Trading With Risk – Understanding UK Sanctions and Commercial Exposure

Procurement and Supply Chain Management Made Simple.

Foreword

International trade has always involved risk, but sanctions have changed the nature of that risk. Commercial relationships can now be legally restricted almost overnight due to political developments, ownership changes, new designations, or emerging concerns about where goods, services, or money ultimately flow. What may appear to be an ordinary supplier, customer or payment arrangement can therefore have consequences that extend far beyond price, quality, delivery and conventional contractual performance.

For procurement, supply chain, finance, and commercial professionals, sanctions compliance has become part of responsible trading rather than a specialist issue reserved for banks, exporters, or legal teams. Understanding who owns and controls a counterparty, where products originate and are destined, how payments are routed, and whether restricted parties benefit from a transaction is increasingly fundamental to effective due diligence and sound commercial decision-making.

The difficulty lies in the complexity. UK sanctions can affect individuals, companies, ships, financial transactions, technology, services, imports, exports and transport arrangements, while ownership and control rules can extend restrictions beyond names appearing on official lists. International organisations must also navigate overlapping UK, EU and US requirements, differing licensing regimes and financial institutions whose risk appetite may be more restrictive than the law itself.

Effective sanctions compliance is therefore less about memorising prohibited names and more about understanding commercial relationships in sufficient depth to recognise exposure before it becomes a problem. Strong governance, proportionate due diligence, informed professional judgement, and clear escalation processes enable organisations to trade confidently while safeguarding legal compliance, financial resilience, and reputation. In an increasingly fragmented trading environment, understanding who sits behind a transaction has become as important as understanding the transaction itself.

Introduction – Trading With Risk

Sanctions have moved from a specialist legal concern to a mainstream commercial risk. A procurement team buying software, engineering components, freight, professional services, or finance can now encounter restrictions due to ownership structures, banks, shipping routes, or end-users. The scale is substantial: UK public procurement is about £400 billion annually, while UK goods and services trade totalled £1.868 trillion in 2025. Sanctions therefore sit directly inside everyday purchasing and supply-chain decisions.

The financial consequences can be significant even where the underlying transaction appears routine. In 2024, more than £37.079 billion in assets were reported frozen under UK financial sanctions, including £22.518 billion under the Russia regime and £12.955 billion under the Libya regime. By May 2025, assets frozen in connection with Russia since February 2022 had reached £28.678 billion, illustrating how sanctions can reshape access to capital, property, payments and commercial relationships.

Recent enforcement shows that sanctions risk is not theoretical. In September 2026, the Office of Financial Sanctions Implementation (OFSI) published a £4.733 million penalty against Citibank's London branch. Earlier cases included £1.001 million against Sabre Global Technologies, £465,000 against Herbert Smith Freehills CIS LLP Moscow, £390,000 against Apple Distribution International and £160,000 against Bank of Scotland. The common lesson is that sophisticated organisations can still fail when screening, escalation, ownership analysis or payment controls are inadequate.

For supply chain and procurement professionals, the practical issue is broader than checking a name against a list. Organisations must understand who owns or controls counterparties, where goods will ultimately travel, which banks and intermediaries will touch a payment, whether services are restricted, and whether licences are required. The commercial exposure includes contract failure, blocked payments, delayed shipments, stranded inventory, regulatory investigation and reputational damage, all of which can arise before any court determines criminal liability.

This article addresses the practical questions that matter to procurement, finance and supply-chain teams: which UK authorities administer sanctions, what ownership and control actually catches, how civil and criminal liability differ, and why licences, due diligence and voluntary disclosure influence enforcement outcomes. It also examines how UK, EU and US regimes interact, and why banks and counterparties often apply standards stricter than the law itself requires.

Why Sanctions Have Become a Supply Chain Issue

The expansion of sanctions following Russia's 2022 invasion of Ukraine transformed compliance into a supply-chain discipline. In 2021, the UK imported £9.142 billion of goods from Russia and exported £3.179 billion. By 2025, goods imports had fallen to £81 million and exports to £542 million. Those reductions reflect far more than the loss of bilateral trade: companies have had to replace inputs, redesign routes, re-screen distributors, and verify that third-country customers are not facilitating diversion.

Modern sanctions increasingly target goods, technology and services that move through complex networks rather than directly between the UK and a sanctioned country. UK guidance warns that circumvention can involve third-country intermediaries, re-export hubs, freight forwarders and opaque corporate structures. The Office of Trade Sanctions Implementation (OTSI) now analyses trade flows to identify higher-risk diversion routes and goods, including items beyond the G7 Common High Priority List, making end-use verification and distributor due diligence central supply-chain controls.

That matters because an apparently compliant first-tier supplier can still expose the buyer through its owners, subcontractors, customers or logistics partners. A manufacturer may lawfully sell to a distributor in one country yet face risk if the goods are subsequently diverted *to Russia. A professional services business may be caught by a services prohibition even if no physical product crosses a border. Sanctions due diligence therefore resembles supply-chain mapping: visibility beyond Tier 1 becomes legally important.*

The public sector faces the same exposure at scale. UK public procurement was approximately £407 billion in 2023/24, around one third of public-sector spending. Procurement Policy Note 007 also instructs specified contracting authorities to consider how they can further cut ties with companies backed by Russia and Belarus. Sanctions screening therefore interacts with supplier selection, national security assessment, contract management, and subcontractor oversight, rather than operating as a separate finance or legal compliance exercise.

What Are Economic Sanctions?

Economic sanctions are legally binding restrictions used to limit specified economic activity in pursuit of foreign-policy, national-security or international objectives. UK measures can include asset freezes, prohibitions on making funds or economic resources available, restrictions on financial services, trade bans, arms embargoes, investment restrictions and controls on particular professional or business services. Separate sanctions can also restrict travel, aircraft, shipping, and company directorships, so "sanctions" refers to a toolkit rather than a single prohibition.

Financial sanctions commonly focus on designated persons and entities they own or control. An asset freeze generally prevents dealing in frozen funds or economic resources. It can prohibit making such funds or resources available, directly or indirectly, to or for the benefit of a designated person. This is why screening only the contracting company's name is insufficient: ownership and control can extend restrictions to an unlisted entity, depending on the applicable regulations and facts.

Trade sanctions operate differently. They can prohibit the export, supply, delivery, making available or transfer of specified goods and technology, as well as related technical assistance, financial services, brokering or other ancillary services. Under the Russian regime, serious trade-sanctions breaches can carry up to 10 years' imprisonment on indictment, a fine, or both. Civil trade penalties can also reach the greater of £1 million or 50% of the estimated breach value.

Why Governments Use Sanctions

Governments use sanctions because they offer coercive and signalling options short of armed force while allowing pressure to be targeted at states, organisations, sectors, vessels or individuals. The UK describes its approach as "deter, disrupt and demonstrate": deter future malign activity, disrupt activity already occurring and demonstrate willingness to defend international norms. Sanctions can restrict access to finance, technology, markets, and services while preserving diplomatic space and, when carefully designed, limiting wider humanitarian harm.

The statutory purposes are broader than those related to warfare. Under the Sanctions and Anti-Money Laundering Act 2018, sanctions regulations may support UN or other international obligations, prevent terrorism, protect national security, maintain international peace and security, promote conflict resolution and civilian protection, deter gross human-rights violations, support international humanitarian law, counter weapons proliferation, promote democracy and good governance, or further another foreign-policy objective. Ministers must identify the purpose when making regulations.

Russia illustrates the economic leverage governments seek. Before the full-scale invasion of Ukraine, Russia was a material UK energy supplier: in 2021, the UK imported £5.2 billion of Russian fuel, including £3.0 billion of refined oil, which accounted for 24.1% of UK refined oil imports. By 2025, total UK goods imports from Russia had fallen to £81 million. Sanctions, import bans and commercial withdrawal collectively forced significant sourcing substitution *within a few years.*

Sanctions also communicate standards to domestic markets. The Procurement Act 2023, which commenced in February 2025, introduced stronger national-security exclusion and debarment mechanisms across covered public procurement. Contracting authorities must assess relevant suppliers, associated persons and intended subcontractors where national-security grounds are engaged. Although procurement exclusions and sanctions are legally distinct regimes, they increasingly operate in the same risk environment: government buying, investment controls, trade restrictions, and financial sanctions all reinforce economic security policy.

The Government's toolkit for economic security continues to expand beyond sanctions. The National Security (State Threats) Act 2026, which received Royal Assent on 8 July 2026, allows the Home Secretary to designate bodies involved in foreign power threat activity and creates new offences for supporting or benefiting from a designated body, carrying penalties of up to 14 years' imprisonment. Although separate from sanctions, it demonstrates the same direction of travel: an expanding perimeter of restricted counterparties that procurement teams must screen against.

