sanctions (e.g., export bans, import controls, and related licensing).

Both authorities operate under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA 2018) and the Policing and Crime Act 2017, and each has published its own enforcement guidance setting out how it determines breaches, calculates penalties, and exercises discretion to publicise enforcement outcomes.

i. Civil Monetary Penalties

Both OFSI and OTSI have the power to impose **civil monetary penalties** for breaches of sanctions.

- **Legal Basis:** Section 146 of the Policing and Crime Act 2017 allows either OFSI or OTSI to impose a penalty where, on the balance of probabilities, a person has breached financial or trade sanctions.
- **Strict Liability:** Since 15 June 2022, under the Economic Crime (Transparency and Enforcement) Act 2022, OFSI can impose civil penalties for breaches even where the person did not know or have reasonable cause to suspect they were breaching sanctions. The same approach applies to OTSI's regime for trade sanctions.
- **Penalty Limit:** The maximum civil penalty is the greater of £1 million or 50% of the value of the funds, goods, or services involved in the breach.
- **Voluntary Disclosure:** Both OFSI and OTSI take voluntary disclosure and cooperation into account as mitigating factors. Their policies explicitly encourage self-reporting to reduce penalty exposure.
- OFSI, *Monetary Penalties for Breaches of Financial Sanctions – Guidance* (August 2023)
- OTSI, *Trade Sanctions Enforcement Guidance* (April 2024)

ii. Criminal Penalties

Serious or deliberate breaches may result in **criminal prosecution**.

- **Legal Basis:** Offences are created under SAMLA 2018 and each of the specific sanctions regulations (e.g., Russia (Sanctions) (EU Exit) Regulations 2019, regulations 77–78).
- **Penalty:** Conviction may result in an unlimited fine, and individuals can face up to seven years' imprisonment.
- **Referral:** OFSI and OTSI will refer suspected criminal cases to law enforcement agencies (such as the National Crime Agency or the Crown Prosecution Service) where intentional misconduct, concealment, or evasion is indicated.
- **Enforcement Policy:** Both offices apply a proportionality test when deciding whether to refer a case for criminal investigation, considering factors such as intent, harm, and systemic weakness in compliance systems.

iii. Publication and Reputational Penalties

Under section 149 of the Policing and Crime Act 2017, both OFSI and OTSI may publicly identify persons or companies that breach sanctions, even where no monetary penalty is imposed.

This may include:

- the entity's name;
- the nature of the breach; and
- a summary of the enforcement action (penalty, warning letter, or caution).

Both regulators treat publication as an integral enforcement tool designed to promote deterrence and transparency.

Publication on OFSI's or OTSI's websites can have substantial reputational consequences for firms in regulated sectors such as financial services, professional services, logistics, or export control.

iv. Aggravating Factors

When deciding on an enforcement action or setting a penalty, OFSI (para. 5.19 ff.) and OTSI (para. 7.15 ff.) consider the following as aggravating when setting penalties:

1. **Knowledge or deliberate conduct** – the breach was knowing, intentional, or reckless.
2. **Wilful circumvention or concealment** – use of false documentation, indirect structures, or third-party routing to evade sanctions.
3. **Significant harm or value** – high-value transactions or conduct causing substantial economic benefit to a designated person or harm to the sanctions regime.
4. **Repeated or systemic failures** – multiple breaches, poor governance, or disregard of prior warnings.
5. **Lack of cooperation** – delay, obstruction, or failure to supply information requested by OFSI/OTSI.
6. **Failure to remediate** – absence of corrective action after a breach is identified.
7. **Position of responsibility** – senior management involvement or failure of oversight.
8. **Market impact or sector risk** – behaviour likely to undermine public confidence or the deterrent effect of sanctions.

v. Mitigating Factors

Conversely, the following are recognised as mitigating:

1. **Voluntary disclosure** – full, timely self-reporting prior to OFSI/OTSI detection.
2. **Cooperation** – openness during the investigation and provision of all relevant evidence.
3. **Effective compliance controls** – existence of proportionate, risk-based screening and escalation systems.
4. **Remediation** – prompt corrective measures, including staff retraining or system upgrades.
5. **Low value or inadvertence** – genuinely inadvertent, technical, or de-minimis breaches.
6. **External factors** – reliance on inaccurate data from third-party screening tools where reasonable diligence was exercised.
7. **Public-interest considerations** – humanitarian or similar justifications consistent with the object of the sanctions regime.

