

# ***Beyond the Supplier – Sanctions Due Diligence Across the Supply Chain***



***Procurement and Supply Chain Management Made Simple.***

## **Foreword – The Supplier You Know May Not Be the Party Creating the Risk**

*Sanctions risk rarely sits neatly with the organisation named on the contract. A supplier may appear legitimate, pass routine screening and operate from a low-risk jurisdiction, yet still be connected to restricted ownership, sanctioned banks, sensitive goods, opaque intermediaries or prohibited end users. The modern procurement challenge is therefore not simply to know the supplier, but to understand the wider commercial network through which goods, services and money actually move.*

*That requires a different mindset from traditional supplier onboarding. Due diligence must increasingly look beyond Tier One and consider beneficial ownership, directors, subcontractors, agents, distributors, logistics providers, vessels, banks, origin, destination and end use. The objective is not to investigate every participant in every supply chain without limit. It is to follow identifiable risk far enough to establish whether the transaction remains lawful, commercially credible and reasonably understood.*

*This creates one of the most difficult questions in sanctions compliance: how far down the supply chain must a reasonable organisation investigate before it can say that adequate due diligence has been undertaken? There is no universally correct answer expressed as Tier Two, Tier Three or Tier Four. A proportionate investigation should deepen as risk increases and stop when credible concerns have been resolved, remaining uncertainty is understood, and the decision can be properly defended.*

*The distinction matters across both public and private procurement. Complex international sourcing, layered corporate structures, third-country trading routes and increasingly sophisticated attempts to circumvent sanctions can all place considerable distance between the buyer and the party ultimately creating the risk. Effective sanctions due diligence, therefore, depends on combining screening technology with commercial judgement, documentary evidence, ownership analysis, and an understanding of the wider transaction structure.*

*The most resilient organisations will not treat sanctions screening as a single compliance checkpoint completed before contract award. They will recognise that ownership changes, new banks, altered routes, different subcontractors and emerging designations can change the risk throughout the commercial relationship. Knowing the supplier remains essential, but it is no longer enough. Procurement must also be prepared to follow the money, trace the goods and understand the network behind the transaction.*

## **Introduction – Beyond Tier One**

Sanctions risk rarely stops at the legal entity named on a purchase order. A supplier may be legitimate in its own name while being owned, financed, supplied or controlled by parties subject to restrictions. Goods may also pass through several manufacturers, traders, banks and logistics providers before reaching the buyer. For procurement teams, understanding the transaction therefore means looking beyond Tier One and asking who, what and where sits behind it.

The scale of UK commercial exposure makes that task significant. The Government Commercial Function states that the public sector spends more than £400 billion each year on goods and services. OFSI's 2024 frozen-asset review recorded £37.08 billion subject to UK financial sanctions, while the FCA reported that the comparable figure had been £24.4 billion in 2023–24. Sanctions exposure therefore extends well beyond specialist financial institutions to ordinary purchasing, contracting, and supply-chain decisions.

Apple Distribution International illustrates the point. OFSI imposed a £390,000 penalty in March 2026 after two payments totalling £635,618.75 were made to Okko LLC, which was not itself the designated person but was wholly owned by designated JSC New Opportunities. The lesson is not that every supplier requires forensic investigation; it is that a clean name-screening result does not answer the more important question of who ultimately owns, controls or benefits from the transaction.

## **Why Supplier Screening Alone Is No Longer Enough**

Traditional supplier screening normally asks whether a counterparty's name appears on the UK Sanctions List. That remains essential, but it is only the starting point. UK financial sanctions can apply to entities owned or controlled by designated persons even where those entities are not individually listed. A procurement system that screens only the contracting company can therefore return a reassuring "no match" while the underlying transaction remains prohibited or exposes the organisation to sanctions risk.

The FCA's 2026 review of sanctions controls demonstrates the limits of automation. Among firms that make relevant regulatory returns, 70% reported automated screening and 81% reported repeat-customer screening. Yet FCA testing found that exact-name cases were identified more reliably than altered-name cases: 90% of alerts correctly identified the relevant sanctioned party when names matched exactly, compared with 75% when names appeared in slightly different forms. Screening quality, therefore, depends heavily on data, configuration, and judgement.

Supply-chain transactions also contain risks that a name-screening engine may never see. A legitimate distributor may purchase sensitive components from another country, use an intermediary bank, ship through a diversion hub or sell to an undisclosed end user. UK government guidance specifically warns about indirect shipping routes, falsified end-use information, and third-country intermediaries used to obtain restricted goods. These are transactional facts, not merely names that can be matched against a list.

Screening infrastructure is changing too. From 28 January 2026, the UK Sanctions List became the single official source for all UK sanctions designations, replacing the OFSI Consolidated List of Asset Freeze Targets. The move was designed to reduce duplication and the risk that firms screen against an outdated or incomplete source. Consolidation improves the raw material available to a screening system, but it does not substitute for testing what lies behind a clean result.

## **What Does Sanctions Due Diligence Mean?**

Sanctions due diligence is the process of gathering, testing and evaluating sufficient information to determine whether a proposed or continuing commercial relationship creates sanctions exposure. Depending on the transaction, that may include checks on designated persons, ownership and control, directors, beneficial owners, goods and services, banks,

vessels, origin, destination and end use. OFSI expressly recognises that there is no single level or type of due diligence appropriate to every business or circumstance.

The process therefore extends beyond simply searching a sanctions list. It requires an organisation to understand how the transaction is structured, who ultimately benefits from it, where goods and funds will move, and whether any intermediary changes the risk. A routine domestic purchase may justify limited enquiries, while sensitive goods, complex ownership or higher-risk jurisdictions may require deeper investigation. The appropriate scope should follow the facts rather than a predetermined checklist.

That distinction matters because due diligence is investigative rather than mechanical. Information supplied by a vendor should be corroborated where the risk justifies it, using corporate registers, ownership records, shipping data, trade documentation and reliable public information. FCDO guidance recommends checking ownership information against public sources and proceeding cautiously where reliable details of owners or ultimate beneficial owners cannot be established. The objective is not perfect knowledge, but a defensible understanding of sanctions risk.

### **The Difference Between Screening and Due Diligence**

Screening and due diligence are related controls, but they answer different questions. Screening asks whether a name, identifier or transaction feature matches information held on a sanctions or internal watchlist. Due diligence asks whether the commercial facts reveal a prohibited or higher-risk relationship even when no direct match exists. Screening is therefore a detection mechanism; due diligence is the broader process by which an organisation assesses ownership, control, geography, behaviour, and transactional context.

The FCA's findings illustrate the operational difference. Some firms could identify exact sanctioned names but struggled with variant spellings, non-Latin characters, missing dates of birth and ownership-and-control relationships. Other firms strengthened controls through vessel tracking, corporate structure analysis, and documentary review. A screening alert may initiate an investigation, but the absence of alerts cannot conclude it. Good compliance combines technology with corroboration, escalation and human assessment rather than treating software output as a legal opinion.

This matters particularly in procurement because the contracting supplier is only one data point. The same supplier may present low risk when delivering UK-manufactured stationery and materially higher risk when sourcing dual-use electronics through unfamiliar overseas intermediaries. The company name has not changed, but the risk has. Due diligence, therefore, examines the relationship among counterparty, product, jurisdiction, payment route, and destination, allowing the depth of investigation to vary as the underlying commercial facts change.

The FCA's May 2026 review of 150 authorised firms' sanctions systems and controls found the same pattern at scale. Firms had improved materially since 2022, yet significant gaps remained: 35% of breaches reported in 2025 concerned conduct that had occurred earlier, and most reports still involved Russia, though a growing share concerned Iran, North Korea and Libya. Improved technology had not closed the gap between detecting a breach and preventing one.

### **A Risk-Based Approach to Sanctions Compliance**

A risk-based approach starts from the proposition that sanctions controls should be proportionate to actual exposure. OFSI recognises that there is no one-size-fits-all due diligence model, while the FCA expects sanctions systems and controls to reflect the risks firms face. For procurement, this means avoiding two equally weak extremes: performing only superficial checks on every transaction, or attempting exhaustive investigation of every supplier regardless of value, geography, product or credible indicators of sanctions exposure.

Risk should be assessed cumulatively. A low-value purchase from a transparent UK

*manufacturer supplying ordinary goods may justify relatively limited enquiries. The same value spent on microelectronics routed through several trading companies may require significantly more scrutiny because the goods, intermediaries, and destination create different levels of exposure. Government circumvention guidance identifies military and dual-use goods, aerospace, automotive products, microelectronics, and heavy machinery as sectors where additional oversight is particularly important regarding diversion to Russia.*

*The approach also needs to respond to change. A supplier assessed as low risk in January may acquire a new shareholder, change its bank, route goods through another jurisdiction or appoint an unfamiliar distributor by June. Sanctions designations can also change rapidly. Effective risk management therefore combines proportionate onboarding checks with reassessment triggers, rather than treating due diligence as a certificate issued once and filed for the duration of a multi-year contract.*

*A risk-based model is equally relevant to public procurement. Government spends more than £400 billion across the public sector, and the Procurement Act 2023 framework requires contracting authorities to consider supplier-related exclusion and debarment risks. Guidance instructs authorities to check the debarment list for suppliers, associated persons and intended subcontractors. Sanctions analysis remains a separate legal exercise, but the policy direction is consistent: understand the parties behind delivery, not merely the name submitting the tender.*

### **Assessing Sanctions Risk Before Contracting**

*The strongest time to identify sanctions exposure is before commercial commitment, when procurement can still pause, investigate, or restructure the transaction. OTSI's 2025–26 annual review illustrates the scale of activity: it closed 104 enforcement cases during the year, including 40 referred to HMRC, while several active investigations were expected to reach decision points during 2026–27. Early assessment therefore reduces both legal exposure and costly contractual disruption.*

*A meaningful pre-contract review should establish what is being purchased, from whom, where the goods or services originate, how they will be delivered, who will receive payment, and whether another party ultimately benefits. It should also consider ownership, control, subcontractors, intermediaries, banks and intended end users where relevant. The purpose is to understand the complete commercial structure before obligations are created, rather than discovering material sanctions concerns after orders, payments or shipments have already begun.*

*Pre-contract assessment should also test whether the proposed transaction makes commercial sense. UK guidance identifies warning signs including products inconsistent with the customer's business, unclear end use, unusual routes, significant changes in volumes or prices, and documentation naming only an intermediary rather than the true end user. An unusually attractive price can therefore be a risk indicator rather than simply good procurement, particularly where other aspects of the transaction appear commercially abnormal.*

### **Country Risk, Sector Risk and Transaction Risk**

*Country risk asks where the supplier, owners, manufacturers, banks, goods and end users are located or connected. It should not be reduced to a single list of "high-risk countries": exposure can arise through neighbouring or intermediary jurisdictions where goods are re-exported. FCDO guidance specifically warns that Russia continues to obtain Western military, dual-use and other critical goods through third countries, using indirect shipping, false end-use information and professional networks designed to obscure the final destination.*

*Sector risk concerns what is being supplied and how it could support a sanctioned economy or designated party. UK counter-circumvention guidance highlights military and dual-use goods, aerospace, automotive, microelectronics, and heavy machinery, as well as items such*

as industrial machinery, navigation instruments, vehicle parts, pumps, turbojets, gas turbines, and semiconductor equipment. An organisation buying these categories may require deeper provenance and end-use checks than one purchasing ordinary domestic consumables, even where supplier values are comparable.