The UK's Sanctions Framework

The modern UK framework rests principally on the Sanctions and Anti-Money Laundering Act 2018, commonly called SAMLA, together with regime-specific regulations made under it. These regulations translate policy objectives into enforceable prohibitions, exceptions, licensing grounds, reporting duties and enforcement powers. Regimes can be geographic, such as Russia, Belarus or Iran, or thematic, such as Global Human Rights, Global Anti-Corruption and cyber sanctions, enabling the Government to target both territories and types of conduct.

The framework is deliberately multi-agency because different sanctions regulate different forms of activity. The Foreign, Commonwealth & Development Office (FCDO) leads overall sanctions policy and most designations; HM Treasury and OFSI implement financial sanctions; the Department for Business and Trade implements trade sanctions through OTSI, the Export Control Joint Unit (ECJU) and import-control functions; His Majesty's Revenue and Customs (HMRC) enforces customs-related trade sanctions; the Department for Transport handles transport sanctions; the Home Office implements travel bans; and criminal financial-sanctions cases may involve the National Crime Agency and police.

The UK Sanctions List is now the single official source for UK sanctions designations, following the closure of OFSI's former Consolidated List on 28 January 2026. The scale remains large. At the end of 2024/25, the then-consolidated list contained 3,750 individuals, 968 entities, and 15 ships, for a total of 4,733 entries. Russia accounted for 2,113 designations, or 44.6% of the total, underscoring the screening workload facing regulated businesses and international supply chains.

The regime is dynamic rather than static. During 2026 alone, the UK Sanctions List was repeatedly amended across Russia, Iran, Sudan, cyber, chemical-weapons, Afghanistan, Libya, Global Human Rights and Global Anti-Corruption regimes. That pace matters operationally: screening completed at onboarding can become obsolete over the course of a multi-year contract. Organisations therefore need event-driven re-screening, contractual information rights, and escalation processes that respond when a counterparty, beneficial owner, vessel, bank, or jurisdiction becomes restricted.

Enforcement increasingly complements designation. Excluding counter-terrorism cases, OFSI recorded 394 suspected financial-sanctions breach cases in 2024/25 and had 240 active cases by April 2025. Financial services accounted for 142 recorded cases, legal services 46, cryptoassets 40, insurance 17, housing 11, professional services 11 and manufacturing eight. The distribution is important: sanctions exposure is demonstrably cross-sector, reaching property and housing organisations as well as banks, exporters and multinational *corporations.*

The number of regimes illustrates the framework's breadth. By the end of the Brexit transition period, the Government had laid secondary legislation under SAMLA for more than 35 sanctions regimes, replicating the effect of former EU measures without adopting identical wording. Regimes are added, merged or repealed as policy needs change; the Sanctions (EU Exit) (Miscellaneous Amendments) Regulations 2026 alone amended provisions across 11 regimes when it took effect on 13 May 2026.

The Sanctions and Anti-Money Laundering Act 2018

SAMLA was enacted to preserve the UK's ability to implement UN sanctions and pursue autonomous sanctions after withdrawal from the European Union. Part 1 provides the framework for creating sanctions regimes, designations, reviews, exceptions, licences, information powers and enforcement. Part 2 addresses anti-money-laundering and counter-terrorist-financing regulation. The Act therefore supplies the enabling architecture, while most day-to-day commercial prohibitions are found in secondary regulations made for individual sanctions regimes.

Section 1 permits the Secretary of State or Treasury, as appropriate, to make sanctions regulations for defined purposes. Where regulations are not simply implementing UN or other international obligations, section 2 requires the Minister to determine that there are good reasons to pursue the stated purpose and that sanctions are a reasonable course of action. This embeds purpose and proportionality into the statutory design rather than giving government an unrestricted power to impose economic restrictions.

SAMLA also enables regulations to include enforcement provisions, such as criminal offences and anti-circumvention measures. The Act permits sanctions regulations to apply to persons in the UK and UK persons abroad. It allows relevant provisions to be extended to British Overseas Territories and Crown Dependencies by Order in Council. That architecture explains why an overseas transaction can remain subject to UK sanctions even when neither the goods nor the counterparty is physically located in Britain.

UK Sanctions Authorities – Policy, Licensing and Enforcement

No single authority administers every UK sanction. Responsibility is distributed across departments according to the activity being regulated, including policy, designation, financial restrictions, trade controls, customs enforcement, transport measures and immigration sanctions. This reflects the specialist nature of the regime: freezing assets requires different expertise from licensing controlled technology or stopping a sanctioned vessel. Businesses must therefore identify the relevant prohibition before determining which authority's guidance, licence or enforcement process applies.

The Foreign, Commonwealth & Development Office sits at the centre of sanctions policy. It develops geographic and thematic regimes, works with other departments on implementation and is responsible for most designations. HM Treasury has a particular role in domestic counter-terrorism designations, while the Office of Financial Sanctions Implementation, within Treasury, administers financial sanctions. Since January 2026, designation information has been consolidated in the UK Sanctions List, replacing the previous need to reconcile separate lists.

OFSI issues financial sanctions guidance and licences, receives reports, investigates suspected breaches, and can impose civil monetary penalties. In 2024/25 it recorded 394 suspected breach cases and issued 57 enforcement actions. Its published penalties have included £465,000 against HSF Moscow, £390,000 against Apple Distribution International, £1.001 million against Sabre Global Technologies, and £4.733 million against Citibank's London branch, demonstrating that financial sanctions enforcement now extends well beyond traditional banking activity.

The Department for Business and Trade leads implementation of trade sanctions, principally *through the Office of Trade Sanctions Implementation and the Export Control Joint Unit. OTSI was launched in October 2024 and, during 2025/26, received 178 suspected-breach reports or referrals, including 156 connected with Russia. It closed 104 cases, referred 40 to HMRC, handled 169 stakeholder queries and delivered more than 60 engagement events across affected sectors.*

OTSI also plays an important licensing role. In 2025/26, it received 51 licence applications, including 12 from medical and pharmaceutical businesses, 11 from legal services, and 7 from food production and distribution. Of the 39 applications closed, 17 were granted, 8 required no licence, and 2 were refused. Average completion time was 96 working days, with a median of 89, underscoring the need to consider licensing during sourcing and contract planning rather than immediately before shipment.

HMRC remains central where trade sanctions intersect with customs and criminal enforcement. It investigates suspected breaches, can pursue criminal cases and may resolve appropriate matters through compound settlements, including £1.161 million with an unnamed UK exporter in 2025 and £569,157 with Petrofac Facilities Management in 2026. ECJU, meanwhile, licenses strategically controlled sanctioned goods, software and technology, while OTSI handles relevant non-strategic sanctioned items and services, meaning some transactions can require multiple approvals.

Who Must Comply With UK Sanctions?

UK sanctions apply to every individual, business or organisation undertaking relevant activity within the UK or its territorial sea. They also apply worldwide to UK nationals and to legal entities incorporated or constituted under UK law, including their branches. The rules are not limited to banks, defence contractors or listed companies. Public authorities, housing providers, charities, universities, professional services businesses, manufacturers, logistics businesses and small suppliers can all incur sanctions obligations through ordinary commercial activity.

The obligation is particularly important for organisations that believe their domestic focus makes sanctions remote. OFSI's 2024/25 case data included 11 suspected breaches in housing, 8 in manufacturing, 10 involving NGOs or charities, and 11 in professional services. Integral Concierge Services, a UK property management company, was fined £15,000 for 26 payments made to a designated person for services provided. The case illustrates how property maintenance and routine supplier payments can become matters of sanctions.

Compliance also extends beyond direct counterparties. Asset freezes may capture entities owned or controlled by designated persons, while trade restrictions can apply to end-users, destinations, services and indirect supply. Organisations therefore need proportionate due diligence covering beneficial ownership, control, end use, intermediaries, banks, freight routes, and subcontractors. A simple "sanctions clause" in a contract is useful risk allocation, but it does not replace screening, investigation or the operational ability to stop performance when facts change.

Certain sectors have additional reporting duties. OFSI imposes reporting obligations on specified "relevant firms", while OTSI requires certain financial, legal and money-service businesses to report suspected trade-sanctions breaches in defined circumstances. OTSI received 111 mandatory reports during 2025/26, representing 62% of its 178 cases received. For procurement and contract management, this means sanctions governance must include escalation and recordkeeping: discovering a concern can itself activate a legal reporting obligation, not merely an internal review.