Businesses are strongly encouraged to self-report any potential breaches to OFSI. Self-reporting demonstrates a commitment to compliance and may lead to reduced penalties. If a breach is identified through a third party (e.g., an external audit or regulatory investigation), the penalties could be significantly higher than if the business had come forward voluntarily.

A dedicated form has been introduced by OFSI for the purpose of reporting breaches:

Financial sanctions suspected breach reporting form.

vi. Appealing Penalty Decisions

To appeal an Office of Financial Sanctions Implementation (OFSI) penalty, the defendant must first seek a review from OFSI. If the defendant disagrees with the outcome, it may then apply to the High Court or Court of Session in Scotland for a judicial review.

The process for review and appeal is detailed in Chapter 7 of OFSI's enforcement and monetary penalty guidance. The grounds for seeking judicial review will be those laid down in general public law (e.g. illegality, irrationality and procedural impropriety, see *Council of Civil Service Unions v Minister for the Civil Service* [1985] A.C. 374)

vii. Reform

At the time of witing, OFSI is conducting a consultation for the possible reform of its enforcement policy. OFSI is canvassing views on increasing the maximum fines, such that it would be able to impose penalties of the higher of:

a. £2 million; or
b. 100% of the total value of the funds or resources (where the case relates to particular funds or reserves, such as an unauthorised payment to a designated person).

OFSI would retain discretion to fix a penalty up to these maxima, assessing the proportion of the case. It has also outlined a number of other proposals to streamline its processes, such as an early settlement scheme.

STRICT LIABILITY AND INTENT

A key concept in UK sanctions law is strict liability. This means that businesses can be penalised for breaches of sanctions even if they did not intentionally commit a violation. In such cases, OFSI does not need to prove that the business was aware of the breach; it only needs to establish that a breach occurred. Thus, it is crucial for businesses to have robust screening and due diligence systems in place, as a simple oversight can result in significant penalties.

RECORD KEEPING REQUIREMENTS

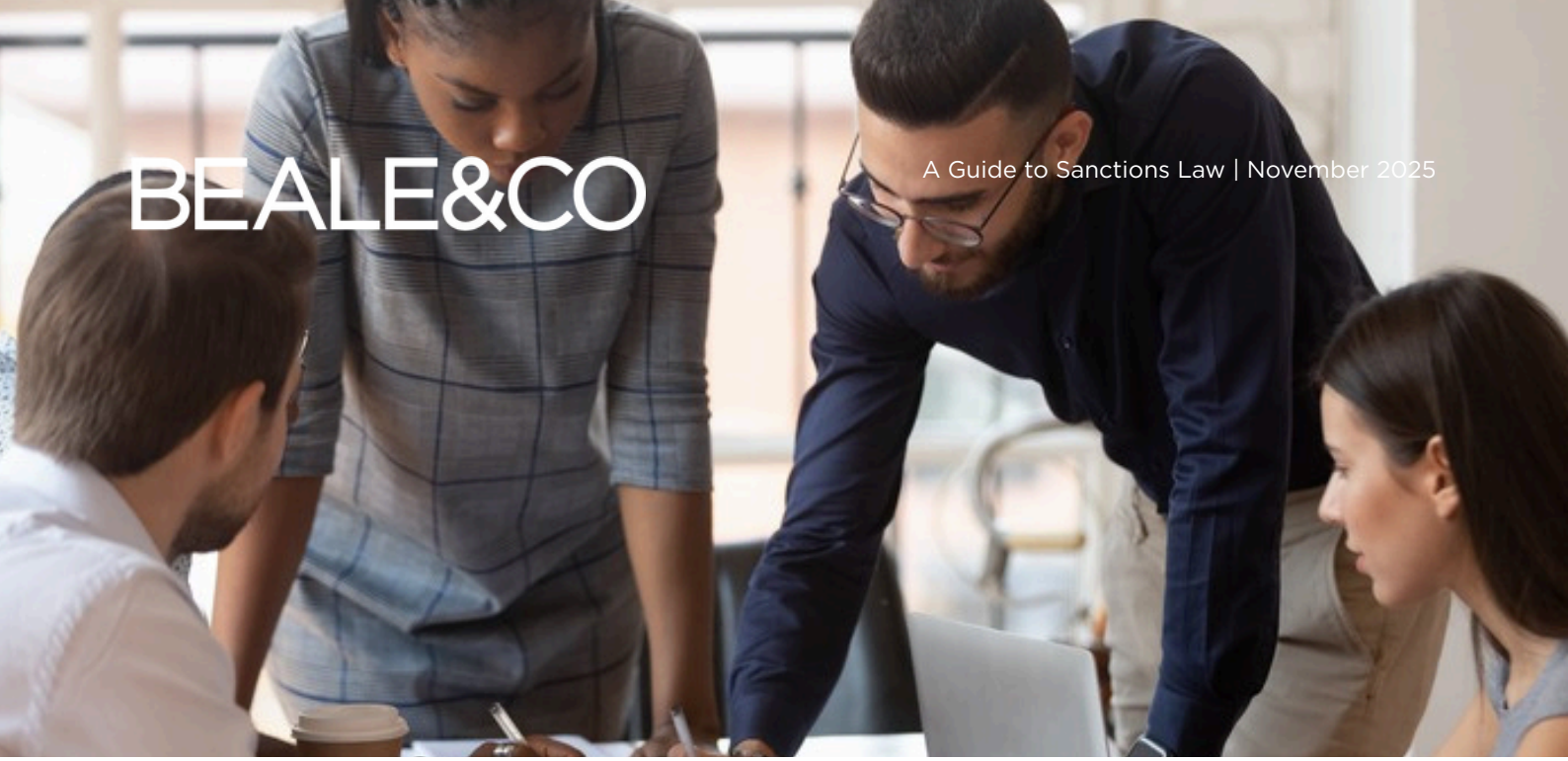
In addition to reporting obligations, businesses must maintain detailed records of their transactions and sanctions screening processes. These records must be available for review by OFSI or other relevant enforcement bodies, such as HMRC, during investigations. Records should include:

- **Screening Logs:** Evidence of sanctions screening for clients, suppliers, and third parties.
- **Transaction Details:** Full documentation of any transactions involving designated persons, including attempts to secure a licence or exemption.
- **Internal Policies and Procedures:** Written records of the business's sanctions compliance policies, including training records for staff and descriptions of internal processes for monitoring and reporting.

CONCLUSION

Reporting obligations and record-keeping requirements are essential components of the UK's financial sanctions regime. Businesses must not only ensure that they have the appropriate systems in place to monitor and report any dealings with designated persons or entities, but must also maintain a strong paper trail to demonstrate their compliance. Failure to meet these obligations can lead to significant financial penalties, criminal prosecution, and reputational damage. By adhering to these obligations, businesses can avoid the pitfalls of non-compliance and safeguard their operations from the risks associated with financial sanctions.

In the next section, we will explore real-world case studies that highlight how businesses have navigated financial sanctions challenges and the lessons learned from enforcement actions.



Case Studies and Examples

To provide a practical understanding of financial sanctions compliance, this section explores real-world case studies where businesses have faced sanctions challenges and the lessons learned from enforcement actions. These examples highlight common pitfalls, illustrate successful compliance strategies, and demonstrate the potential consequences of breaches.

CASE STUDY 1: THE BANK AND THE DESIGNATED ENTITY

A UK-based bank inadvertently facilitated payments to a designated entity. The bank's compliance team failed to screen the counterparty thoroughly, resulting in the transfer of funds to an organisation subject to sanctions under OFSI regulations. Despite the lack of intent, OFSI imposed a significant penalty on the bank under the principle of strict liability.

Key Lessons

- **Thorough Screening:** The bank's failure highlights the importance of rigorous and continuous screening. Implementing real-time updates and automated systems to flag designated persons can prevent such breaches.
- **Mitigating Actions:** Although the bank was fined, the penalty was reduced due to its swift self-reporting and cooperation with OFSI. This illustrates the importance of prompt action and transparency when a breach occurs.

CASE STUDY 2: LEGAL FIRM AND LICENSE FOR SERVICES

A UK law firm applied for a licence to provide legal advice to a designated person under financial sanctions. The firm needed to receive payment from frozen assets, which would have violated sanctions without the proper licensing. By working closely with OFSI and ensuring compliance with the terms of the license, the firm successfully navigated the complexities of sanctions compliance.