Transaction risk then asks whether the particular deal behaves as expected. Relevant indicators include unexplained third-party payments, a newly inserted intermediary, delivery to a freight forwarder rather than the customer, inconsistent invoices, unusual currencies or banks, sudden routing changes and reluctance to identify an end user. No single red flag proves evasion: UK government guidance expressly says indicators should be considered holistically. Their value lies in identifying when ordinary due diligence should become enhanced investigation.

Recent designations illustrate how country and sector risk interact in practice. On 24 February 2026, marking the fourth anniversary of the invasion, the UK designated 240 entities and 7 individuals, including three civil nuclear energy companies and 175 companies within the “2Rivers” shadow-fleet oil network, as well as 50 specified vessels. Energy, maritime, and nuclear-adjacent sectors therefore warrant closer country-risk scrutiny than a single sanctioned counterparty might otherwise suggest.

### **Supplier Onboarding – What Should Procurement Investigate?**

Supplier onboarding should establish a reliable commercial identity before screening begins. Procurement should obtain the legal name, registration number, registered and trading addresses, incorporation jurisdiction, key directors, ownership information and the bank account into which payments will be made. Those details should be checked against independent sources. A sanctions search against an inaccurate or abbreviated supplier name provides little assurance, particularly where aliases, transliteration or similarly named entities create scope for mistaken identification.

Ownership and control should then be examined to identify persons or entities that may bring the supplier within financial sanctions. For UK companies, Companies House can provide information on directors, persons with significant control, filing history, and corporate documents, but it should be treated as evidence rather than a complete sanctions conclusion. Overseas structures may require local registries, corporate databases, supplier declarations, or specialist research when ownership passes through holding companies, trusts, or opaque jurisdictions.

Procurement should also understand how the supplier intends to perform. That may require identifying critical subcontractors, manufacturing locations, logistics providers, distributors and, where relevant, the source of sensitive components. Public procurement guidance under the Procurement Act illustrates the wider direction of travel by requiring checks concerning associated persons and intended subcontractors in the debarment context. The same commercial discipline helps expose sanctions risks that would remain invisible if onboarding stopped with the prime contractor.

The file should record not only what was checked, but what was concluded and why. If a supplier operates entirely within the UK, has transparent ownership and provides low-risk goods, a concise record may be enough. If ownership is layered, goods are sensitive, or third-country routing is involved, the rationale should explain additional enquiries and escalation procedures. This audit trail matters if circumstances change or an enforcement authority asks what the organisation did before proceeding.

### **Verifying the Supplier’s Legal Identity**

Verifying legal identity means establishing that the organisation exists, that the entity entering the contract is the entity actually trading, and that the people acting for it have a credible connection to the business. At the end of June 2026, the Companies House register contained 5,516,377 companies, with 192,287 incorporations during the preceding quarter. That scale

*makes disciplined verification essential: a plausible company name, website, email address or invoice is not proof of legal identity.*

*Procurement should therefore corroborate core information through reliable sources before contracting. Relevant checks include the registered company name, company number, incorporation date, registered office, trading address, current status, directors, filing history and persons with significant control. Bank-account details and contractual documentation should also be consistent with the verified entity. Discrepancies, recently altered addresses, unexplained changes in directors, or documents issued under different company names should be investigated rather than treated as routine administrative errors.*

*The UK corporate register is being strengthened. Companies House began mandatory identity verification on 18 November 2025 under reforms introduced by the Economic Crime and Corporate Transparency Act 2023. New directors must verify their identity for incorporation or appointment, while existing directors and persons with significant control are being brought into the regime through transition arrangements. These reforms strengthen corporate transparency, but identity verification alone does not establish that a supplier or transaction is sanctions-compliant.*

### **Understanding Corporate Ownership Structures**

*Corporate ownership structures matter because UK financial sanctions can extend beyond the designated person named on the UK Sanctions List. Under the ownership and control rules, an entity may be caught where a designated person holds, directly or indirectly, more than 50% of its shares or voting rights, can appoint or remove a majority of its board, or can reasonably be expected to ensure that its affairs are conducted in accordance with that person's wishes.*

*The difficulty is rarely the first shareholder shown on a register; it is tracing the chain far enough to understand who ultimately owns or controls the entity. A supplier may be held by a domestic parent, then an overseas holding company, then another vehicle. Each layer can obscure the relevant person. UK guidance therefore expects reasonable, good-faith due diligence rather than reliance on whether the immediate supplier appears on the sanctions list by name.*

*Apple Distribution International's 2026 case provides a concrete example. The recipient, Okko LLC, was wholly owned by designated JSC New Opportunities, and OFSI concluded that two payments totalling £635,618.75 breached the Russia financial sanctions regime; the resulting penalty was £390,000. The case demonstrates the practical consequence of ownership analysis: certain financial sanctions, including asset-freeze restrictions, can extend to an unlisted company where the relevant ownership or control tests are satisfied.*

*Strict liability sharpens the stakes of getting ownership analysis wrong. Since 15 June 2022, OFSI has been able to impose civil monetary penalties for breaches of financial sanctions without proving that an organisation knew of or had reasonable cause to suspect the breach. Where a counterparty is owned or controlled by a designated person, an organisation cannot rely on ignorance as a defence, which makes ownership due diligence a control rather than an optional extra.*

### **Identifying Beneficial Owners**

*Beneficial ownership is where the visible corporate name begins to give way to the people behind it. Companies House describes a person with significant control, or PSC, as someone who owns or controls a company. UK companies generally report persons holding more than 25% of shares or voting rights, among other tests. Procurement should therefore use PSC information as an investigative starting point, not as a substitute for sanctions ownership analysis.*

*The thresholds are not identical. Under UK financial sanctions, an entity may be owned or controlled by a designated person where that person holds, directly or indirectly, more than*

50% of shares or voting rights, can appoint or remove a majority of the board, or can ensure that the entity's affairs are conducted according to their wishes. A 30% shareholder may therefore be a PSC without automatically satisfying the sanctions ownership limb.

Complex structures require analysis to continue through intermediate companies, trusts, and nominees until the relevant natural persons or controlling entities can be identified. Government guidance warns that sanctions circumvention networks may use shell companies, frequent changes in ownership and multiple management layers to conceal ultimate beneficial owners. Procurement should treat unexplained opacity, recent restructuring or an unwillingness to provide ownership information as reasons to investigate further rather than administrative inconvenience.

Identity verification strengthens the evidence available without eliminating the need for judgement. Compulsory Companies House identity verification for directors and PSCs began on 18 November 2025, and Companies House now publishes quarterly compliance data. That reform makes false or misused identities harder to sustain, but it does not establish whether a verified individual is designated, acting for another person, or exercising control through arrangements that do not appear neatly in the public share register.

### **Investigating Directors and Other Connected Parties**

Directors matter because formal share ownership does not reveal all the routes through which influence may be exercised. Procurement should consider directors, senior officers, authorised signatories and other persons materially involved in the relationship, particularly where they have links to designated persons or sanctioned jurisdictions. FCA guidance identifies weak customer due diligence that fails to reveal connected parties and corporate structures as poor practice, reinforcing the importance of understanding who actually directs commercial decisions.

A designated director does not automatically make every company they serve subject to an asset freeze. The question remains whether the applicable ownership or control tests are met, or whether funds or economic resources would otherwise be made available to or for that person's benefit. Nevertheless, board dominance, veto rights, family relationships, shared addresses, powers of attorney, or repeated instructions from an outside individual can provide evidence warranting closer examination of practical control.

This is where procurement records become surprisingly valuable. Tender contacts, negotiation behaviour, bank mandates, organisational charts and correspondence may reveal that the person apparently running a supplier differs from the individual shown as its principal owner. OFSI's 2026 call for evidence acknowledged industry difficulty in assessing "hypothetical control", particularly where a designated person can direct an entity even if available evidence does not show that power being exercised at the time.

### **Tier One Is Not the Whole Supply Chain**

Tier One is simply the organisation with which the buyer contracts; it is not necessarily where sanctions exposure originates. A UK distributor may obtain components from overseas manufacturers, appoint an agent, use a freight forwarder and pay through several financial institutions. None may appear as the purchase-order supplier, yet each can alter the sanctions analysis. Government guidance therefore encourages businesses to examine ownership, business partners, goods, routes, payments and end users where circumstances justify it.

This matters because sanctions risk can emerge several steps away from the contractual relationship. A supplier may be legitimate, while a sub-supplier may be owned by a designated person, a bank in the payment chain may be restricted, or goods may be shipped on a sanctioned vessel. Procurement needs enough visibility to identify which downstream or supporting parties are material to performance and compliance, rather than assuming responsibility ends with the name on the contract.

The problem is acute where restricted or sensitive goods can be diverted. UK guidance on

*Russian circumvention highlights indirect shipping routes, false end-use information, shell companies and third-country intermediaries. An apparently low-risk UK supplier may require deeper questions if its products originate in, pass through or are financed through higher-risk channels. The correct unit of analysis is the transaction and its commercial ecosystem, not simply the Tier One relationship at the top of the chain.*

*Public procurement illustrates the same discipline in a different legal register. Under the Procurement Act 2023, contracting authorities assessing exclusion and debarment grounds must check whether associated persons—including consortium partners or subcontractors relied on to satisfy conditions of participation—and intended subcontractors appear on the debarment list. However, a supplier must normally be given the chance to replace a subcontractor first. Tier One is no safer a stopping point in public contracts than in private ones.*

### **Mapping Subcontractors and Sub-Suppliers**

*Supply-chain mapping converts an abstract concern into a visible network. Procurement can begin by identifying which organisations actually manufacture, assemble, store, transport or materially contribute to the goods and services being purchased. The objective is not to demand an exhaustive family tree for every contract, but to understand the nodes that can create sanctions exposure. Critical subcontractors, sole-source manufacturers and entities handling controlled or high-risk goods should normally receive greater attention than incidental suppliers.*

*Public procurement already reflects a wider conception of supplier risk. Under section 28 of the Procurement Act 2023, contracting authorities must request details of intended subcontractors, while Cabinet Office guidance states that intended subcontractors of all tiers must be checked against the debarment list. These requirements concern exclusion and debarment rather than sanctions compliance, but they demonstrate that modern public procurement expressly recognises risk extending beyond the prime contracting entity.*