The Territorial Reach of UK Sanctions

The territorial reach of UK sanctions is intentionally broad. Sanctions regulations apply to conduct in the United Kingdom and its territorial sea, regardless of nationality, and to UK nationals and UK-incorporated or constituted entities wherever they operate. A UK company *cannot avoid its obligations simply by executing a transaction through an overseas branch. Equally, a foreign company can enter UK jurisdiction when relevant conduct occurs in Britain or otherwise creates a sufficient UK nexus.*

OFSI explains that a UK nexus may arise through a UK company operating overseas, UK clearing services, activity directed from the UK, an overseas subsidiary subject to UK governance, or financial products and insurance bought on UK markets. These are examples, not automatic rules, and each case is fact-specific. The practical consequence is that transaction architecture matters: payment routing, decision-making location and group governance can be as significant as the contracting parties' registered addresses.

Apple Distribution International demonstrates this principle. The Irish-incorporated Apple subsidiary was fined £390,000 in March 2026 after it instructed a UK-based bank to make two payments totalling £635,618.75 to a company owned by a designated person. OFSI treated the relevant conduct as occurring in the UK. The case is particularly important for multinational supply chains because it shows that non-UK incorporation does not eliminate exposure when a transaction engages with UK-based financial infrastructure.

Territorial reach also explains why sanctions compliance must be designed at the group and transaction levels rather than at the country level alone. UK persons working abroad, overseas branches of UK entities, non-UK counterparties using UK services and transactions directed from Britain may all create exposure. Procurement teams should map the entire transaction: parties, ownership, end users, goods and services, banks, currencies, routes, and decision-makers. Sanctions risk follows economic activity, not merely the purchase order address.

For multinational groups, that means local-law compliance is only one layer of control. A foreign subsidiary may not itself be a UK person. Yet, instructions from a UK parent, use of UK banking infrastructure or conduct occurring in Britain can create a UK nexus. Conversely, UK entities remain subject to UK sanctions abroad. Effective governance, therefore, requires group policies, escalation routes, and responsibility for resolving conflicts among overlapping UK, US, EU, and local sanctions regimes.

The Different Types of UK Sanctions

UK sanctions are not a single form of restriction. Government guidance identifies five principal categories: financial sanctions, director disqualification sanctions, trade sanctions, transport sanctions affecting aircraft and shipping, and immigration sanctions or travel bans. A particular regime may combine several measures against the same target. Russia demonstrates the breadth of its toolkit, combining asset freezes, securities and lending restrictions, trade controls, trust-services restrictions, transport measures, and targeted prohibitions on specific financial activities.

Financial sanctions range from targeted asset freezes to restrictions affecting investment, capital markets, loans, correspondent banking, payment processing and financial services. Their scope can therefore extend far beyond money already held in a frozen account. At the end of the 2024 frozen-asset review, more than £37.079 billion was reported frozen under UK financial sanctions, including £22.518 billion under the Russia regime and £12.955 billion under the Libya regime.

Trade sanctions regulate goods, technology and services rather than merely counterparties. They can prohibit the export, supply, delivery, transfer, import, acquisition, provision of technical assistance, brokering, or financing of specified activities. Russia currently demonstrates its depth, with restrictions covering areas such as military goods, aviation, energy, oil refining, luxury goods, iron and steel, metals, gold, diamonds, uranium, software, and professional services. Compliance, therefore, requires analysis of commodity, destination, end-use, and customer together.

Transport and immigration measures complete the main framework. Transport sanctions can prevent specified ships from entering ports or Russian aircraft from entering UK airspace. In *contrast, travel bans can prevent designated individuals from entering or remaining in the United Kingdom. Some newer Russia designations also carry director-disqualification, trust-services, correspondent-banking or internet-services sanctions. The practical lesson is that procurement teams must identify the sanctions that are actually imposed, rather than assuming that every listed target is subject to identical restrictions.*

The UK Sanctions List

Since 28 January 2026, the UK Sanctions List has been the single official source for all UK sanctions designations, replacing OFSI's former Consolidated List of Asset Freeze Targets. Maintained by the FCDO, it identifies designated individuals and entities and specified ships, the regime under which action was taken, the sanctions imposed, identifying information and the Government's statement of reasons where applicable. It is available in searchable and downloadable data formats.

The change matters operationally because screening systems built around the OFSI list had to migrate to the UK Sanctions List. The list can be searched by name, address, and identifier, and filtered by regime, designation type, date, source, and sanctions imposed. Its search service warns that reliance on search results does not remove the obligation to conduct due diligence, reflecting risks created by aliases, transliteration, incomplete identifiers and entities owned or controlled by listed persons.

The scale of screening is substantial and continually changing. At the end of 2024/25, the predecessor Consolidated List contained 4,733 entries: 3,750 individuals, 968 entities and 15 ships. Russia alone accounted for 2,113 designations, or 44.6% of the total as of 5 April 2025. Those figures are historical snapshots rather than current totals: additions, amendments and delistings continue, so periodic onboarding checks are insufficient for long-running contracts.

Designated Persons – Individuals, Organisations and Ships

A designated person is an individual or entity made subject to specified sanctions under the relevant regulations. Entities can include companies, partnerships, bodies, organisations or associations, depending on the statutory wording. The UK Sanctions List records the sanctions attached to each designation, as a designation does not automatically mean that every possible restriction applies. Procurement and finance teams should therefore establish both identity and the precise sanctions imposed before deciding whether activity can lawfully proceed.

Ships require slightly different terminology. Government guidance distinguishes "designated persons" from "specified ships", although both can appear on the UK Sanctions List. A ship may be specified for transport sanctions, potentially restricting port access, registration or movement, and maritime transactions may separately engage financial or trade controls. This distinction matters to charterers, insurers, commodity traders and freight purchasers because screening a vessel involves more than checking the registered owner's corporate name.

Designation information can include aliases, former names, dates of birth, nationalities, addresses, identification numbers and other details intended to distinguish the target from innocent parties with similar names. The current UK Sanctions List search tool also offers fuzzy searching. However, screening technology is only a starting point: a close match must be investigated, and a clean name search cannot establish that an unlisted company is free from ownership or control by a designated person.

The commercial implications extend into procurement databases, supplier onboarding and contract management. Sanctions status can change after award, and the relevant person may be a parent company, a beneficial owner, a bank, a subcontractor, or a logistics provider rather than the named supplier. In 2024/25 alone, 191 new Russia-related designations were added to the former consolidated list, comprising 74 individuals and 117 entities. Effective controls, therefore, require re-screening when ownership, payment routes, or geopolitical circumstances change.

Financial Sanctions – What Do They Restrict?

Financial sanctions are designed to restrict access to funds, economic resources, markets and financial services. Their most familiar form is an asset freeze, but UK regimes can also restrict dealing in transferable securities or money-market instruments, loans and credit, correspondent banking, payment processing, investments, trust services, insurance, brokering and other financial assistance. The precise restrictions vary across regimes, making transaction-level legal analysis necessary when activity goes beyond a straightforward frozen-account scenario.

Russia provides a clear example of sectoral financial restrictions. The regulations restrict dealings in transferable securities and money-market instruments and prohibit particular new loans or credit arrangements. They also allow prohibitions on correspondent banking and payment processing to be imposed on designated institutions and entities they own or control. These measures can disrupt treasury operations even when neither contracting party is asset-frozen, because the prohibited activity may relate to the financing structure rather than to ownership of the underlying goods.

More recent cases reinforce that point. In September 2026, Citibank's London branch received a £4,732,830.58 penalty for making funds available for the benefit of designated persons under the Russia and Global Anti-Corruption regimes. OFSI's public enforcement record now spans banking, technology, legal services, property, manufacturing and fintech. Financial sanctions are therefore an enterprise-wide control issue involving procurement, accounts payable, treasury, legal, compliance and operational teams rather than solely regulated financial institutions.

Asset Freezes – Funds and Economic Resources

An asset freeze does not confiscate property or transfer ownership to the Government. Instead, the person holding or controlling relevant assets must freeze them and generally must not deal with funds or economic resources belonging to, owned, held or controlled by a designated person, unless an exception or licence applies. The same restrictions can extend to entities owned or controlled by that person. OFSI must also be informed, where applicable, when reporting obligations are triggered.

"Funds" is deliberately broad. OFSI guidance includes cash, cheques, bank deposits, debts, shares, bonds, derivatives, interest, dividends, credit, guarantees, performance bonds, letters of credit and other financial instruments. "Economic resources" means assets that are not funds but can be used to obtain funds, goods or services, potentially including property, vehicles, precious metals, stones and antiques. Cryptoassets can also fall within the statutory concepts of funds or economic resources.