Key Lessons

- **Licensing as a Compliance Tool:** This case demonstrates the importance of obtaining the necessary licenses when dealing with designated persons. Legal, financial, and humanitarian services may be exempt from sanctions if proper licenses are secured.
- **Understanding Licensing Conditions:** The firm's success lay in strictly adhering to the conditions of the license, ensuring no funds were misused or transferred without authorisation.

CASE STUDY 3: EXPORTER AND TRADE SANCTIONS

A UK-based exporter was penalised for inadvertently selling goods that were restricted under UK trade sanctions. The company had failed to assess its supply chain thoroughly, and its goods ended up in a sanctioned country. HMRC imposed a civil penalty on the business, emphasising the need for comprehensive due diligence in international trade.

Key Lessons

- **Supply Chain Due Diligence:** Businesses must conduct thorough due diligence, especially when exporting goods that could be diverted to sanctioned countries. Knowing where products end up is crucial to compliance.
- **Sectoral Sanctions Awareness:** Sectoral sanctions can be complex, particularly when they target specific industries like energy or technology. Exporters must stay updated on the restrictions relevant to their industry.

CASE STUDY 4: A MULTINATIONAL'S BREACH OF SECTORAL SANCTIONS

A multinational company dealing in energy services was fined by OFSI for breaching sectoral sanctions related to Russia. The company continued to provide technical assistance and financial support to a Russian entity in the energy sector, unaware that the sanctions restricted such activities. The case resulted in heavy fines and reputational damage to the company.

Key Lessons

- **Sectoral Sanctions Compliance:** Sectoral sanctions are less obvious than traditional asset freezes, as they focus on prohibiting specific types of support, such as financing or equipment provision. Companies in sectors like energy or defence must understand how these sanctions apply to their operations.
- **Continuous Training:** Employees involved in high-risk areas, such as international sales and procurement, must be trained regularly to identify and avoid sectoral sanctions breaches.

CONCLUSION

These case studies emphasise the need for rigorous due diligence, ongoing training, and the use of automated compliance tools to ensure compliance with financial and trade sanctions. By understanding the common pitfalls faced by other businesses and learning from their experiences, companies can better navigate the complex regulatory landscape and avoid costly penalties.

In the next section, we will explore practical steps for compliance, outlining strategies and tools that businesses can implement to safeguard their operations against sanctions risks.

Effect of Sanctions on Contractual Performance

A question our sanctions team is asked frequently is whether parties are still required to perform contracts where the other party, or for that matter the subject matter of the contract itself, has become affected by sanctions.

For example, if the Russian employer which has commissioned works from a contractor has become a designated person under the Russia (Sanctions) (EU Exit) Regulations 2019, can the works still be performed? Can it still be paid? Is there a separate risk of contractual liability from abruptly stopping works?

Clearly, legal advice is required in this specific situation. As a general comment (and not advice), even where there is a risk of sanctions breach, the safest course of action almost always will be to stop work and, where necessary, seek a licence to obtain payment before doing anything further.

i. Supervening Illegality and (some) Statutory Protection

If performance of a contractual obligation becomes prohibited by law, perhaps due to financial or trade sanctions imposed after contract formation, English law generally treats this as supervening illegality. In such cases, the contract is likely to be frustrated, discharging both parties from further performance.

For example, a supplier is prevented from delivering goods to a newly sanctioned counterparty because export controls or financial prohibitions make performance unlawful.

The frustration doctrine applies only where the supervening event is unexpected, beyond the parties' control, and renders performance impossible or radically different from what was agreed.

Section 44 of the Sanctions and Anti-Money Laundering Act 2018 provides a defence from civil liability (in contract or tort) for an act or omission where something is done (or not done) in the reasonable belief it is to comply with regulations made under SAMLA or instructions given under SAMLA. Whether or not section 44 applies will depend on the facts of the case and the reasonableness of the belief that the acts must be taken to comply (see e.g. *Celestial Aviation Services Limited v UniCredit Bank GmbH, London Branch* [2024] EWCA Civ 628).

ii. Force Majeure Clauses

Many contracts include force majeure provisions that expressly cover government action or sanctions. If properly drafted, such clauses may excuse non-performance or delay without invoking frustration. Parties should review:

- Whether sanctions or "compliance with law" are listed as qualifying events.
- Whether the clause allows suspension, termination, or renegotiation.
- Any notice requirements or mitigation duties.

iii. Contractual Representations and Warranties

Sanctions clauses often include warranties that neither party is a designated person and undertakings to comply with applicable sanctions laws. Breach of these warranties may entitle the innocent party to terminate or seek damages.