*The map should capture both geography and names. Manufacturing country, warehouse locations, export points, ports, freight routes, and destinations can expose risks that corporate screening may miss. UK sanctions-evasion guidance identifies abnormal or circuitous routing, unexplained changes in destination and goods inconsistent with a customer's business as potential warning signs. Mapping therefore connects corporate due diligence with physical supply chain evidence, making discrepancies easier for procurement, compliance, and logistics teams to identify.*

*A useful map also distinguishes criticality. A subcontractor providing routine packaging may create little sanctions exposure, while a specialist semiconductor producer or shipping company could be central to both performance and compliance. The buyer should therefore record why particular nodes were investigated and why others were not. That creates a proportionate audit trail and avoids the impossible expectation that every minor supplier, regardless of relevance, must receive the same level of scrutiny.*

### **How Far Down the Supply Chain Must Due Diligence Extend?**

*There is no universally correct number of tiers. OFSI expressly states that it does not prescribe a single level or type of due diligence; instead, it considers whether the work undertaken was appropriate to the sanctions risk, the transaction, and the commercial relationship. The practical question is therefore not whether every Tier Two or Tier Three supplier was screened, but whether a reasonable investigation followed the risk far enough to support the conclusion reached.*

*For ordinary domestic purchasing, that point may arrive quickly. A transparent UK manufacturer supplying standard office furniture from known UK facilities may present limited reasons to investigate every raw-material provider. By contrast, a distributor supplying advanced electronics manufactured abroad, routed through several intermediaries and paid*

*through unfamiliar banks presents multiple risk indicators. Applying the same due diligence to both transactions would conflate administrative consistency with risk management and could waste resources without improving compliance.*

*The investigation should deepen whenever new information creates a credible pathway to a restriction. That might be an opaque shareholder, a subcontractor in a higher-risk jurisdiction, a vessel linked to a designated party, an unexplained change in bank accounts, or evidence that goods are being re-exported. Each answer can close a line of enquiry or create another. The process therefore resembles tracing a risk pathway rather than mechanically descending a predetermined number of supply-chain levels.*

*This approach also aligns with OFSI's enforcement framework. When ownership or control is relevant to a breach, OFSI considers the degree and quality of research undertaken and whether the conclusion was reached in good faith. Appropriate due diligence may mitigate enforcement, while inadequate work may aggravate it. Crucially, OFSI expects evidence of a decision-making process showing that the organisation considered the sanctions risk and selected a proportionate level of investigation.*

*The consequence for procurement is practical: depth should be defensible, not infinite. A buyer should be able to explain which risks were identified, what evidence was obtained, what inconsistencies were resolved and why further investigation would not reasonably have changed the assessment. That standard cannot guarantee that hidden misconduct will never escape detection. It can, however, demonstrate that due diligence was structured, proportionate and responsive to the information reasonably available at the contracting stage.*

### **A Risk-Based Model for Determining Investigation Depth**

*A workable model can classify each transaction across four dimensions: counterparty, geography, product or service, and transactional behaviour. Low-risk results across all four may justify standard screening and identity checks. A material concern in any dimension should increase the depth of investigation; several concerns together should normally trigger enhanced due diligence. The model should be documented to show why a particular supplier received basic, intermediate, or enhanced scrutiny, rather than leaving the decision to intuition.*

*Counterparty risk includes ownership opacity, recent incorporation, unexplained changes in directors and nominees, links to designated persons, and reluctance to disclose beneficial ownership. Geographic risk considers incorporation, manufacturing, transit, banking and destination jurisdictions. Product risk rises where goods are controlled, dual-use, technologically sensitive or attractive for military-industrial purposes. Transaction risk considers unusual pricing, intermediaries, payment instructions, routing and commercial behaviour. These dimensions should be assessed together because combinations often reveal more than individual indicators.*

*A simple scoring system can help, provided it does not become a substitute for judgement. For example, an organisation might allocate increasing internal risk weights to sanctioned-country connections, opaque ownership, sensitive goods, third-country transit, and abnormal payment structures, with escalation thresholds that trigger specialist review. The numbers themselves have no legal status. Their value lies in producing consistent decisions and a record showing that relevant risk factors were identified before the contract was approved.*

*The model must also accommodate information quality. An apparently low-risk supplier supported only by incomplete or unverifiable records may warrant more scrutiny than a higher-value supplier whose ownership and supply chain are transparent. OFSI expects scrutiny of information obtained in ownership-and-control assessments, especially where arrangements appear designed to avoid thresholds. Confidence in the evidence should therefore influence the depth of the investigation, alongside the inherent risk posed by the transaction itself.*

### **When Is It Reasonable to Stop Investigating?**

*Due diligence can reasonably stop once identified sanctions risks have been investigated,*

*provided the remaining uncertainty is proportionate to the transaction, and no unresolved red flag reasonably demands further enquiry. This is not the same as proving that no hidden risk exists. Commercial organisations rarely possess investigative powers sufficient to establish every fact. The defensible standard is a reasonable, good-faith assessment based on appropriate evidence, not absolute certainty about an entire global supply network.*

*Stopping is easier to justify where ownership is transparent, independent sources corroborate supplier information, goods and routes fit the stated business purpose, payment arrangements are conventional and no material connection to designated persons has emerged. OFSI's enforcement guidance places the onus on the organisation seeking mitigation to demonstrate that its ownership-and-control due diligence was reasonable and appropriate. A short written conclusion can therefore be as important as retaining the underlying searches and documents.*

*The decision should remain reversible. OFSI states that ownership and control are not static and expects ongoing relationships to be reviewed at appropriate times. A buyer who paused onboarding may need to restart enquiries following a new designation, an ownership change, a bank account amendment, an unusual routing request, or an acquisition. "Reasonable to stop" should mean reasonable on the evidence and date recorded, not permanent clearance for every transaction made throughout a long-term contract.*

### **When Should Enhanced Due Diligence Begin?**

*Enhanced due diligence should begin when ordinary checks leave material uncertainty or reveal indicators that increase the probability or consequence of a sanctions breach. Triggers include opaque ownership, newly formed intermediaries, unexplained third-country routing, sensitive goods, designated-person connections, unusual payment requests or inconsistent end-use information. Government guidance also identifies sudden changes in trading patterns, quantities, prices, or counterparties as warning signs that may warrant a more detailed investigation before goods, services, or funds are released.*

*Enhanced work may involve obtaining full ownership charts, constitutional documents, shareholder agreements, source-of-funds information, end-user undertakings, export documentation, bills of lading or evidence explaining intermediary roles. Independent corporate research, vessel information and legal advice may also be appropriate. OFSI encourages organisations to conduct their own research, request further information and seek legal advice where necessary. The aim is targeted corroboration of the specific risk, rather than indiscriminately collecting more documents.*

*Refusal or inability to answer reasonable questions is itself information. UK guidance warns that circumvention structures may involve shell companies, opaque ties, and multiple layers of ownership. At the same time, payment red flags include shell-company wire transfers, circuitous financial flows and last-minute routing changes. Procurement should resist treating missing information as neutral. Where important facts cannot be established, the residual uncertainty may justify escalation, contractual safeguards, licensing analysis or a decision not to proceed.*

*The escalation process should identify who can approve continuation and what evidence they require. Higher-risk cases may need sanctions specialists, legal counsel, export-control expertise or senior management rather than unilateral procurement approval. This separation improves challenge and creates an auditable rationale. It also helps distinguish a genuinely difficult but lawful transaction from one in which the commercial participants repeatedly ask the buyer to accept unexplained opacity, unusual routing, or unsupported assurances to preserve the deal.*

### **Following the Money – Banks and the Payment Chain**

*Sanctions exposure travels with money as well as goods. A straightforward invoice can involve the buyer's bank, beneficiary bank, correspondent institutions, payment processors and sometimes separate banks used by agents or logistics providers. OFSI's general guidance*

*treats payment and money-transmission services as financial services, and some sanctions regimes prohibit particular payment relationships or routes. Procurement and accounts-payable teams should therefore understand that a clean supplier screen does not automatically make the proposed payment chain permissible.*

*Bank of Scotland provides a useful example of enforcement. OFSI imposed a £160,000 penalty after the bank processed 24 payments totalling £77,383.39 involving an account held by a person designated under the Russia Regulations. The four incoming payments totalled £76,000 and the 20 outgoing payments £1,383.39. OFSI highlighted weaknesses in screening configuration, escalation, and training, demonstrating how relatively modest transaction values can still generate significant regulatory consequences when payment controls fail.*

*The financial consequences can be much larger. On 11 August 2026, OFSI imposed a £4,732,830.58 penalty on Citibank, N.A., London Branch for breaches involving funds made available for the benefit of a designated person. Earlier UK enforcement included a £20.47 million penalty against Standard Chartered Bank in 2020. These cases concern financial institutions, but procurement's lesson is broader: payment routing is part of sanctions due diligence, not an administrative step after contracting.*

### **Correspondent Banks and Other Financial Intermediaries**

*Correspondent banking allows one financial institution to provide services to another, enabling cross-border payments where the payer and beneficiary banks do not deal directly. That additional layer can create sanctions exposure even when neither the buyer nor supplier is designated. Under the Russia regime, UK credit and financial institutions face restrictions on correspondent relationships and on processing certain payments to, from or through designated banks, including intermediary institutions used for clearing and settlement.*

*For procurement and finance teams, the important point is that the payment chain can contain parties that do not appear anywhere in the contract. A supplier may nominate a legitimate beneficiary bank, yet funds may still pass through a correspondent or intermediary institution subject to restrictions. Payment instructions should therefore be obtained and reviewed early enough to identify relevant banks, jurisdictions and routing arrangements before an invoice reaches the point of settlement.*

*OFSI's July 2026 FAQs make the position explicit: relevant prohibitions can apply where a designated bank appears as the remitting, correspondent, intermediary or beneficiary bank, and can extend to banks it owns or controls. Last-minute bank substitutions, circuitous payment routes through unfamiliar overseas institutions or unexplained third-party payments should therefore prompt further enquiry. The financial route can create sanctions exposure regardless of the supplier's apparent legitimacy.*

*Screening failures within a single institution can undermine an entire payment chain. The FCA fined Starling Bank £28,959,426 in October 2024 for financial crime and sanctions control failures after finding its screening covered only a fraction of relevant customers; a subsequent back-book screening review generated approximately 48,000 alerts. Procurement teams relying on a bank's assurances should remember that a beneficiary institution's controls are not automatically as robust as its size or reputation might suggest.*

### **Agents, Brokers and Distributors**

*Agents, brokers and distributors can obscure the relationship between buyer, manufacturer and ultimate customer because they sit between parties that may never communicate directly. Under the Russia Regulations, brokering services include introducing parties, negotiating arrangements and facilitating transactions. Restrictions may apply to direct or indirect brokering involving sanctioned goods. Procurement should therefore understand what an intermediary actually does, whom it represents, how it is paid and which parties it introduces.*

*A distributor's legitimate incorporation does not make the underlying trade legitimate. UK guidance warns that Russian companies may operate through third countries and that*

sanctioned goods can be made available indirectly through intermediaries. In May 2025, HMRC agreed a £1,160,725.67 settlement with a UK exporter for making goods available to Russia. HMRC specifically highlighted the risk of exporting sanctioned goods to Russian companies operating from otherwise non-sanctioned third countries.