The numbers illustrate the practical significance. OFSI's 2024 frozen-asset review recorded £37,079,363,495.69 of assets frozen under UK sanctions, up from £24.421 billion reported in the preceding review. Russia represented £22.518 billion and Libya £12.955 billion. These totals include assets in the UK and certain assets overseas subject to UK sanctions legislation. For commercial organisations, freezing therefore concerns far more than bank balances: physical and intangible assets can also require controls.

Property demonstrates how asset freezes extend beyond bank balances. Since 2022, Transparency International UK has identified UK real estate connected to sanctioned Russian nationals worth hundreds of millions of pounds, including a Kensington mansion linked to Roman Abramovich and Highgate's Witanhurst, London's second-largest house. Analysts have also found dozens of properties worth some £700 million that had not been publicly flagged as restricted, despite reported links to sanctioned individuals and apparent connections to designated persons, illustrating gaps in the public visibility and implementation of asset freezes.

Making Funds or Economic Resources Available

Asset-freeze rules operate in both directions: organisations must not unlawfully deal with frozen assets, but they must also avoid making new funds or economic resources available, directly or indirectly, to a designated person. Funds can include obvious payments as well as credit and other financial benefits. Economic resources are broader still, potentially capturing property, vehicles, commodities, and access to systems or services that can be exchanged or used to obtain funds, goods, or services.

The prohibition on making resources available "for the benefit of" a designated person is equally important. OFSI explains that this can arise where the designated person obtains, or can obtain, a significant financial benefit. Financial benefit includes discharging all or part of an obligation for which that person is responsible. Paying a third party can therefore create sanctions exposure if the economic effect is to satisfy a designated person's liability or benefit them.

Wise Payments illustrates that modest value does not eliminate legal exposure. OFSI's 2023 disclosure concerned a £250 cash withdrawal from a business account held by a company owned or controlled by a designated person. OFSI did not impose a monetary penalty, but concluded that Wise had made funds available in breach of the Russia Regulations. The case also highlighted the importance of sanctions screening and alert capability outside normal weekday operating patterns.

Non-cash benefits can be equally problematic. In 2022, OFSI imposed a £30,000 penalty on Hong Kong International Wine and Spirits Competition Limited after it received funds and economic resources from a designated person and made economic resources available without a licence. OFSI has cited that case to explain that publicity may constitute an economic resource. This is commercially significant because marketing exposure, software access, consultancy and other services may have measurable economic utility.

Sabre Global Technologies provides a more recent example of technology. OFSI imposed a £1,000,920.59 penalty in May 2026 after finding that the UK company made funds and an economic resource available to the designated Russian airline Ural Airlines and circumvented prohibitions. OFSI said services continued for several months after potential breaches were identified and alternative payment routes were tested. The case demonstrates why continued performance, not simply receipt of money, can create sanctions exposure.

Direct and Indirect Provision of Funds

The word "indirectly" prevents sanctions from being avoided through intermediaries. A payment need not move straight from a UK buyer to a designated person to be prohibited. Routing value through an agent, subsidiary, distributor, bank or other intermediary may still amount to making funds available if the designated person ultimately receives them. Procurement teams therefore need visibility into payment chains and beneficiaries, particularly when suppliers request unusual accounts, currencies, jurisdictions, or last-minute changes.

Indirect provision also interacts with ownership and control. Making funds available to an unlisted entity owned or controlled by a designated person may be subject to the same restrictions as payments to the listed person. This is why beneficial-ownership analysis is fundamental to sanctions compliance. A supplier's certificate that it is "not sanctioned" answers only part of the question; the buyer must consider whether a sanctioned person stands behind, controls or financially benefits from the organisation.

Deutsche Bank AG London Branch illustrates how apparently routine processing can create liability. OFSI imposed a £165,000 penalty in May 2026 for making funds available to a designated person without a licence under the Russia Regulations. The case sits alongside Apple Distribution International's £390,000 penalty and other payment cases. Collectively, they demonstrate that automated systems, established banking relationships and ordinary processing procedures do not displace the requirement to identify sanctions exposure before value is released.

Controls should therefore follow the complete transaction rather than merely the invoice. Organisations should establish who is paying, who receives the money, which banks process it, who ultimately benefits and whether any owner or controller is designated. Changes to remittance instructions deserve particular scrutiny. Where legitimate activity would otherwise breach a prohibition, an applicable statutory exception or appropriate licence must be identified before performance; commercial urgency cannot retrospectively legalise a prohibited payment.

Prohibited Financial Transactions and Services

Some financial sanctions prohibit particular transactions irrespective of a conventional asset freeze. Under the Russia regime, restrictions include certain transferable securities and money-market instruments, loans and credit, correspondent banking, payment processing, investments and trust services. A UK credit or financial institution can be prohibited from establishing or continuing correspondent relationships with specified designated institutions and from processing payments to, from or through them, including relevant owned or controlled institutions.

Trust-services restrictions show how sanctions reach professional structures. Russian measures can prohibit the creation of trusts or similar arrangements, the supply of registered, business, correspondence, or administrative addresses, the operation or management of trusts, the acting as a trustee or arranging trustees, and the acting as a nominee shareholder for prohibited beneficiaries. Such measures affect lawyers, accountants, corporate service providers, banks, and family offices. Procurement of financial and professional services, therefore, requires sanctions scrutiny even where no controlled physical goods are involved.

Standard Chartered remains a useful benchmark for the cost of financial-sanctions failure: its £20.47 million 2020 OFSI penalty is still far larger than most subsequent UK financial-sanctions penalties. More importantly, the enforcement principle remains current. OFSI states that restrictions vary between regimes and that businesses must understand the exact legislative prohibition. Controls should therefore classify the proposed activity—payment, lending, investment, insurance, trust service or security transaction—before deciding what screening and licensing steps are required.

Trade Sanctions – Imports, Exports and Restricted Goods

Trade sanctions restrict the movement, supply and acquisition of specified goods, technology and services. Depending on the regime, prohibitions can cover export, supply, delivery, making goods available, transfer of technology, import, acquisition, technical assistance, financial services and brokering. They may operate by commodity code, product description, destination, origin, end-user or intended use. Correct tariff classification is therefore necessary but not sufficient: businesses must also understand the origin, ownership, destination, and end use.

The Russian regime demonstrates the breadth now encountered by supply chains. Restricted categories include military and dual-use items, aviation and space goods, maritime technology, energy equipment, oil-refining goods, luxury goods, iron and steel, metals, revenue-generating goods, oil, coal, LNG, gold, diamonds, uranium, vulnerable goods, sectoral software and specified professional services. Some bans also capture goods processed in third countries using Russian-origin inputs, making supplier declarations and evidence of origin increasingly important.

Enforcement is becoming more visible. During 2025/26, HMRC reported 58 seizures of sanctioned goods, 18 warning letters arising from voluntary disclosures and three positive charging decisions across two cases awaiting trial. OTSI separately received 178 suspected trade-sanctions breach reports or referrals, of which 156 related to Russia. Those figures show that trade restrictions are being tested not only through licensing systems but also through border interventions, civil assessments, settlements, and potential criminal prosecutions.

For procurement, trade sanctions can create both inbound and outbound risk. A UK buyer may breach restrictions by acquiring prohibited Russian-origin goods, while a supplier can breach them by exporting controlled products or related services. The safest approach is transactional: classify goods, establish origin and destination, identify counterparties and end-users, map intermediaries, check applicable schedules and confirm licensing requirements before commitment. A purchase order cannot override sanctions legislation, and contractual indemnities cannot legalise prohibited trade.

Import Restrictions and Country of Origin

Import restrictions are often triggered not simply by where goods are shipped from, but by where they originated, were located or were consigned. Under the Russia regime, different prohibitions use different connecting factors, so a container arriving from Turkey, India or the UAE may still contain prohibited Russian-origin goods. Procurement teams therefore need evidence of origin and supply-chain history, rather than treating the exporter's country or invoice address as decisive.

Country-of-origin controls are particularly visible in iron and steel. Since 30 September 2023, specified iron and steel products processed in third countries can be prohibited where they incorporate listed Russian-origin inputs. Government guidance gives the example of Russian steel slabs transformed abroad into alloy-steel coils: subsequent processing may change the conventional customs origin, yet the UK sanctions prohibition can still apply because the product incorporates qualifying Russian material.

The evidential burden consequently extends well beyond a supplier declaration. Government guidance identifies mill test certificates, certificates of origin, invoices, bills of lading and CMR transport documents as possible evidence, together with information on processing countries and facilities. Importers should retain verifiable records because HMRC may request documentation retrospectively. From May 2026, Russia restrictions also expanded to include uranium and certain oil products processed in third countries, further increasing origin-tracing requirements.