Practical Steps for Compliance

In order to ensure full compliance with the UK's financial sanctions regime, businesses need to implement robust systems and procedures that minimise the risk of breaching sanctions. This section outlines the **practical steps** businesses can take to navigate sanctions compliance effectively.

DEVELOPING A SANCTIONS POLICY

Every business, especially those involved in international transactions, should have a clearly defined sanctions compliance policy. This policy should outline:

- The legal requirements for complying with financial sanctions.
- Internal processes for screening clients, suppliers, and transactions.
- Roles and responsibilities within the company for maintaining compliance.

The policy should be regularly updated in line with changes to UK sanctions laws, particularly when new sanctions are imposed on specific countries, sectors, or individuals. In its recent decision in *Colorcon* (2025), OFSI made clear that it will not necessarily consider the existence of sanctions policies and processes mitigating if they are not fit for purpose. For those purposes, a sanctions policy that was seven years old would not be considered effective.

IMPLEMENTING A SANCTIONS SCREENING SYSTEM

A key part of any compliance program is a robust sanctions screening system. This involves checking clients, business partners, and transactions against the OFSI Consolidated List and other relevant sanctions lists (such as those from the US, EU, or UN). Automated screening tools can help businesses:

- Identify designated persons and entities before engaging in transactions.
- Ensure real-time compliance by checking updates to sanctions lists.
- Flag potential risks early, preventing inadvertent breaches.

Screening should not be a one-time process but should be carried out continuously, particularly for ongoing relationships with suppliers, contractors, and financial partners.

CONDUCTING DUE DILIGENCE

In addition to sanctions screening, businesses must carry out thorough due diligence on their partners, clients, and suppliers to avoid indirect exposure to sanctions. This includes:

- Verifying the ownership structures of third parties to ensure they are not controlled by designated persons.
- Reviewing the jurisdictional risks of doing business in sanctioned countries or with businesses that have ties to sanctioned regimes.
- Ensuring that the company's entire supply chain complies with relevant sanctions laws.

Effective due diligence helps businesses identify any high-risk partners and mitigates the potential of indirect sanctions breaches through third-party relationships.

TRAINING AND AWARENESS

Sanctions compliance requires awareness at all levels of an organisation. Businesses should implement regular training programs for employees, particularly those working in finance, legal, sales, and procurement. Training should cover:

- How to identify sanctioned persons and entities.
- The specific sectoral sanctions that may apply to their industry (e.g., energy, defence, finance).
- How to handle potential breaches and report them to OFSI.

Training ensures that all employees understand the risks of non-compliance and know how to follow internal sanctions protocols.

MONITORING AND AUDITING

Sanctions compliance is an ongoing process that requires monitoring and regular audits. Companies should regularly review their transactions and client relationships to ensure continued compliance. This can involve:

- Auditing transaction records to check for potential red flags.
- Monitoring high-risk areas of the business, such as international trade and export services.
- Conducting internal audits of the compliance program itself to identify weaknesses or areas that require improvement.

Regular auditing and monitoring help businesses stay ahead of potential risks and ensure their compliance processes remain effective

REPORTING AND RECORD-KEEPING

As outlined in Section 7, businesses are required to report any suspicious activity or breaches of sanctions to OFSI. In addition to reporting, businesses should maintain detailed records of:

- All transactions involving high-risk clients or jurisdictions.
- Screening and due diligence processes.
- Any licenses or exemptions obtained from OFSI.

These records should be available for review during an internal audit or a regulatory investigation, providing evidence that the business has taken all necessary steps to comply with sanctions laws.

ENGAGING LEGAL AND COMPLIANCE EXPERTS

Given the complexity of the financial sanctions regime, businesses should engage legal and compliance experts to provide advice on specific transactions or potential risks. Experts can help:

- Interpret the nuances of sanctions laws and provide tailored advice for high-risk sectors or jurisdictions.
- Assist with license applications for activities that may fall under sanctioned categories.
- Ensure that businesses are following best practices and complying with international sanctions.

External counsel or compliance consultants can provide valuable guidance, especially in areas where the business is unsure about the implications of certain transactions.