Intermediaries deserve particular scrutiny where their commercial purpose is unclear. Warning signs include commissions disproportionate to the service provided, newly inserted agents, instructions not to contact the end customer, payment to unrelated entities, or distributors whose facilities cannot plausibly handle the goods. The point is not to treat agents as inherently suspicious; it is to establish whether each intermediary has a credible economic role and whether that role changes sanctions exposure.

### **Freight Forwarders and Logistics Providers**

Freight forwarders and logistics providers are not merely transport administrators. They may select carriers, consolidate cargo, prepare customs documents, arrange warehousing, alter routes and hand consignments between operators. UK government guidance therefore tells freight forwarders, carriers, hauliers, customs intermediaries, postal operators and express businesses to undertake due diligence on each consignment they handle. Screening the supplier while ignoring the organisations physically moving the goods leaves a substantial part of the transaction unexamined.

The documentary trail is especially valuable. Government guidance recommends checking commodity codes, descriptions, packing lists, weights, dimensions, consignee details and bills of lading for inconsistencies. A shipment described simply as “spare parts” or “electrical goods”, a package whose weight does not match the declared contents, or Cyrillic labelling for a destination that does not normally use Cyrillic may justify further investigation before the consignment moves.

Logistics behaviour can itself reveal diversion. UK guidance identifies unusual final-mile handovers, delivery of heavy equipment to residential addresses, multiple third-country parties without clear rationale and last-minute substitutions of Russian or Belarusian parties with entities elsewhere. It also warns about blind shipments and switch bills that can conceal consignees. These practices have legitimate uses, but their presence alongside other red flags should prompt deeper due diligence.

Enforcement activity shows that goods movements are actively scrutinised. HMRC reported 58 seizures of sanctioned goods during 2025–26, together with 22 ongoing criminal investigations and 29 voluntary disclosures. It also issued 18 warning letters following voluntary disclosures. Those figures matter to procurement because freight documentation, routing, and customs information are not merely peripheral compliance records; they can provide evidence that a transaction is lawful before a prohibited movement occurs.

### **Shipping Companies, Vessels and Ports**

Shipping risk extends beyond the company that issued the freight invoice. Due diligence may need to consider the vessel, registered owner, operator, flag, port calls and, for relevant oil trades, the applicable price-cap requirements and associated services. UK guidance specifically advises importers and exporters to consider who is shipping their goods and whether a sanctioned vessel is involved. A legitimate cargo can therefore encounter sanctions exposure through the platform used to move it.

The scale of vessel designations has increased sharply. By July 2026, the UK had specified more than 600 vessels under the Russia sanctions regime, including more than 580 oil tankers. In June 2026, Royal Marines and National Crime Agency officers boarded the sanctioned tanker SMYRTOS in the Channel in the first UK-led interdiction of its kind, demonstrating that vessel sanctions can have immediate operational consequences for maritime movements.

Ports can also become decisive points of sanctions control. On 28 January 2026, the

Secretary of State for Transport issued a movement direction to the Russian-flagged cargo vessel SINEGORSK after it anchored in UK internal waters. The Maritime and Coastguard Agency delivered the direction, and the vessel left UK waters. For buyers, this illustrates why vessel identity, flag, operator and intended ports should be checked where maritime exposure is material.

### **Where Did the Goods Really Come From?**

Knowing where goods were purchased is not the same as knowing where they originated. A UK wholesaler may invoice goods from an EU warehouse even though they were manufactured, substantially transformed or extracted elsewhere. Sanctions restrictions can turn on origin, consignment, location or connection with a sanctioned country, depending on the relevant measure. Procurement should therefore obtain evidence that can trace provenance rather than relying on the supplier's billing address or the departure port.

HMRC defines country of origin as the country where goods were produced or manufactured, or where the last substantial processing or transformation occurred. That distinction can materially change risk. Goods dispatched from a low-risk trading hub may retain their origin, which is subject to import prohibitions. UK Russia guidance expressly notes that restrictions may apply to goods originating in Russia, even when the immediate place of shipment was elsewhere.

Procurement evidence may include certificates of origin, manufacturer declarations, customs entries, batch records, bills of materials and shipping documents. The required strength should follow the risk: ordinary domestic consumables may need little more than credible supplier confirmation, while metals, energy products, industrial components, or other sanctioned categories may warrant independent corroboration. A certificate should also be tested against the commercial narrative where the supply route, manufacturer or processing history appears inconsistent.

Petrofac Facilities Management Limited demonstrates how product and destination rules can reach ordinary corporate operations. In June 2026, HMRC announced that Petrofac had paid £569,157.07 for Russia-sanctions offences committed during the divestment of its Russian operations in 2022–23. The breaches involved sanctioned industrial goods made available to a person connected with Russia and for use in Russia, together with prohibited technical assistance. Petrofac voluntarily disclosed and cooperated with HMRC.

### **Country of Origin Versus Country of Dispatch**

Country of origin and country of dispatch describe different commercial facts and should not be treated as interchangeable. HMRC's 2026 methodology defines origin as the country where goods were produced, manufactured or last substantially processed, whereas dispatch concerns the country associated with the relevant commercial movement. A product can therefore be dispatched from one jurisdiction while retaining an entirely different origin, which may materially affect sanctions, customs and procurement risk.

This distinction matters because sanctions restrictions may attach to the origin of particular goods rather than simply the place from which they were shipped. A buyer receiving goods from an established European distributor could still face sanctions exposure if those goods originated in a restricted jurisdiction. Procurement teams should obtain sufficiently reliable provenance information, particularly for higher-risk products, instead of assuming that the supplier's address or dispatch country determines the legal character of the goods.

The distinction is commercially significant enough for HMRC to publish separate import statistics. Since January 2022, customs declarations underpinning Great Britain–EU import data have included country-of-origin information alongside dispatch data. For sanctions purposes, procurement should retain both where relevant: origin helps identify restrictions attached to the goods, while dispatch helps reveal intermediaries and routing. A mismatch between the two is not inherently suspicious, but it can indicate where further enquiry should

begin.

### **Where Are the Goods Really Going?**

*Destination analysis asks more than which address appears on the purchase order. The immediate consignee might be a warehouse, distributor or freight forwarder, while the goods are ultimately intended for another country or user. UK Russia sanctions guidance confirms that some export prohibitions apply even where Russia is not the immediate destination. Procurement and sales teams should therefore understand the anticipated onward movement when goods are sensitive, routes are unusual, or intermediaries dominate the transaction.*

*Commercial logic provides an important cross-check. A customer purchasing sophisticated computing equipment despite operating a small bakery is an example used in UK freight guidance to illustrate a product that does not fit the consignee's business. Other warning signs include delivery to residential addresses, unexplained storage facilities and final-mile handovers to another logistics provider. None establishes diversion on its own, but each tests whether the declared destination is credible in practical terms.*

*The UK strengthened this approach in April 2026 through Sanctions End-Use Controls. Where the government identifies a specific risk that goods exported to a non-sanctioned third country may be diverted to a sanctioned destination or person, an exporter can be formally informed that a licence is required. Once informed, proceeding without the necessary licence is a criminal offence. The regime is targeted, not a blanket licensing requirement for all third-country exports.*

*Government case studies illustrate the intended operation. One example describes industrial cooling systems destined for a Central Asian distributor being stopped at port after diversion concerns indicated likely re-export to a sanctioned Russian entity; the subsequent licence application is refused. Another describes precision electronics exports to a Middle Eastern country, with licensing contingent on satisfactory end-use evidence, reducing the perceived diversion risk. These are illustrative government scenarios rather than published enforcement findings against named companies.*

### **End Users and End Use**

*The end user is the person or organisation ultimately using the goods, while end use concerns what the goods will actually do. Both can matter even when the contractual buyer is legitimate. Due diligence may therefore require an end-user statement, a business-purpose explanation, a delivery-site confirmation, or evidence that the quantities purchased are consistent with normal operations. Sensitive technology deserves particular attention because legitimate civilian products can also have military, industrial or proliferation-related applications.*

*An end-user certificate should not be treated as conclusive merely because it is signed. Government circumvention guidance recommends checking whether the stated use matches the customer's business, whether documentation is internally consistent and whether the consignee can plausibly receive the goods. Procurement should be alert where customers resist identifying users, provide generic descriptions, change destinations after contracting or request documentation that removes commercial parties. Those behaviours can undermine otherwise reassuring paperwork.*

*Sanctions End-Use Controls materially reinforce this principle. They can apply across several regimes, including Russia, Belarus, Iran, North Korea, Syria, Libya and Myanmar, where the relevant legislation contains broader trade restrictions. The government can target a particular good, exporter, route, intermediary or end user where diversion risk has been identified. The regulatory message is clear: lawful shipment to a non-sanctioned country does not necessarily resolve the question of ultimate use.*

### **Re-Exports and Trans-Shipment**

*Re-export occurs when goods already exported to one country are subsequently exported*

onward; trans-shipment generally involves movement through an intermediate location before the final destination. Neither is inherently improper, and both are routine features of global trade. They become sanctions concerns when an intermediate country or commercial step obscures a prohibited destination, person or use. Procurement should therefore distinguish legitimate distribution networks from structures whose commercial purpose appears principally to disguise onward movement.

UK guidance recognises that Russia has sought restricted goods through indirect routes and complex supply chains. The government's voluntary "no re-export to Russia" clause is aimed particularly at Common High Priority Items and other products relevant to Russian military development. It is not legally mandatory under UK Russia sanctions rules, but government guidance says contractual restrictions can form part of due diligence best practice, alongside monitoring and information rights further down the commercial chain.

The consequences of indirect supply are visible in enforcement. HMRC's £1,160,725.67 Russia-sanctions settlement in May 2025 concerned a UK exporter that made goods available to Russia, and its published lessons specifically warn that Russian companies operate in third countries. A UK company can therefore breach relevant prohibitions even when exporting to a non-Russian jurisdiction if the sanctioned goods are being made available to a person connected with Russia through that route.

OTSI's remit is principally concerned with certain trade-sanctions breaches involving services and movements of sanctioned goods, technology or ancillary services outside the UK where a UK person is involved. This can include arrangements in which goods are purchased in one overseas jurisdiction and subsequently supplied to a sanctioned destination. OTSI can impose civil penalties on a strict-liability basis, with a maximum penalty of the greater of £1 million or 50% of the estimated breach value.