The commercial effect can be substantial. UK goods imports from Russia fell from £9.142 billion in 2021 to only £81 million in 2025, but sanctions exposure has not disappeared with direct trade. Third-country processing, transhipment and indirect acquisition can preserve a Russian connection after goods have travelled through several jurisdictions. Effective sourcing therefore requires origin verification at the material level where regulations demand it, especially for metals, diamonds, energy products, and other sanctioned categories.

Diamonds illustrate how origin verification is becoming increasingly rigorous. Since January 2024, G7 measures have progressively restricted imports of non-industrial diamonds of Russian origin, including certain stones processed in third countries. UK importers must therefore be able to demonstrate supply chain history and non-Russian origin using reliable evidence, such as Kimberley Process documentation, invoices, certificates of origin, G7 verification certificates, and other provenance records. A simple country-of-origin declaration on an invoice may no longer provide sufficient assurance.

Export Restrictions – Destination, End User and End Use

Export sanctions require businesses to look beyond the immediate destination. Under the Russia Regulations, several categories of sanctioned goods are prohibited not only when exported directly to Russia but also when exported "for use in" Russia. A shipment to Kazakhstan, Türkiye, or another third country can therefore remain prohibited if the goods are ultimately intended for use in Russia. Destination screening must consequently include the ultimate country, end-user and foreseeable onward movement.

The end-user question has become central because Russia has relied on third-country procurement networks, indirect shipping routes and false end-use descriptions to obtain Western technology. UK guidance recommends examining whether the customer's *commercial rationale is credible, whether volumes or prices fit normal trade patterns, whether intermediaries obscure the actual user and whether the customer resists providing documentation. Contractual non-reexport clauses can strengthen controls, but they do not replace investigation of credible diversion risks.*

HMRC's £1,160,725.67 compound settlement announced in 2025 provides a clear example. A UK exporter made sanctioned goods available to Russia through activity involving a third country, prompting HMRC to warn that Russian companies operating outside Russia can still be subject to UK prohibitions. Sanctions End-Use Controls, which took effect on 13 May 2026, close a related gap: once Government formally notifies an exporter of a diversion risk, a licence becomes mandatory even though the exporter itself is not designated and the goods are not otherwise export-controlled.

Technology, Technical Assistance, Brokering and Services

Trade sanctions can reach knowledge, software and services as readily as physical goods. Under the Russia Regulations, "technical assistance" includes technical support relating to repair, development, production, assembly, testing, use or maintenance, together with other technical services relating to sanctioned goods or technology. A UK engineer can therefore create exposure without shipping anything: remote troubleshooting, design support, software configuration or maintenance advice may be prohibited where the relevant sanctions conditions are met.

Technology restrictions are similarly broader than handing over a physical drawing. Strategic export-control guidance expressly treats software, data, information and technical assistance as potentially controlled. At the same time, sanctions legislation can prohibit the transfer of specified technology to Russia, to persons connected with Russia, or for use there. Cloud delivery, email attachments, shared repositories and remote system access therefore require the same destination and end-user scrutiny as tangible exports when controlled or sanctioned technical information is involved.

Brokering closes another potential route around direct supply restrictions. Russia regulation 21 defines brokering services broadly to include selecting or introducing parties, negotiating arrangements, facilitating entry into arrangements and providing assistance that promotes or facilitates them. A UK intermediary may consequently face restrictions even where goods never enter Britain. This is particularly relevant to procurement consultancies, commodity traders, agents, and group companies that coordinate transactions between suppliers and customers located entirely overseas.

Standalone services can also be prohibited. Current Russian measures cover categories including accounting, advertising, architecture, auditing, business and management consulting, construction, engineering, IT consultancy and design, public relations, and specified legal advisory services. Since 27 April 2026, OTSI has licensed sanctioned goods and technology not subject to strategic export controls, as well as associated ancillary services and standalone sanctioned services, while ECJU retains responsibility for items that are also subject to strategic export controls.

Petrofac Facilities Management Limited demonstrates the operational risk. In June 2026, HMRC publicly named the company after it paid a £569,157 compound settlement for breaches of Russia sanctions while winding down its Russian operations in 2022 and 2023. HMRC said Petrofac supplied sanctioned industrial goods to persons connected with Russia and provided related technical assistance. The case shows that servicing legacy equipment during market exit can remain prohibited even after new sales have stopped.

Transport and Shipping Sanctions

Transport sanctions can restrict ships and aircraft independently of ordinary trade prohibitions. Under the Russian regime, specified ships and certain Russian ships can be barred from UK ports, detained, directed to move or remain in place, prevented from UK registration, and *prohibited from being chartered or operated. Separate trade measures can also prohibit technical assistance, crew, operating, chartering, brokering and financial services connected with specified vessels, making maritime compliance a multi-layered exercise.*

The scale has grown rapidly. By July 2026, the UK Government stated that more than 600 vessels had been specified under the Russia sanctions regime, including more than 580 oil tankers. These measures target the "shadow fleet" used to transport Russian oil through opaque ownership, flagging, insurance and operating arrangements. Vessel screening must therefore cover IMO numbers, current and former names, flags, owners, operators, charterers and relevant service providers, not simply the ship's displayed name.

The significance of the enforcement became tangible on 14 June 2026, when Royal Marines and National Crime Agency officers boarded the sanctioned tanker SMYRTOS in the English Channel, marking the first UK-led interdiction of a Russian shadow-fleet vessel. OFSI had issued a general licence permitting necessary steps and related payments for interdiction activity. The episode shows sanctions moving beyond financial blocking into physical disruption of transport assets considered to support Russia's war economy.

Transport restrictions do not automatically prohibit every ship carrying cargo to or from Russia. Government guidance states that shipping sanctions generally bite where a vessel falls within the relevant Russian-ship definition or is specifically listed. Separate cargo, oil price cap, financial, or trade rules may nevertheless apply. Logistics teams must therefore assess vessel status and cargo legality separately; a lawful commodity cannot make a prohibited vessel lawful, and an unsanctioned vessel cannot legitimise prohibited cargo.

Sanctions and Export Controls – Related but Different

Sanctions and export controls overlap, but they are not the same legal regime. Strategic export controls regulate sensitive military, dual-use, and other specified items principally under the Export Control Act 2002, the Export Control Order 2008, and applicable dual-use legislation. Sanctions derive principally from SAMLA and regime-specific regulations. An item may therefore be strategically controlled, sanctioned because of destination, both, or neither, and each classification can produce a separate licensing requirement.

The administrative split reflects that distinction. ECJU licenses the export, transfer, and making available of sanctioned goods, software, or technology that are also subject to strategic export controls. Since 27 April 2026, OTSI has handled licensing for sanctioned goods and technology not strategically controlled, together with related ancillary and standalone services. OFSI may need to license a payment involving frozen funds separately. One transaction can therefore require permissions from more than one authority.

Compliance teams should resist treating an export-control licence as a universal clearance certificate. OFSI expressly warns that its financial-sanctions licences address only its own area of competence, and the same transaction may require an export or trade-sanctions licence. Conversely, an item absent from strategic control lists can still be sanctioned because of its destination or end use. The correct workflow is cumulative: classify the item, assess destination and parties, analyse sanctions, then identify every licence needed.

Ownership and Control – Why the Sanctions List Is Only the Starting Point

The UK Sanctions List is indispensable, but it is only the first stage of financial-sanctions due diligence. OFSI states that asset freezes and certain financial-services restrictions can extend to entities owned or controlled, directly or indirectly, by a designated person even when those entities are not separately listed. A clean list search, therefore, does not establish that a supplier, customer, parent company, or intermediary is outside sanctions if the ownership-and-control criteria are nevertheless satisfied.

The current test contains three principal routes. A designated person may hold, directly or indirectly, more than 50% of shares or voting rights; possess the right to appoint or remove a majority of directors; or be able, considering all circumstances, to ensure that the entity's *affairs are conducted in accordance with that person's wishes. The third route makes control fact-sensitive and prevents formal minority ownership from becoming an automatic safe harbour.*

OFSI's 2026 call for evidence acknowledged the practical difficulty. Financial- and legal-sector respondents reported uncertainty, compliance costs, litigation risk, and inconsistent interpretations, particularly regarding a designated person's ability to exercise "hypothetical control". The Government described the control limb as deliberately broad because sanctions could otherwise be circumvented through trusts, proxies, multi-jurisdictional chains, or opaque arrangements. The consultation therefore highlights why sanctions ownership analysis is a substantive investigation rather than a database exercise.