PRACTICAL MEASURES

- **Screening:** Regularly screen counterparties and intermediaries against sanctions lists throughout contract performance.
- **Contract Drafting:** Incorporate tailored sanctions clauses allocating risk, defining "sanctions event," and specifying termination rights.
- **Licensing:** Where possible, seek a licence from OFSI or OTSI to permit continued performance of otherwise prohibited activities.

CONCLUSION

By developing a clear sanctions policy, implementing a rigorous screening and due diligence process, providing regular employee training, and maintaining a proactive monitoring system, businesses can significantly reduce the risks associated with financial sanctions. In an increasingly regulated environment, a comprehensive compliance program is essential to avoiding breaches, penalties, and reputational damage.

In the final section, we will provide additional resources and contact information to help businesses stay informed about financial sanctions and access expert advice.

Additional Resources

To effectively navigate financial sanctions and ensure ongoing compliance, businesses must stay informed and have access to the latest guidance, tools, and support. This section provides a list of key resources that can help organisations monitor changes in sanctions regimes, seek expert advice, and understand their obligations under UK law.

OFSI RESOURCES

The Office of Financial Sanctions Implementation (OFSI) offers several tools and guidance documents to help businesses understand their sanctions obligations:

- **OFSI Consolidated List:** This is the official list of designated persons and entities that businesses must avoid transacting with. It is regularly updated and can be accessed on the OFSI website.
- **Financial Sanctions Guidance:** OFSI publishes detailed guidance on how businesses should comply with financial sanctions, including advice on reporting, licensing, and penalties.
- **OFSI Reporting Portal:** For businesses needing to report suspected breaches, asset freezes, or request licenses, OFSI offers an online portal for these submissions.

HMRC EXPORT CONTROL AND TRADE SANCTIONS

For businesses involved in international trade, especially those exporting goods to sanctioned countries or dealing with dual-use items, HMRC provides guidance on trade sanctions and export control:

- **Export Control Joint Unit (ECJU):** The ECJU manages the UK's export licensing system in accordance with the Export Control Order 2008, providing advice and licenses for controlled goods.
- **HMRC Trade Sanctions Guidance:** For detailed advice on trade sanctions and penalties for breaches.

EXTERNAL SANCTIONS SCREENING TOOLS

To assist with due diligence and compliance screening, businesses may consider using third-party services that offer sanctions screening tools. These services provide automated checks against various global sanctions lists.

LEGAL AND COMPLIANCE ADVICE

For complex sanctions issues or questions about specific transactions, businesses should seek advice from external legal advisors, ensuring that this is covered by legal privilege.
Beale & Co's financial sanctions team can help with any queries you may have. Our contact details are included at the end of this booklet.

INTERNATIONAL SANCTIONS BODIES

For businesses operating internationally, it is crucial to understand the sanctions regimes in other jurisdictions. Below are resources from other key sanctions bodies:

- **United States Department of the Treasury, Office of Foreign Assets Control (OFAC):** Provides guidance on US sanctions, lists of designated persons, and license applications.
- **European Union Sanctions:** The EU provides its own consolidated list of sanctioned persons and entities under its jurisdiction.

TRAINING AND WORKSHOPS

Organisations can benefit from regular training on sanctions compliance. Many professional bodies and consultancy firms offer workshops and certification programs.

We regularly run sanctions webinars and can provide specific, tailored training for clients. We can direct this to the particular needs of your business and the sectors in which you operate. If this is of interest please do not hesitate to contact us using the contact details at the end of this Guide.

CONCLUSION

The resources outlined in this section can help businesses to stay updated on changes to sanctions regimes, improve their compliance systems, and seek expert advice when necessary. Maintaining a proactive approach to sanctions compliance not only ensures that companies avoid penalties but also protects their reputation and operational integrity in the global marketplace.

For more information, please refer to the sanctions section of Beale & Co's website.

For any further questions or specific advice, please contact us via the details below.

KEY CONTACTS

Paul Henty
Partner

DDI: +44 20 7469 0499
E: p.henty@beale-law.com

Deen Taj
Solicitor

DDI: +44 (0) 20 7469 0414
E: d.taj@beale-law.com

Charlie Bayliss
Solicitor

DDI: +44 (0) 20 3053 3082
E: c.bayliss@beale-law.com

BEALE&CO

International Construction and Insurance Law Specialists

www.beale-law.com