### **Third-Country Trading Routes**

Third-country risk has become more important as direct UK-Russia trade has collapsed. UK government figures show that, between October 2024 and September 2025, UK goods imports from Russia were 98.1% lower and exports 97.5% lower than in 2021. That contraction does not make third-country commerce suspicious; rather, it explains why procurement teams must distinguish legitimate regional distribution from routes that may conceal diversion of restricted goods to Russia.

Red flags often appear in combination: a newly formed distributor, sensitive products, vague end use, an unexpected transit country, third-party payment and unusually high willingness to pay for complicated shipping. Freight guidance also identifies multiple third-country parties without clear rationale and last-minute substitutions of Russian or Belarusian entities. A single feature may be innocent; several together create a stronger reason to map ownership, payment, logistics and ultimate destination before approving the transaction.

OTSI's 2025–26 review confirms that this is now an enforcement priority. The agency closed 104 cases during the year, referring 40 to HMRC, and reported research into services-enabled trade diversion and circumvention. Its remit includes certain movements of sanctioned goods outside the UK that involve a UK person. For procurement organisations with multinational operations, the absence of a UK border crossing therefore does not necessarily remove UK sanctions exposure.

### **Indirect Transactions – Hidden Exposure Behind Legitimate Counterparties**

Indirect transactions are difficult because each visible participant can appear legitimate in isolation. A lawful supplier may contract through a lawful distributor, use a lawful bank and ship to a lawful third country, yet the combined arrangement can still benefit a designated person or deliver restricted goods to a prohibited destination. Effective due diligence therefore tests relationships between parties and events, rather than treating each screening result as proof that the overall transaction is safe.

*Sabre Global Technologies Limited shows a different form of indirect exposure. OFSI imposed a £1,000,920.59 penalty in May 2026 after finding breaches involving designated JSC Ural Airlines. Three payments linked to invoices totalling £744,305.13 were frozen by Sabre's UK bank, and Sabre later explored alternative payment options. OFSI also found breaches of circumvention, demonstrating that changing the route or mechanism of a transaction does not neutralise an underlying sanctions restriction.*

*For procurement, the practical test is whether the complete commercial story makes sense. Who manufactured the goods, who owns the supplier, who introduced the parties, who pays, which bank receives the money, who transports the cargo, where it travels and who finally uses it? When those answers align, risk may become manageable. When they conflict, due diligence should follow the discrepancy until the organisation can explain why proceeding remains lawful and reasonably defensible.*

*UK guidance groups the resulting red flags into recognisable categories rather than a single checklist: unusual routing and documentation, inconsistent payment behaviour, and corporate structures that obscure ownership are treated as distinct but overlapping signals. No category is conclusive alone, but guidance is consistent that indicators from more than one category together should prompt closer examination of the transaction rather than reassurance from a single clean screening result.*

### **Sanctions Evasion and Sanctions Circumvention**

*In sanctions practice, "evasion" is the broader term for efforts to circumvent restrictions, while certain UK regimes expressly prohibit circumvention. Under the Russia Regulations, it is prohibited to intentionally participate in activities where a person knows that their object or effect is, directly or indirectly, to circumvent prohibitions or to enable or facilitate a breach. For procurement, the danger is that an apparently lawful transaction may be deliberately structured to disguise what it really achieves.*

*Circumvention exploits legitimate commercial processes rather than obviously illicit ones. An intermediary may be genuine, a bank regulated, and a shipment supported by formal documentation, yet the combined arrangement may still conceal a prohibited end user or destination. UK government guidance stresses that checking external screening databases is not a defence where a business has facilitated circumvention. Compliance, therefore, depends on understanding the commercial substance, not simply on collecting evidence that individual counterparties appeared legitimate.*

*Sabre Global Technologies Limited demonstrates the point. OFSI imposed a £1,000,920.59 penalty in May 2026 after finding breaches involving designated JSC Ural Airlines, including circumvention. Three payments connected with invoices totalling £744,305.13 were frozen by Sabre's UK bank, after which alternative methods of receiving payment were explored. OFSI assessed the case as "most serious", illustrating that restructuring a blocked transaction can itself worsen sanctions exposure rather than resolve it.*

*The broader commercial context explains the enforcement focus. UK government guidance states that more than £20 billion of UK trade with Russia is now sanctioned and that direct trade has fallen to historic lows. Russia has nevertheless continued seeking Western military, dual-use and other critical goods through third countries. Procurement teams should therefore regard sudden intermediaries, unusual routing, or altered end-user information as possible indicators of circumvention that require explanation before proceeding.*

### **How International Supply Chains Can Be Used to Circumvent Sanctions**

*Modern supply chains offer multiple opportunities for a restricted end-user to separate from the supplier that ultimately provides the goods. Government guidance describes a typical covert procurement cycle involving an international supplier, one or more intermediaries, a front or shell company and the true sanctioned end-user. Not every stage appears in every case. The important feature is layering: each additional commercial participant can make the*

*final destination, controlling party or intended use harder to identify.*

*A manufacturer may sell to a long-established distributor in one country, which supplies a newly incorporated trader elsewhere, which then consigns goods through another jurisdiction before onward shipment. Each step may resemble ordinary commerce. The sanctions risk emerges only when the chain is viewed as a whole. Procurement therefore needs sufficient downstream visibility to recognise when geographic, corporate and logistical complexity has no convincing commercial explanation or is disproportionate to the goods being purchased.*

*UK guidance specifically warns that overseas subsidiaries and manufacturing operations may themselves be targeted by front companies seeking sanctioned items for Russia. This matters for multinational organisations whose UK headquarters may maintain strong controls while overseas sales or distribution channels operate differently. Group-wide procurement governance should therefore consider who can release goods, approve customers and alter routes across jurisdictions. A weak overseas node can undermine a sophisticated compliance framework maintained at corporate headquarters.*

### **Diversion and Re-Routing of Goods**

*Diversion occurs when goods intended or documented for one destination are redirected to another person, jurisdiction or use. Re-routing may be legitimate when logistics change due to congestion, weather, cost, or capacity, but unexplained alterations can be significant indicators of sanctions. UK guidance highlights abnormal transportation routes, complex journeys involving multiple third countries and shipments through locations that do not import the product concerned. Procurement should distinguish logistical necessity from changes that obscure ultimate delivery.*

*Trade data can reveal patterns that individual invoices do not. Government guidance identifies significant increases in exports of goods, such as semiconductors or machine parts, to destinations with little prior trade as a potential indicator of circumvention. Buyers and exporters with access to historical purchasing and sales data can apply a similar test. A sudden increase may be legitimate market growth, but it should be understood before unusually large or strategically sensitive orders are approved.*

*The physical route should also be compared with the declared commercial structure. Multiple freight forwarders, ship-to-ship transfers, last-minute consignee substitutions and freight companies listed as final destinations are among indicators identified by UK authorities. None proves wrongdoing. Their importance increases where they occur alongside higher-risk goods, opaque ownership or inconsistent end-use information. Procurement should therefore combine logistics data with evidence from customers, products, and ownership rather than assess routing in isolation.*

*Route changes deserve particular attention after a sanctions event. The FCA reported in 2026 that some stronger businesses reviewed customer activity before and after major sanctions developments to identify possible rerouting or behavioural changes. Procurement teams can apply the same logic to goods: compare historical destinations, intermediaries and freight routes with current transactions. A sudden new hub or consignee may be legitimate, but the reason should be established and recorded.*

*The introduction of UK Sanctions End-Use Controls in April 2026 makes diversion risk even more explicit. Where government informs an exporter that goods destined for a non-sanctioned third country risk ultimate diversion to a sanctioned destination or person, a licence becomes necessary. The measure applies to relevant goods not otherwise covered by specified strategic export controls, reinforcing the principle that an apparently lawful immediate destination does not always determine the legality of the ultimate transaction.*

### **Front Companies and Newly Created Trading Entities**

*Front companies can appear entirely conventional because incorporation, banking facilities, invoices and commercial correspondence may all be genuine. Their distinguishing feature is*

*purpose: they act on behalf of another party whose involvement is deliberately concealed. UK circumvention guidance warns about customers sharing premises with numerous similar businesses, residential registered addresses, layered offshore structures and changes of beneficial ownership around the time sanctions are imposed. These features should prompt corroboration rather than automatic rejection.*

*Recency can also matter. Government guidance identifies newly established overseas customers dealing in military or dual-use goods, particularly those incorporated after 24 February 2022, as potential risk indicators when combined with other concerns. Procurement should examine trading history, directors, ownership, websites, staffing, premises and evidence of previous activity. A new company may be entirely legitimate, but an entity claiming substantial technical capability without an observable commercial footprint deserves proportionately stronger verification.*

*Networks can sometimes be identified through repeated details that individual company checks overlook. Shared directors, telephone numbers, email domains, bank accounts, addresses or contact names can connect apparently unrelated counterparties. UK guidance recommends cross-checking new trading partners against internal customer information and official company records. Procurement data, therefore, has investigative value beyond contract administration: historical vendor records can reveal recurring identifiers that link a newly presented supplier or distributor to earlier relationships of concern.*

*A useful response is to test economic substance. Does the company employ people with relevant expertise, occupy suitable premises, hold inventory, maintain plausible customers and have a reason to participate in this particular trade? A newly formed intermediary buying sophisticated electronics at unusual volumes, while providing only a virtual office and a generic website, presents a different risk from a new subsidiary with transparent ownership, established facilities, and a documented commercial rationale.*

### **Unusual Payment Structures and Other Financial Red Flags**

*Payment behaviour can expose relationships that corporate documentation conceals. UK circumvention guidance identifies invoice splitting designed to remain below control thresholds, prices significantly above market value, third-party payments and transfers involving importers, exporters, agents or brokers near sanctioned borders as potential red flags. The commercial question is whether the money logically follows the transaction. Where the contracting supplier, invoice issuer, payer and beneficiary differ, procurement and finance should understand why before releasing funds.*

*The FCA's 2026 sanctions review found that suspected breaches involved counterparties using third parties, intermediaries and correspondent banks to obscure links to sanctioned persons. It also reported funds routed through cryptoasset or e-money wallets and cash withdrawn for onward movement to higher-risk jurisdictions. These examples arise in financial services, but the procurement implications are direct: payment instructions can reveal hidden participants and geographic exposure that supplier onboarding alone may never identify.*

*Sabre again provides a clear warning. After payments from designated Ural Airlines were frozen, Sabre explored alternative payment options for amounts it was already owed. OFSI concluded that this amounted to circumvention under regulation 19 of the Russia Regulations. Commercial pressure to recover legitimate contractual debts does not justify finding an alternative payment route where sanctions prohibit the underlying transfer. Any proposed workaround should be escalated for a specialist sanctions assessment before action is taken.*

### **Higher-Risk Goods and Technologies**

*Not all products present equal circumvention risk. The UK, the European Union, Japan, and the United States maintain a Common High Priority List that identifies 50 items Russia seeks for its war effort. The list includes integrated circuits, communications equipment, other electronic components, mechanical components, equipment used to manufacture and test*

electronics, and computer-numerically-controlled machine tools. Tiers One and Two contain particularly sensitive items, making product classification central to proportionate due diligence.