The courts have also exposed the complexity. In Mints v PJSC National Bank Trust, the Court of Appeal considered arguments that designated officials, including President Putin, controlled Russian state-linked claimants. Later, in Litasco SA v Der Mond Oil and Gas Africa SA, the Commercial Court rejected an argument that President Putin controlled the private company merely because state power could, in theory, be exercised over it, stressing the need for evidence of relevant influence.

For procurement professionals, the practical response is proportionate corporate mapping. Screening should identify direct shareholders, intermediate holding companies, voting rights, board appointment powers, trusts, nominees, and credible indicators of influence. Higher-risk suppliers may require constitutional documents, registers, shareholder agreements or independent corporate intelligence. The objective is not to prove every negative worldwide, but to establish a defensible, documented basis for concluding whether designated persons own or control the counterparty at the time of transaction.

The 50% Ownership Test

The expression "50% ownership test" is convenient shorthand but slightly misleading under current UK financial-sanctions rules. The statutory threshold is more than 50% of shares or voting rights, held directly or indirectly; exactly 50% does not satisfy that ownership limb by itself. A designated person holding 50% may nevertheless control the company through voting arrangements, director appointment rights, or other forms of influence, so procurement teams should never treat a 50% shareholding as automatically clear.

The UK position also differs from some international approaches. In February 2026, OFSI stated that Government was exploring possible alignment with partners by changing the rule to "50% or more" and considering an aggregation model, but no such change had been implemented by 5 September 2026. Cross-border groups therefore cannot safely apply US or EU assumptions mechanically to UK sanctions analysis; jurisdiction-specific ownership calculations remain necessary.

Separate designated persons' minority holdings are not ordinarily added together simply because their combined interests exceed 50%. OFSI states that aggregation may become relevant where shares or rights are jointly held, subject to a joint arrangement, or one designated person controls another's rights. Thus, two unrelated designated persons holding 30% each do not automatically make a company owned under the UK test, although separate control analysis may still produce a different conclusion.

The threshold should also be distinguished from Companies House's PSC regime. A person with significant control is generally reportable if they hold more than 25% of the shares or voting rights, can appoint or remove a majority of the directors, or otherwise exercise significant influence or control. A 30% shareholder may therefore appear as a PSC without making the company sanctions-owned. Conversely, sanctions control may arise through influence even where formal ownership is below both headline thresholds.

Indirect Ownership Through Corporate Structures

Indirect ownership matters because sanctions cannot be avoided by inserting holding *companies between a designated person and an operating business. OFSI guidance expressly distinguishes between direct and indirect ownership. It gives a simple example of an unlisted company that is majority-owned by a designated entity: the unlisted company becomes subject to the same relevant financial restrictions. Procurement due diligence should therefore trace ownership upwards through intermediate entities rather than stopping at the immediate registered shareholder.*

Corporate chains can become difficult where ownership is dispersed across subsidiaries, trusts, nominees and multiple jurisdictions. The practical question is whether the designated person ultimately holds the required proprietary or voting interest, or otherwise controls the entity through the chain of control. Public registries may reveal only part of that picture, particularly where jurisdictions do not publish beneficial owners. Supplier questionnaires and warranties are useful, but higher-risk cases require corroboration from independent records and corporate documents.

Joint interests create an additional complication. OFSI states that where shares or rights are jointly held, each holder can be treated as owning those shares or rights; the same principle may apply to joint arrangements that require rights to be exercised jointly. This differs from ordinary non-aggregation of separate minority holdings. A procurement assessment should therefore identify shareholder agreements, voting pacts and nominee arrangements rather than calculating percentages solely from a static ownership chart.

Control Without Majority Ownership

Control can arise without majority ownership, which is why percentage screening alone is inadequate. OFSI identifies two non-ownership routes: the right to appoint or remove a majority of the board, and circumstances in which it is reasonable to expect that a designated person could ensure the entity's affairs are conducted in accordance with that person's wishes. Either can make financial sanctions applicable even where the designated person holds a minority shareholding.

The control limb is deliberately broad. OFSI's 2026 call for evidence describes "hypothetical control" as the ability of a designated person, if they chose, to achieve the relevant result, even where evidence shows that power has not actually been exercised. Government says this protects against circumvention through proxies, trusts and opaque structures, but it also acknowledges industry concerns about uncertainty, risk and the cost of investigating influence that may be informal or difficult to evidence.

English case law has helped define the boundaries. In Mints, the Court of Appeal considered whether Russian state-linked entities could be controlled by designated public officials and observed that the statutory language was broad. The judgment prompted concern that state authority might be read expansively. However, subsequent cases have emphasised the factual context and resisted treating the mere existence of governmental power over domestic companies as sufficient evidence of sanctions control.

Litasco SA v Der Mond Oil and Gas Africa SA is particularly useful. The Commercial Court held that there was no arguable evidence showing President Putin presently exercised the relevant de facto control over Litasco, a private company, notwithstanding the Russian state's wider coercive power. The court distinguished theoretical sovereign power from evidence that a company's relevant affairs were actually subject to a designated person's influence, narrowing an excessively literal reading of Mints.

Kevin Hellard v OJSC Rossiysky Kredit Bank added further structure in 2024 by discussing different forms of control, including legal, de facto, and potential control. OFSI expressly drew on that typology in its 2026 consultation. For businesses, the message is practical: examine constitutional rights, board composition, financing dependencies, vetoes, personal relationships and documented directions, while avoiding unsupported assumptions based solely on nationality, political office or commercial prominence.

Beneficial Ownership and Ultimate Controllers

Beneficial ownership asks who ultimately owns, benefits from or controls an organisation beyond the legal name appearing on a contract. In the UK, Companies House's PSC framework generally identifies individuals holding more than 25% of shares or voting rights, persons able to appoint or remove a majority of directors, and those otherwise exercising significant influence or control. Those records are valuable due-diligence tools, but their statutory purpose and thresholds differ from sanctions ownership rules.

The Register of Overseas Entities adds another source of information on overseas entities that own UK land, requiring relevant beneficial-owner information to be provided to Companies House. Yet public registers are not complete sanctions solutions. Structures may involve trusts, nominee shareholders, foreign companies, contractual rights or jurisdictions with limited transparency. Procurement teams should combine registry evidence with constitutional documents, credible databases, sanctions screening and targeted questions whenever the ownership chain contains unexplained gaps or higher-risk jurisdictions.

The objective is to identify the real decision-makers and economic beneficiaries before money, goods, or services move. That means understanding who supplied the capital, who receives the distributions, who appoints the directors, who can veto decisions, and whether ownership changed after sanctions were imposed. For public and private procurement alike, documenting that analysis strengthens both compliance and auditability. A transparent supplier structure lowers uncertainty; unexplained complexity, nominee layers or sudden restructuring should increase scrutiny rather than end it.

Front Companies, Nominees and Proxy Arrangements

Front companies are a recognised sanctions-evasion technique because they allow a restricted buyer, beneficial owner or end-user to sit behind an apparently ordinary trading entity. UK Government guidance identifies warning signs, including recently created companies, residential or shared addresses, limited trading history, complicated intermediaries, layered letters of credit, and ownership changes around the date sanctions were imposed. None proves wrongdoing alone, but combinations justify enhanced investigation before goods, services or funds move.

Nominees and proxies can create similar opacity. A nominee shareholder may hold legal title while voting or receiving dividends according to another person's instructions, while an intermediary may contract or pay on behalf of the true beneficiary. Russia sanctions specifically regulate certain trust and nominee-shareholder services. Procurement teams should therefore identify who directs the transaction, supplies funds, exercises voting rights and receives economic benefit, rather than relying solely on the name printed on incorporation records.

The UK's 2026 counter-evasion guidance gives practical red flags for front companies. These include customers whose products do not match their business, companies sharing premises with numerous comparable traders, offshore structures linked to higher-risk jurisdictions and buyers reluctant to disclose end-users. The FCA has observed comparable behaviour in financial services, including sanctioned persons accessing services through relatives, complex ownership chains, intermediaries, correspondent banks, cryptoassets and e-money wallets designed to obscure underlying connections.

A useful commercial lesson is that evasion frequently looks ordinary until several anomalies are viewed together. A new distributor, an unusual payment bank, an altered delivery destination, and a refusal of installation support may each have innocent explanations; collectively, they can indicate diversion. Government guidance therefore recommends a holistic assessment rather than automatic rejection based on a single red flag. The strongest response is documented escalation, corroborated ownership and end-use evidence, and refusal to proceed where material uncertainty remains.