UK guidance identifies additional sectors at a higher risk of diversion, including military and dual-use goods, aerospace, automotive products, microelectronics, and heavy machinery. It also highlights industrial machinery, laboratory equipment, aeronautical and radio-navigation instruments, vehicles and engines, tractors, excavators and centrifugal pumps. Procurement professionals do not need to become export-control engineers, but they should know when a specification requires specialist classification and when ordinary supplier checks are plainly insufficient.

Product capability should also be compared with the buyer or end-user. Government guidance uses the example of sophisticated computers ordered for a small bakery and semiconductor manufacturing equipment destined for a country without an electronics industry. Such discrepancies are not proof of evasion, but they weaken the stated commercial explanation. Technical colleagues can be crucial to sanctions due diligence because they can identify when quantities, specifications, or applications do not align with credible operational needs.

Common High Priority items illustrate why apparently mundane components deserve attention. Integrated circuits, passive electronics and mechanical parts may be commercially ubiquitous yet recoverable from Russian weapons systems or essential to military production. Risk cannot therefore be judged by unit price alone. A relatively inexpensive component can carry greater strategic sensitivity than a far more expensive ordinary asset. Procurement risk models should incorporate product classification, end-use potential and diversion attractiveness alongside contract value.

The April 2026 Sanctions End-Use Controls broaden that perspective. They allow targeted licensing requirements in which goods or related technology exported to a third country are assessed as posing a diversion risk to a sanctioned destination or person, provided the items fall within the control's scope. This bridges part of the gap between conventional export controls and sanctions. A product outside strategic control lists can still become sanctions-sensitive because of route, recipient or end use.

### **Higher-Risk Jurisdictions and Trading Hubs**

Jurisdictional risk should identify where additional enquiry is justified, not create a blacklist of legitimate markets. UK guidance currently suggests considering enhanced due diligence for higher-risk products involving customers in Armenia, China including Hong Kong and Macau, India, Israel, Kazakhstan, Kyrgyzstan, Malaysia, Serbia, Thailand, Türkiye, the United Arab Emirates, Uzbekistan and Vietnam. The Government expressly states that inclusion does not assign responsibility to those countries and that legitimate trade remains fully supported.

The list is based on factors including trade flows in Common High Priority goods and analysis of UK-origin products at elevated diversion risk. It is also expressly non-exhaustive and subject to change. Procurement should therefore avoid converting it into a static prohibited-country matrix. A transparent transaction with a genuine manufacturer in one listed jurisdiction may present less risk than an opaque transaction elsewhere involving sensitive goods, unusual payment arrangements and an implausible end-user.

Geography becomes more informative when combined with product and route. Government guidance notes that countries sharing a land border with Russia and that do not impose sanctions on Russia can be attractive sourcing locations for sanctioned goods. Transit through a jurisdiction identified for enhanced due diligence may increase risk. The response is targeted verification of destination, customer capability, ownership, and onward supply, rather than assuming that every company incorporated in that jurisdiction participates in circumvention.

Higher-risk trading hubs are commercially important precisely because they are genuine centres of international trade. Large volumes, sophisticated logistics and extensive re-export

activity can provide both legitimate efficiency and opportunities for concealment. Procurement should therefore examine whether the route makes commercial sense for the product concerned. Where goods travel through several hubs, the organisation should understand each intermediary's function and retain enough documentation to reconstruct the chain if later challenged.

### **Sanctions Red Flags Procurement Professionals Should Recognise**

Red flags should trigger questions, not automatic accusations. UK guidance groups indicators by product, customer, transaction, and export destination, emphasising that no single warning sign conclusively demonstrates illicit activity. Procurement professionals are well positioned to recognise anomalies because they understand normal prices, lead times, quantities, supplier behaviour and contracting structures. A sanctions control framework should therefore capture commercial judgement rather than leave identification exclusively to compliance software or legal specialists.

Customer indicators include opaque beneficial ownership, links to designated persons, shared addresses with numerous similar businesses, residential premises, unexplained ownership changes and limited history in the relevant market. Product indicators include military or dual-use capability, inconsistent technical requirements and quantities that do not fit the customer's operations. Destination indicators include abnormal routes, multiple third-country intermediaries, unexplained transit and shipments to locations with little established demand for the particular product concerned.

Transaction indicators can be even more revealing: significantly above-market prices, invoice splitting, payments by unrelated parties, last-minute changes from Russian or Belarusian entities to companies elsewhere, telephone country codes inconsistent with destination and documentation that omits the true end-user. Freight forwarders presented as final customers and unnecessarily complex logistics should also attract attention. The significance lies in patterns; several modest inconsistencies together can justify enhanced due diligence even where screening produces no match.

Internal data should form part of that assessment. A new customer may share a director, bank account, telephone number, or address with an earlier-rejected counterparty. A supplier's volumes may change sharply after a new restriction is introduced. The FCA reported in 2026 that stronger businesses used intelligence, internal watchlists, transaction monitoring and thematic investigations to identify evasion patterns. Procurement systems contain comparable data and should be designed so relevant relationships can be recognised.

Escalation should be proportionate and documented. A red flag may be resolved through credible evidence, such as an ownership document, a technical explanation, or an established distribution agreement. Multiple unresolved indicators may justify legal review, transaction suspension or refusal to proceed. The discipline is to record the anomaly, the investigation, and the conclusion. This makes sanctions due diligence demonstrable and prevents commercial urgency from overriding concerns that would be obvious upon review of the transaction.

### **Sanctions Screening – What Should Actually Be Screened?**

Screening should extend beyond the supplier's registered name. Depending on the risk, relevant subjects include beneficial owners, directors, controlling persons, customers, end users, agents, brokers, subcontractors, banks, freight providers, vessels, and other transaction participants. Since 28 January 2026, the UK Sanctions List has been the sole UK government list for sanctions designations. Financial restrictions can also reach unlisted entities owned or controlled by designated persons, so list matching alone is insufficient.

Identifiers should be broader than names alone. The UK Sanctions List can contain dates and places of birth, nationalities, passport and national identification details, addresses, positions, registration numbers, parent companies, subsidiaries, websites, telephone numbers and other

information. These details help distinguish a genuine target from an innocent namesake. Procurement systems should preserve sufficient counterparty data to investigate matches rather than collecting only a trading name and relying upon software to determine identity.

Technology should complement, rather than replace, investigation. FCA reviews found gaps caused by outdated lists, poor configuration, incomplete data feeds and weaknesses in ownership screening. Some businesses strengthened detection by using vessel-tracking, corporate-structure analysis, documentation review, and internal watchlists alongside conventional screening. For procurement, this supports a layered control model: automated screening identifies potential matches, while due diligence determines whether the relationship or transaction actually presents prohibited or elevated exposure.

### **Names, Aliases and Transliteration**

Names are deceptively difficult sanctions identifiers. A person may have several spellings, aliases, honorifics, reordered family names or names recorded in non-Latin scripts. The UK Sanctions List distinguishes primary names, primary-name variations, and aliases, and can include non-Latin-script versions. The government's current search tool also provides fuzzy matching intended to identify small spelling differences and transliteration variants. Procurement screening should therefore avoid assuming that one exact English spelling is sufficient.

The FCA quantified the problem in 2026. In its sanctions screening testing, 90% of alerts generated for exact-name test cases correctly identified the relevant sanctioned party, compared with 75% where names appeared in slightly different forms. The FCA also encountered systems that mishandled titles, excluded one-word names or names containing digits, truncated long names and struggled with non-Latin characters. These are configuration weaknesses that can produce false reassurance at scale.

Fuzzy matching improves resilience but must be calibrated carefully. The UK Sanctions List search tool allows fuzzy searching for variations such as "Alexander", "Alecsander" and "Aleksander", with permitted character differences increasing for longer search terms. Broader matching inevitably creates more potential matches, so analysts need secondary identifiers to distinguish false positives from genuine targets. Good screening, therefore, combines flexible name recognition with dates of birth, addresses, registration numbers, nationality, and other corroborating data.

Transliteration risk affects documents beyond the sanctions list itself. A Russian, Ukrainian or Gulf-state counterparty name may be rendered consistently on Companies House filings, inconsistently on shipping documents, and differently again on an end-user certificate, particularly where patronymics, family-name order or diacritics are involved. Procurement should treat inconsistent name renderings across a transaction's own paperwork as a prompt for manual verification, rather than relying on a screening tool to reconcile them.

### **False Positives and False Negatives**

A false positive occurs when screening flags an innocent party because its name or identifiers resemble those of a designated person. False positives are inconvenient but necessary to manage because poorly calibrated systems can generate large alert volumes, stretching review teams and increasing the likelihood of errors. The FCA has warned that excessive sensitivity can make screening operationally inefficient, while insufficient sensitivity can allow sanctioned persons to pass unnoticed as false negatives.

False negatives are more serious because no alert is generated when a relevant sanctions connection exists. In the FCA's 2026 testing, 90% of alerts raised for exact-name cases correctly identified the sanctioned party, but performance fell to 75% where names contained minor variations. The regulator also found failures involving titles, one-word names, digits, long names and non-Latin characters, showing that apparently minor data differences can materially weaken detection.

*Procurement teams therefore need an alert-resolution process, not merely a screening subscription. Potential matches should be tested using dates of birth, addresses, registration numbers, ownership information and other identifiers, with decisions recorded and difficult cases escalated. Repeated false positives can justify calibration changes, but suppressing alerts to reduce workload is dangerous. Equally, a supplier cleared yesterday should not be assumed safe today if reference data, ownership or designations have changed.*

### **Screening Ownership Rather Than Merely Company Names**

*Company-name screening only answers whether the visible entity appears on the UK Sanctions List; it does not establish whether the company is owned or controlled by a designated person. UK financial sanctions can apply to an unlisted entity where the statutory ownership or control tests are satisfied. Procurement therefore needs a second layer of analysis that traces shareholders and controlling interests rather than treating a clean corporate-name result as definitive clearance.*

*Ownership screening should identify direct and indirect shareholders, relevant voting rights and, where the risk justifies it, other mechanisms capable of conferring control. OFSI's enforcement guidance points to shareholder and voting agreements, options, coordination arrangements, benefits conferred on designated persons and evidence of actual or potential influence. Layered structures require the analysis to move through intermediate entities until the organisation can reasonably understand who ultimately owns or controls the supplier.*

*Apple Distribution International provides a striking illustration. Okko LLC was not itself designated as a person, yet it became subject to asset-freeze restrictions because the designated JSC New Opportunities wholly owned it. Apple Distribution International instructed two payments totalling £635,618.75 to Okko and was ultimately penalised £390,000. OFSI emphasised that third-party ownership tools had not identified the ownership change quickly enough and that responsibility remained with the payer.*

*The lesson is broader than one enforcement case. Ownership data can become stale quickly, especially where assets are transferred after sanctions are imposed or corporate registries provide incomplete information. Screening systems should therefore connect name screening with reliable ownership information and an escalation mechanism for opaque structures. A supplier's legal name may remain unchanged while the sanctions position changes overnight because an upstream shareholder is designated, sells its interest or acquires effective control.*

### **When Should Suppliers Be Re-Screened?**

*Suppliers should be screened at onboarding and again whenever a risk-based trigger makes the earlier clearance potentially unreliable. OFSI expects continuing relationships and ownership-and-control assessments to be reviewed at appropriate times because ownership and control are not static. Sensible triggers include a new designation, ownership or director change, bank-account amendment, new subcontractor, altered destination, higher-risk product, unusual payment instruction, or a material change in geographical exposure or business activity.*

*Periodic re-screening should supplement these event-driven checks during longer contracts. The FCA reported in 2026 that 81% of businesses making relevant REP-CRIM returns performed repeat customer screening, while 76% of businesses in its proactive work conducted name screening daily. Procurement organisations need not automatically replicate banking frequencies, but higher-risk suppliers may justify automated daily monitoring, whereas transparent, low-risk domestic suppliers may reasonably be reviewed at longer, documented intervals.*

*The appropriate frequency should therefore reflect both inherent risk and the speed at which relevant circumstances could change. A supplier handling sensitive technology through multiple jurisdictions may require substantially closer monitoring than a domestic provider of routine services. Procurement should also define who owns the re-screening process, how*

alerts are escalated, and what happens when a previously approved supplier develops a new sanctions connection before another purchase order, payment or shipment is authorised.

### **Continuous Monitoring and Changes in Risk**

Continuous monitoring is the process of detecting changes that occur after onboarding rather than repeating the original exercise unchanged. Relevant changes include new beneficial owners, designations, sanctions regimes, payment banks, trading routes, end users and product categories. The objective is to identify whether the assumptions supporting the original risk rating remain valid. A low-risk supplier can become materially higher risk without changing its trading name, contract value or immediate relationship with the buyer.

The Apple Distribution International case vividly demonstrates dynamic risk. Sberbank had owned Okko until 17 May 2022, when Okko was sold to JSC New Opportunities, which was not designated at that time. JSC New Opportunities was then designated on 29 June 2022, immediately bringing wholly owned Okko within the relevant asset-freeze restrictions. Static screening of Okko's own name would not necessarily have captured that sequence without timely ownership monitoring.

Monitoring should also consider behaviour rather than changes in reference data alone. Sudden order increases, new countries of dispatch, unexplained freight routes, payments from unrelated entities or a request to substitute one bank for another can indicate rising risk even where sanctions lists remain unchanged. Procurement, finance, and logistics need mechanisms to share relevant changes. Continuous monitoring is most effective when commercial anomalies can trigger fresh due diligence rather than remain isolated within operational systems.

The pace of designation changes makes static screening inadequate on its own. In the first half of 2026 alone, the UK added at least 411 individuals and entities to the Sanctions List under the Russia regime across separate February, May and June tranches, together with dozens of specified vessels. A supplier cleared in January cannot safely be assumed clear in July without a mechanism that re-checks names against a list that keeps moving.

### **Technology and Automated Screening Systems**

Automated screening systems are valuable because they can compare large volumes of names and transactions against sanctions data much faster than manual checking. The FCA reported that 70% of businesses making relevant REP-CRIM returns used automated screening in 2024–25. In its proactive work, 73% screened transactions or payments at least daily, and nearly six in ten businesses screening payments did so in real time, illustrating the scale achievable through technology.

More sophisticated platforms can combine fuzzy name matching, ownership databases, corporate identifiers, vessel data and transaction rules. Procurement teams can use such tools to screen suppliers, shareholders and intermediaries at onboarding and then generate alerts when reference data changes. Automation is particularly valuable in organisations with thousands of suppliers or frequent international payments, where wholly manual review would be slow, inconsistent and difficult to repeat whenever the UK Sanctions List changes.

Technology also creates a measurable control environment. Screening logs can show when a party was checked, which list version was used, what matching threshold applied and how an alert was resolved. The FCA identifies periodic calibration, quality-assurance testing and retesting after material list or system changes as stronger practice. Those records can help demonstrate that screening was systematic rather than reconstructed after an incident, although they do not prove the underlying due diligence was sufficient.

The procurement objective should therefore be controlled automation rather than maximum automation. Systems should be configured around the organisation's actual jurisdictions, supplier population, products and transaction risks, with responsibility assigned for list updates, testing and unresolved alerts. Vendor technology can provide scale and specialist

*data, but governance remains internal. The FCA has criticised businesses that relied heavily on screening vendors or group arrangements without sufficient local oversight, challenge or assurance over how those controls operated.*

### **The Limitations of Screening Software**

*Screening software is only as reliable as its data, matching logic, configuration and coverage. The FCA found systems that mishandled honorifics, excluded one-word names or names containing digits, truncated long names and struggled with non-Latin characters. It also encountered outdated or poorly maintained lists and gaps in ownership-and-control screening. A green result can therefore mean “no match under these parameters”, not “this transaction is legally safe”, a distinction procurement teams should understand clearly.*

*Third-party databases also lag behind events or contain incomplete corporate information. In the Apple Distribution International case, OFSI noted that external tools failed to identify Okko’s ownership change in time, despite open-source reporting describing the transfer of Sberbank’s digital assets to JSC New Opportunities. Software is strongest when it accelerates investigation; it is weakest when organisations treat absence of an alert as conclusive evidence and stop asking whether the commercial facts themselves create risk.*

### **Human Judgement and Investigative Due Diligence**

*Human judgement becomes critical where facts are incomplete, contradictory or commercially unusual. An experienced procurement professional may recognise that a supplier’s price is implausible, a distributor has no obvious role, an order exceeds normal demand or a proposed route makes little logistical sense. These observations may never trigger automated screening because none is a sanctions-list match. Investigative due diligence converts such anomalies into questions about ownership, destination, end use, payment and intermediary relationships.*

*OFSI expressly expects businesses and individuals to consider ownership-and-control risks through measures that can include their own research, requests for further information and legal advice. The regulator does not prescribe a universal level of due diligence. This gives organisations flexibility but also responsibility: judgement must determine when documentary evidence is adequate, when contradictory information requires corroboration and when residual uncertainty is too significant for procurement to proceed without specialist review or additional safeguards.*

*Judgement should be structured rather than intuitive. A reviewer should distinguish an explainable anomaly from an unresolved red flag, record the evidence supporting that conclusion and recognise personal limits when technical, legal or geopolitical expertise is required. Technology can identify patterns and specialists can interpret legislation, but procurement contributes something different: knowledge of ordinary commercial behaviour. That knowledge is often what reveals that an apparently legitimate transaction does not behave like an ordinary commercial transaction.*

### **Documenting Why a Particular Level of Due Diligence Was Considered Reasonable**

*A defensible sanctions file should explain not only what checks were performed, but why their depth was considered proportionate. OFSI’s enforcement guidance places the onus on the person seeking mitigation to demonstrate that reasonable and appropriate ownership-and-control due diligence was undertaken in good faith. Procurement records should therefore identify the initial risk assessment, information obtained, screening performed, red flags identified, additional enquiries made and the reasoning supporting the final decision to proceed or decline.*

*The record should also explain boundaries. If investigation stopped at Tier Two, the file should show why no credible risk pathway justified going further; if beneficial ownership was independently verified, it should identify the evidence relied upon. This avoids a misleading checklist mentality. Two suppliers may receive different levels of scrutiny for entirely legitimate reasons because their products, ownership structures, jurisdictions, payment routes and*

downstream supply chains create different levels of sanctions exposure.

Documentation becomes particularly important when information is unavailable. A foreign register may be inaccessible, ownership may be fragmented, or a supplier may resist providing commercially sensitive detail. The file should record what could not be established, which alternative sources were used and who accepted the remaining uncertainty. OFSI's guidance recognises that due diligence is risk-based rather than uniform, but a conclusion is easier to defend when the decision-maker can show how uncertainty was consciously assessed.

Records should remain connected to later monitoring. A dated approval based on specified owners, banks, routes and end users creates a baseline against which subsequent changes can be tested. If a new designation or ownership event occurs, the organisation can identify which earlier assumptions are affected. This makes sanctions due diligence an auditable lifecycle rather than disconnected searches and provides senior management with evidence that risk acceptance was deliberate, proportionate and reviewable.

### **Case Study – The Apparently Innocent Counterparty**

Colorcon Limited illustrates how sanctions exposure can arise through payments to apparently unremarkable counterparties rather than through an unlisted Tier One supplier. Its Moscow office made 123 payments worth £191,290.57 to non-designated employees and service providers; 44 payments totalling £63,012.85 were permitted under a General Licence, leaving 79 payments worth £128,277.72 in breach because the recipients' accounts were held at designated Alfa Bank, Promsvyazbank, Sberbank and VTB Bank. OFSI imposed a £152,750 penalty.

The failure was therefore not simply a poor supplier-name match. Colorcon's UK signatories checked payment amounts and payee details but did not review the sanctions status of the banks receiving the funds. The company also assumed that its own banking provider would undertake the necessary sanctions screening without independently confirming that this control was sufficient. OFSI made it clear that reliance on third-party screening did not remove Colorcon's own compliance responsibility.

For procurement, the case demonstrates why apparently benign suppliers, employees or service providers cannot always be assessed independently from the wider payment infrastructure surrounding them. The contracting party may be unrestricted while the beneficiary bank, correspondent institution or other financial intermediary creates the sanctions exposure. Effective due diligence should therefore connect counterparty screening with payment-route analysis, particularly where overseas transactions are involved, rather than assuming that a legitimate recipient automatically makes the associated payment permissible.

### **Case Study – The Sanctioned Owner Behind an Unsanctioned Company**

Apple Distribution International offers an unusually clear example of a sanctioned owner sitting behind an unlisted company. Okko LLC operated a Russian online media streaming platform and had previously been owned by Sberbank. It was sold on 17 May 2022 to JSC New Opportunities, which the UK then designated on 29 June 2022. From that designation, Okko became subject to asset-freeze restrictions because JSC New Opportunities wholly owned it.

Apple Distribution International had instructed one payment of £356,429.27 before the designation, with funds released on 30 June, and another payment of £279,189.48 on 30 June, which was released on 28 July. Together they totalled £635,618.75. OFSI concluded that both breached the Russia Regulations and imposed a £390,000 penalty. Importantly, OFSI made no finding of breach against Apple Inc.; the enforcement finding concerned Apple Distribution International.

OFSI found that Apple Distribution International's processes for Russian app developers relied primarily on self-certification and third-party ownership due diligence, and that external tools did not promptly identify Okko's change in ownership. Open-source articles concerning the

transfer were available, while direct ownership information had not been affirmatively requested. The case encapsulates the article's central argument: the supplier's name can remain clean even as the ownership behind it changes the transaction's legal character.