Licences and Exceptions – When Restricted Activity May Still Be Permitted

Sanctions are restrictive, but they are not designed to prevent every transaction involving a sanctioned person or activity. Legislation can contain exceptions that apply automatically where stated conditions are met, while licences can authorise conduct that would otherwise be prohibited. The distinction matters: an exception is part of the law and needs no application, whereas a licence is a permission granted under powers and must be followed exactly, including any reporting, recordkeeping or timing conditions.

General licences permit defined classes of activity without each user obtaining an individual approval. OFSI issues general licences for financial sanctions, while the Department for Business and Trade issues general trade licences. They can be amended, revoked or allowed to expire, so reliance must be checked at the time of performance. Individual licences are case-specific and normally require the applicant to show that a statutory licensing ground or relevant licensing consideration is satisfied.

Typical financial-sanctions licensing grounds include basic needs, legal fees, maintenance of frozen assets, prior obligations, extraordinary expenses, humanitarian assistance, insolvency and divestment. However, the availability of these grounds varies by regime. Since April 2026, OTSI has licensed sanctioned goods and technology that are not subject to strategic export controls, along with associated services, while ECJU retains relevant strategically controlled items. A licence from one authority does not automatically satisfy the restrictions imposed by another so that transactions may require multiple approvals.

Chelsea Football Club remains a striking example of licensing preserving legitimate activity without releasing sanctions pressure. After Roman Abramovich was designated in March 2022, Chelsea and its parent, Fordstam, were treated as subject to an asset freeze. OFSI issued a general licence allowing fixtures, staff wages and defined operating expenses to continue. The government later licensed the sale, while more than £2.5 billion of proceeds remained frozen in a UK account so Abramovich could not benefit.

Licensing should therefore be treated as a controlled exception, not a commercial workaround. An organisation should identify the exact prohibition, confirm whether a statutory exception applies, examine current general licences and, if necessary, apply to the competent authority before acting. Licence conditions should then be embedded into purchase orders, payment controls and operational instructions. Exceeding a value cap, failing to meet a reporting condition, or continuing after expiry can turn otherwise permitted activity back into a breach.

Strict Liability and the Changing Enforcement Environment

The enforcement environment changed fundamentally on 15 June 2022, when reforms under the Economic Crime (Transparency and Enforcement) Act 2022 allowed OFSI to impose civil monetary penalties for breaches of financial sanctions without having to prove that the person knew, or had reasonable cause to suspect, that the conduct breached sanctions. OFSI must still prove the underlying breach on the civil standard, but ignorance is no longer a threshold defence to civil liability for financial sanctions.

Trade, aircraft and shipping sanctions have followed the same direction. Under the Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, OTSI and the Department for Transport can generally assess breaches on a strict-liability basis. Government's March 2026 enforcement strategy confirms that OFSI, OTSI and DfT apply the civil standard of the balance of probabilities, while circumvention offences remain different because intent is required. Knowledge can nevertheless aggravate the enforcement outcome.

Strict liability does not mean every mistake attracts maximum penalty. Enforcement bodies consider seriousness, harm, culpability, compliance systems, cooperation, previous history and remediation when selecting outcomes. Government guidance identifies robust systems and prompt remedial action as mitigating factors, while deliberate conduct, concealment and inadequate controls can aggravate a case. The practical consequence is sharper *accountability: an organisation may be civilly liable despite innocent ignorance, yet the quality of its compliance response can materially affect sanction.*

Civil Penalties, Criminal Offences and Other Consequences

Civil sanctions penalties can be financially substantial. The current statutory maximum for financial and trade sanctions is the greater of £1 million or 50% of the value of the breach; for aircraft and shipping sanctions, the ceiling is the greater of £1 million or 50% of the relevant aircraft or ship's estimated value. Government has proposed increasing OFSI's financial-sanctions maximum to £2 million or 100%, but legislation is still required.

Criminal exposure is separate and depends on the offence and applicable regulations. Under the Russian regime, breaches of the principal financial prohibitions can carry up to seven years' imprisonment on indictment. In comparison, principal trade-sanctions offences can carry up to ten years' imprisonment, alongside unlimited fines. Licensing, reporting and information offences can attract different penalties. OFSI, OTSI, or other authorities may also refer cases to law enforcement where the conduct is serious, deliberate, repeated, or evasive.

Consequences extend beyond fines and imprisonment. The Government's enforcement framework includes warning letters, public disclosure, referral to regulators or professional bodies, detention of transport assets, and, where relevant, immigration action. Financial-sanctions offences can also fall within the Deferred Prosecution Agreement regime for organisations. Commercially, enforcement may trigger banking restrictions, insurer concerns, procurement exclusion questions, contractual termination and reputational damage, meaning the total economic impact can considerably exceed the value of the prohibited transaction itself.

Criminal prosecutions remain rare in practice. In April 2025, Dmitrii Ovsyannikov, Russia's former Governor of Sevastopol, became the principal defendant in the UK's first successful prosecution for breaches of Russia-linked financial sanctions, receiving 40 months' imprisonment for eight offences and money laundering; his brother received a suspended sentence for enabling the breaches. A second prosecution, of a British shipping financier previously reported as linked to Lukoil-related tanker acquisitions, who was subsequently charged with an alleged sanctions breach and money laundering, followed in April 2026, signalling the NCA's growing appetite for enabler cases.

Does Lack of Knowledge Provide a Defence?

In civil financial sanctions enforcement, lack of knowledge is not a complete defence. Since 15 June 2022, OFSI may impose a monetary penalty without proving that the person knew or had reasonable cause to suspect that the conduct breached sanctions. The same broad strict-liability approach now applies to most trade, aircraft and shipping civil enforcement. An organisation can therefore face civil action even where the breach arose from mistaken screening, incomplete information or an overlooked restriction.

That position must not be confused with criminal liability. Many sanctions offences retain knowledge, suspicion, reasonable-cause or intent elements specified in the relevant regulations, and circumvention offences particularly depend on intentional conduct. OFSI's 2026 enforcement guidance expressly states that the strict civil-liability amendment is not relevant to deciding whether a criminal offence has been committed. The exact wording of the applicable regulation, therefore, matters when determining personal or corporate criminal exposure.

Actual knowledge is, in fact, the more demanding state of awareness, since it requires genuine knowledge that conduct breached sanctions. "Reasonable cause to suspect" is a lower, objective threshold that does not require actual knowledge: OFSI describes it as asking whether factual circumstances existed from which an honest, reasonable person should have inferred knowledge or formed a suspicion. Deliberately avoiding inconvenient information is therefore dangerous, since ignoring obvious questions about ownership, destination or *payment routes offers no protection.*

Although ignorance does not erase strict civil liability, the reasons for failure remain relevant to enforcement. Government guidance lists robust systems, prompt disclosure, cooperation, clean history and swift remediation as mitigating factors. Conversely, negligence, recklessness, deliberate behaviour, concealment and inadequate systems can aggravate the outcome. This distinction is commercially important: "we did not know" may fail as a legal defence. At the same time, evidence showing why the organisation reasonably missed the issue can still affect the severity of the penalty.

The practical objective is therefore not to create an impossible guarantee that no breach will ever occur. It is to build controls proportionate to exposure and capable of detecting warning signs before performance issues arise. Screening, ownership analysis, contractual warranties, end-use checks, escalation routes and documented decisions demonstrate that sanctions risk was actively managed. When facts remain uncertain, pausing a transaction and obtaining specialist advice is safer than relying on absence of knowledge as permission to proceed.

Due Diligence as Evidence of Responsible Compliance

Due diligence does not create a statutory safe harbour, but it can become powerful evidence of responsible compliance. OFSI states that, where an incorrect ownership-and-control assessment contributed to a breach, it will examine the extent and quality of the research undertaken. Appropriate due diligence can mitigate enforcement where the conclusion was reached in good faith and was reasonable on the information available. OTSI likewise treats proportionate customer due diligence and compliance systems as potential mitigating factors.

Good sanctions due diligence is risk-based rather than mechanical. It should combine sanctions-list screening with ownership and control analysis, jurisdictional risk, product classification, destination, end-use, payment routes and intermediary review. Government guidance recommends checking customer information against public sources and proceeding cautiously when reliable information on the ultimate beneficial owner cannot be established. Higher-risk transactions may justify enhanced questionnaires, corporate records, independent intelligence and contractual obligations restricting onward transfer, re-export or dealings with designated persons.

Bank of Scotland's £160,000 OFSI penalty illustrates why controls must work in practice, not merely exist on paper. OFSI said the banking group had sanctions screening in place, yet its automated systems failed to detect a spelling variation of a designated individual's name. OFSI also highlighted weaknesses concerning escalation and training. Lloyds Banking Group nevertheless notified OFSI within two weeks of identifying the potential breach, demonstrating how detection and disclosure remain important after preventive controls fail.