The case is not isolated. The FCA's May 2026 review, discussed earlier in this article, found that some regulated businesses relied on third-party vendor tools to supplement sanctions screening without independently verifying their coverage or configuration. This pattern echoes Apple Distribution International's reliance on third-party ownership due diligence for Okko. Both regulators reach the same conclusion: outsourcing verification does not outsource legal responsibility for the result.

### **Case Study – The £1.16 Million Settlement and Third-Country Risk**

HMRC's £1.16 million Russia-sanctions settlement illustrates third-country risk, although HMRC did not disclose how the transaction was routed. In May 2025, an unnamed UK exporter paid £1,160,725.67, a record settlement, after making goods available to Russia in breach of the Russia Regulations. HMRC separately warned that Russian companies can operate from third countries and that supplying them with sanctioned goods can breach sanctions, even where the destination is not Russia.

The enforcement notice does not name the exporter or reveal how the transaction was structured, so it would be wrong to infer that goods passed through an intermediate jurisdiction. What matters is the pattern HMRC warned against: a transaction can show a lawful customer address and a non-Russian delivery country, yet still make goods available to a Russian-connected person. Procurement must test ownership, purpose and destination rather than treating the first overseas consignee as conclusive.

The case gives procurement a practical test for third-country transactions: does the customer have a credible reason to buy the goods, facilities capable of using them, and a trading history consistent with the order? Where sensitive goods, opaque ownership and re-export possibilities converge, enhanced due diligence becomes proportionate. HMRC's accompanying guidance reinforces the point that an apparently legitimate third-country destination does not remove the need to understand who ultimately receives or benefits from the goods.

### **Case Study – The Hidden Bank or Shipping Connection**

A hidden financial connection can transform the sanctions analysis, even when neither the buyer nor the seller appears problematic. OTSI published a 2025 case involving the UK branch of a multinational bank, which it did not name. Several payments concerned a UK-sanctioned product moving from Russia to a third country. Because handling payments could facilitate prohibited movement, the UK branch itself may have sat within the sanctions-sensitive supply chain despite acting only as an intermediary.

The bank's screening identified the payments and triggered enhanced due diligence. It then declined to process them, investigated internally and reported the activity to OTSI with supporting material, including transaction information. OTSI concluded that the UK branch had not breached trade sanctions because the payments were stopped. The case is important because effective screening did not merely identify a designated name; it exposed a prohibited underlying trade flow hidden behind an otherwise routine financial-service request.

Shipping can create the same problem. OFSI's maritime guidance warns businesses to examine vessel ownership, control, flag, registration, voyage history and potentially deceptive practices such as ship-to-ship transfers or manipulation of Automatic Identification System data. A legitimate supplier and lawful cargo do not remove risk if a designated vessel, prohibited maritime service, or sanctioned ownership connection enters the transport chain. Procurement should therefore regard transport arrangements as part of counterparty due diligence.

The combined lesson is that commercial invisibility does not equal legal irrelevance. Banks,

*insurers, freight forwarders, shipowners and vessels may be several steps removed from the contracting supplier yet still determine whether funds, goods or services can lawfully move. Procurement need not investigate every intermediary in every transaction, but higher-risk payments and maritime movements should be mapped far enough to identify the institutions and assets whose participation could alter the sanctions position.*

### **What Would Adequate Due Diligence Look Like to an Enforcement Authority?**

*An enforcement authority is unlikely to ask whether an organisation completed a particular checklist; it will examine whether the investigation was appropriate to the actual risk. OFSI's February 2026 enforcement guidance states that it does not prescribe one level or type of ownership-and-control due diligence. Instead, it considers the degree of sanctions risk, nature of the transaction and commercial relationship, and expects evidence that these factors informed the organisation's decision-making process.*

*For ownership and control, OFSI identifies potentially mitigating enquiries, including examinations of shareholdings, voting power, recent divestments, constitutional documents, shareholder agreements, and evidence of indirect or de facto influence. It also points to open-source research, direct enquiries, and investigations into proxies, trusts, financial relationships, and benefits flowing to designated persons. Not every case requires every enquiry, but higher-risk structures should produce correspondingly stronger evidence and a clear explanation for the conclusions reached.*

*Adequacy also depends on timing. OFSI states that ownership and control are not static and expects appropriate reviews to continue where relationships or activities persist. A supplier screened once three years ago cannot automatically be treated as cleared today if ownership, directors, banks, routes or sanctions designations have changed. The due diligence record should therefore show both the original assessment and the events or intervals that trigger re-screening, enhanced review, or renewed approval.*

*Good evidence should demonstrate challenge rather than passive acceptance. Procurement should show how conflicting information was resolved, why supplier declarations were considered credible, which independent sources were consulted and what happened when a red flag appeared. Where information remained unavailable, the record should explain residual uncertainty and who authorised it. OFSI places the onus on the person seeking mitigation to demonstrate that relevant due diligence was reasonable, appropriate and undertaken in good faith.*

*The standard is therefore neither perfection nor minimal compliance. A reasonable organisation should understand enough about the supplier, ownership, payment chain, goods, origin, destination and significant intermediaries to recognise material sanctions pathways and investigate credible concerns. It should also know when specialist legal or export-control advice is necessary. An enforcement authority can then see a risk-based process that followed the evidence, rather than a superficial screening result preserved to prove that a box was ticked.*

### **A Practical Sanctions Due Diligence Framework**

*A practical framework begins with classification. Procurement should identify the legal supplier, ownership structure, goods or services, contract value, countries involved, intended destination, end user and payment route. These factors establish the initial sanctions-risk profile. Low-risk domestic purchases may require standard identity and list checks, while sensitive technology, complex ownership, higher-risk jurisdictions or unusual routes should move immediately into deeper review. The assessment should be recorded before contractual commitment or release of funds.*

*The second stage is verification. Legal names and registration numbers should be corroborated through reliable registries; beneficial owners and controlling persons should be traced to test ownership-and-control rules; and relevant directors, intermediaries and financial*

*institutions should be screened. Procurement should distinguish between what the supplier asserted and what has been independently verified. Where ownership passes through several entities, the investigation should continue until controlling interests are understood or unresolved opacity itself becomes a risk factor.*

*The third stage follows the goods. Procurement should establish origin, manufacturing location, country of dispatch, transport route, consignee, ultimate destination and end use where relevant to applicable restrictions. Sensitive or Common High-Priority goods warrant stronger provenance evidence and downstream questions. Bills of lading, certificates of origin, export documents, end-user statements and logistics records should be compared with the commercial narrative rather than accepted separately without testing whether they tell a coherent story.*

*The fourth stage follows the money. The organisation should understand who invoices, who pays, which account receives the funds and whether banks or payment intermediaries create separate sanctions exposure. Third-party payments, unexplained beneficiary changes, split invoices or sudden substitutions of financial institutions should trigger escalation. OFSI penalties of £152,750 against Colorcon and £390,000 against Apple Distribution International demonstrate how payment arrangements and ownership beyond an immediate counterparty can materially affect sanctions exposure.*

*The fifth stage determines the depth of investigation and approval. Each red flag should be resolved through credible evidence or escalated. The organisation should record why it stopped investigating, what uncertainty remained and who accepted that residual risk. High-risk cases may require sanctions specialists, legal advice, licensing assessment or refusal to proceed. The governing principle remains simple: investigate as far as identified risk requires, not automatically to Tier Two, Tier Three or another arbitrary boundary.*

*The final stage is monitoring. Suppliers should be re-screened at risk-based intervals and when meaningful events occur, including new designations, ownership changes, new banks, changed routes, new subcontractors or altered end users. Automated tools can provide scale, but alert resolution and investigative judgement remain essential. The framework should preserve a dated audit trail linking screening, evidence, decisions and subsequent reviews so the organisation can reconstruct why the transaction was considered lawful at the relevant time.*

### **Summary – Know the Supplier, Follow the Money and Trace the Goods**

*Effective sanctions due diligence begins with the supplier but cannot end there. Ownership can place an unlisted company within restrictions; a bank can change the permissibility of payment; a vessel can change the risk of carriage; and an intermediary can conceal the destination of goods. The central procurement discipline is to integrate corporate, financial, and physical information until the transaction makes commercial and legal sense, rather than treating each participant as an isolated screening exercise.*

*That does not require limitless investigation. OFSI's enforcement approach recognises that due diligence should be proportionate to sanctions risk, transaction type and commercial relationship. A transparent UK supplier of domestic goods may require little investigation beyond ordinary controls. A distributor of sensitive electronics that uses layered ownership, third-country routing, and unfamiliar banks requires more. The stopping point is reached when credible risk pathways have been investigated, and the remaining uncertainty is reasonable, understood, and documented.*

*The enduring rule is consequently straightforward: know the supplier, understand who owns and controls it, follow the money and trace the goods. Re-screen when circumstances change, investigate anomalies rather than explaining them away, and document why the chosen depth of enquiry was proportionate. Sanctions compliance is strongest when procurement can show not only who it contracted with, but why it reasonably understood the wider commercial ecosystem well enough to proceed.*

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. © Procurement and Supply Chain Management Made Simple. All rights reserved.

### **Further Reading**

This article draws on the following primary sources, consulted between 2025 and 2026:

- HM Treasury, Office of Financial Sanctions Implementation (OFSI) — Monetary Penalties and Enforcement Guidance, and published enforcement/penalty notices (Colorcon Limited, Apple Distribution International, Bank of Scotland, Sabre Global Technologies Limited, Citibank N.A. London Branch, Herbert Smith Freehills CIS LLP Moscow), gov.uk.
- Office of Trade Sanctions Implementation (OTSI) — guidance on civil enforcement of trade sanctions under the Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, and the 2025–26 annual enforcement review, gov.uk.
- HM Revenue & Customs — compound settlement notices for export control and trade sanctions breaches, including the May 2025 £1,160,725.67 Russia-sanctions settlement, gov.uk.
- Financial Conduct Authority — sanctions systems and controls reviews (including the May 2026 review of 150 authorised firms) and the Starling Bank Limited final notice of October 2024, fca.org.uk.
- Foreign, Commonwealth & Development Office — the UK Sanctions List and guidance on sanctions circumvention, third-country risk and red-flag indicators, gov.uk.
- Companies House — Incorporated companies in the UK statistical releases and guidance on identity verification under the Economic Crime and Corporate Transparency Act 2023, gov.uk.
- Cabinet Office / Procurement Review Unit — Procurement Act 2023 statutory guidance on exclusions and debarment, gov.uk.
- Legislation.gov.uk — the Procurement Act 2023, the Economic Crime and Corporate Transparency Act 2023, the Sanctions and Anti-Money Laundering Act 2018, the Policing and Crime Act 2017, and the Russia (Sanctions) (EU Exit) Regulations 2019.