The FCA's 2026 review reinforces that lesson. Since February 2022, it has assessed sanctions systems and controls at more than 150 supervised businesses, finding weaknesses in due diligence, screening, alert management, frozen assets and licence compliance. Effective practice included granular risk assessments, documented escalation, monitoring and quality assurance. For procurement organisations, the equivalent is a traceable audit trail showing what was checked, when, against which sources, by whom and why the resulting decision was reasonable.

Voluntary Disclosure, Cooperation and Remediation

Voluntary disclosure can materially affect enforcement, although it does not erase the breach. Under OFSI's February 2026 framework, prompt voluntary disclosure, combined with proactive cooperation, can attract a discount of up to 30% on the baseline monetary penalty. Eligible subjects may also obtain up to 20% through the Early Account Scheme and 20% through settlement. OFSI states that applicable discounts are added before being applied, creating a strong incentive for early, constructive engagement.

OTSI uses a different structure for trade-sanctions cases. Prompt and comprehensive *voluntary disclosure can reduce a monetary penalty by up to 50% in low- and medium-severity cases and up to 30% in high-severity cases. OTSI also considers cooperation, good due diligence, prior compliance history, and steps to address the causes of the breach. Remediation, therefore, means more than stopping a single transaction: organisations should identify root causes, preserve records, strengthen controls, and test whether similar failures have occurred elsewhere.*

Recent enforcement shows the value of prompt reporting. Apple Distribution International voluntarily disclosed the transactions that led to OFSI's £390,000 penalty in March 2026, yet the underlying conduct was still penalised. The lesson is not that self-reporting guarantees leniency, but that voluntary disclosure sits alongside seriousness, harm and culpability in OFSI's assessment: delay, incomplete disclosure or obstruction can forfeit mitigation entirely, heightening regulatory concern once authorities eventually discover the underlying conduct themselves.

UK, EU and US Sanctions – Why International Businesses Face Additional Complexity

International businesses face complexity because UK, EU and US sanctions often pursue similar policy objectives through different legal mechanisms. A multinational transaction may involve a UK contracting entity, an EU subsidiary, a US-dollar payment, an American employee and goods moving through several jurisdictions. Compliance must therefore be analysed on a jurisdiction-by-jurisdiction basis. A licence, exemption or favourable ownership conclusion under one regime does not automatically authorise the same activity under another authority's rules.

Ownership rules provide a clear example. The UK applies a "more than 50%" ownership threshold and ordinarily does not aggregate minority interests of unrelated designated persons unless joint arrangements or comparable control exists. OFAC's US rule blocks entities owned, directly or indirectly, in the aggregate by 50% or more by one or more blocked persons. OFAC's 50 Per cent Rule concerns ownership, not control, although controlled entities may be designated separately, and transactions involving blocked individuals can remain prohibited.

EU practice differs again. European Commission guidance treats an entity as owned where one or more listed persons hold 50% or more in aggregate, while EU asset-freeze analysis also considers control. EU sanctions bind persons within EU territory, EU nationals wherever located and entities incorporated under Member-State law, including their overseas activity. Enforcement remains principally with Member States. A UK group with European operations can therefore face parallel obligations even after Brexit.

The United States adds further complexity through OFAC programme rules, US-person obligations, property-blocking concepts and the role of US financial infrastructure. HM Treasury and OFSI published a dedicated US-UK comparative guide in June 2026, covering differences in sanctions lists, licensing, ownership rules, reporting and recordkeeping. Its existence is instructive in itself: close political coordination between allies does not yield identical legal tests, and multinational compliance cannot be reduced to applying the strictest-looking list to every transaction.

For businesses, the safest model is a sanctions matrix that identifies relevant jurisdictions, entities, employees, banks, currencies, products, and licences. Where regimes overlap, controls should satisfy each applicable requirement rather than assume equivalence. Contracts should anticipate divergence, because one jurisdiction may designate a counterparty sooner, licence activity differently or impose broader restrictions. Sanctions clauses that merely require compliance with "applicable law" are useful, but operational teams still need procedures for determining which laws are applicable.

Why Banks and Other Businesses May Go Further Than the Law Requires

Banks and commercial counterparties can adopt risk appetites more conservative than the *minimum sanctions prohibition. A transaction may therefore be permissible yet be declined because a bank, insurer, freight provider or supplier considers the ownership structure, jurisdiction, commodity or payment route too risky. FCDO guidance expressly warns third-country businesses that international banks and suppliers may withdraw services where they fear sanctioned dealings or diversion, even when those businesses are not themselves designated.*

Several forces drive this caution. Financial institutions must manage sanctions, anti-money-laundering, proliferation-financing, fraud and correspondent-banking risks simultaneously, often across multiple jurisdictions. A bank processing a modest payment may face an investigation, frozen funds, regulatory scrutiny, and substantial operational expenses if the transaction later proves problematic. Commercial systems therefore use internal country restrictions, sector limits, enhanced due diligence and approval thresholds that can exceed the black-letter legal minimum. Those controls are risk-management decisions, not additional sanctions legislation.

The FCA recognises this phenomenon as de-risking, including the withdrawal from customer categories or correspondent banking relationships. Its guidance also states that effective risk management does not necessarily require wholesale de-risking. The balance is important: businesses should assess customers individually and proportionately, rather than assume that every connection to a higher-risk country is prohibited. Nevertheless, a customer cannot compel a private institution to accept sanctions exposure merely because the customer believes a transaction falls outside a statutory prohibition.

Contractual and banking feasibility should therefore be tested before commitment. A supplier may hold a valid licence yet discover that its bank will not process the payment, its insurer excludes the route, or a logistics provider refuses carriage. Procurement teams should identify critical financial and transport dependencies early, seek alternative lawful arrangements where appropriate, and avoid promising delivery dates or payment mechanisms until the organisations required for execution have agreed to participate.

Summary – Understanding the Risk Before Trading

Sanctions risk begins before a contract is signed and continues until goods, services and payments have been fully completed. The UK framework now combines designation screening, ownership and control rules, financial restrictions, trade controls, transport measures, licensing requirements and strict civil enforcement. More than £37 billion of assets were reported frozen in the 2024 review, while hundreds of suspected breaches are assessed annually. Sanctions compliance has therefore become a mainstream discipline across procurement, finance, and supply chain.

The central lesson is that a clean sanctions-list search is only the beginning. Organisations must understand who ultimately owns and controls counterparties, where products originated and where they will end up, who will use them, which services are being supplied, and how money will travel. They must also distinguish exceptions from licences and UK rules from EU or US requirements. Each additional intermediary, jurisdiction or opaque ownership layer increases the need for evidence rather than assumption.

Strong compliance is ultimately a decision-making system. Risk assessments, proportionate due diligence, transaction screening, contractual protections, staff training, escalation, records, licensing controls and prompt remediation should work together. Strict liability means a civil breach can exist without knowledge, but regulators still distinguish between responsible organisations that made a reasonable, documented mistake and those that ignored warning signs. Understanding the risk before trading therefore protects legality, continuity, banking access, public reputation and long-term commercial resilience.

Additional articles can be found at [Procurement and Supply Chain Management Made Simple]. This site looks at procurement and supply chain management issues to assist organisations and people in increasing the quality, efficiency, and effectiveness of their product and service *supply to the customers' delight.*

Further Reading

The following official guidance, legislation and regulatory publications were consulted in the preparation of this article and provide authoritative further reading for procurement, finance and compliance professionals.

- *HM Treasury and Office of Financial Sanctions Implementation, “UK Financial Sanctions: General Guidance”, gov.uk.*
- *HM Treasury and Office of Financial Sanctions Implementation, “OFSI Annual Review 2024–25: Effective Sanctions”, October 2025.*
- *HM Treasury and Office of Financial Sanctions Implementation, “Monetary Penalties for Breaches of Financial Sanctions: Guidance”, gov.uk.*
- *Department for Business and Trade, “Sanctions End-Use Controls: Guidance for Businesses”, gov.uk.*
- *Financial Conduct Authority, “Sanctions Systems and Controls in Our Firms: Our Findings”, 28 May 2026.*
- *Sanctions and Anti-Money Laundering Act 2018, legislation.gov.uk.*
- *Foreign, Commonwealth & Development Office, UK Sanctions List, gov.uk.*
- *Cabinet Office, “Procurement Policy Note 007: Contracts with Suppliers from Russia and Belarus”, originally issued August 2022, updated February 2025.*
- *HM Treasury and Office of Financial Sanctions Implementation, “UK and US Financial Sanctions: A Comparative Guide”, June 2026.*