ANALYTICAL REPORT | 2026

The EU Sanctions Architecture against Russia

Effectiveness, Limits, and Strategic Options for 2026–2030

A comprehensive assessment of the political, economic, social, legal, hybrid, and compliance dimensions of the EU sanctions regime

European Institute for Innovation Development | eiid.eu | Ostrava, Czech Republic

EUROPEAN INSTITUTE FOR INNOVATION DEVELOPMENT

The EU Sanctions Architecture against Russia: Effectiveness, Limits, and Strategic Options for 2026–2030

Dr. Alexander Buychik

Ostrava–Opava, Czech Republic

2026

Imprint

Designed by Tuculart Studio.
All the tables and figures were graphically designed ChatGPT partly.

Publisher:
European Institute for Innovation Development.

Edition:
Buychik, A. et al. The EU sanctions architecture against Russia: Effectiveness, limits, and strategic options for 2026–2030. Ostrava, Opava: Tuculart Edition, European Institute for Innovation Development, 2026. — 800 p. (88.73 printed sheets)

ISBN 978-80-88474-43-2
DOI 10.47451/book-2026-06

For citation (in APA):
Buychik, A. (2026). *The EU sanctions architecture against Russia: Effectiveness, limits, and strategic options for 2026–2030*. Ostrava, Opava: Tuculart Edition, European Institute for Innovation Development.

Content

PART SEVEN

Sanctions Compliance Architecture

7.1. Compliance as a Cornerstone of Sanctions Policy

7.1.1. Compliance as the Operational Transmission Mechanism of Sanctions

Compliance should be understood not as a secondary administrative appendage to sanctions policy, but as the operational mechanism through which restrictive measures are translated from legal text into market behaviour. A sanctions regulation, however precise in doctrinal terms, does not in itself block a payment, stop a container, invalidate an insurance renewal, prevent a letter of credit, or interrupt access to a commercial platform. Those effects emerge only when regulated actors embed the legal prohibition into screening systems, customer-onboarding practices, routing controls, contractual decision-making, and escalation procedures. In that sense, compliance performs the same function in sanctions governance that transmission systems perform in engineering: it converts centrally adopted commands into distributed operational effects across a large and heterogeneous network of actors. This is especially important in the EU context, where sanctions frequently rely on direct applicability of regulations but practical implementation is dispersed across banks, exporters, customs brokers, shipowners, insurers, advisers, and digital intermediaries. The practical force of sanctions therefore depends not only on the breadth of listings or prohibitions, but on the extent to which these actors recognise risk, identify prohibited exposure, and adjust behaviour before a violation materialises. Compliance is thus *ex ante* as much as *ex post*. It is a behavioural governance mechanism, not merely an enforcement afterthought. That is why modern sanctions should be analysed not only as law and not only as coercion, but as law mediated through organisational controls. In operational terms, sanctions begin to matter when compliance systems begin to function[1,2].

This distinction between formal prohibition and operational effect is fundamental for any serious evaluation of sanctions against Russia. A formal prohibition exists at the level of the legal norm, the *Official Journal*, and the consolidated sanctions framework. Operational effect exists when the prohibition is converted into an interruptive event in the life of a transaction, service relationship, or commercial strategy. A bank does not respond to sanctions in the abstract; it responds through customer due diligence, sanctions-list screening, name matching, ownership-and-control analysis, transaction monitoring, and refusal or escalation decisions. An exporter does not comply by acknowledging the existence of a Council Regulation; it complies by redesigning sales controls, end-user checks, route assessment, document scrutiny, and post-shipment review. An insurer does not implement sanctions by endorsing the policy objective; it does so by declining cover, refusing renewal, reclassifying vessel exposure, or enhancing underwriting due diligence. The same logic applies to freight forwarders, consulting firms, software vendors, payment intermediaries, and online platforms. In each case, the legal rule is only the normative starting point, while compliance is the institutional process through which the rule becomes economically consequential. This means that a sanctions regime may appear extensive on paper and still underperform if the transmission layer is weak, fragmented, or

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

inconsistent. Conversely, a regime with fewer headline measures may exert strong pressure if its compliance conversion rate is high across relevant sectors[1,2,3].

A useful way to conceptualise compliance is as a chain of translation running from legal designation to operational blockage. At the first stage, a political and legal authority identifies a target, activity, service, sector, or class of transactions for restriction. At the second stage, that decision is formalised through legal acts, lists, definitions, and interpretative materials. At the third stage, regulated and exposed private actors ingest those rules into internal systems, whether through data feeds, software updates, manual controls, policy revisions, or legal review. At the fourth stage, individual counterparties, vessels, consignments, or payment messages are screened against those systems. At the fifth stage, the private actor decides whether to proceed, block, freeze, reject, report, seek a licence, or escalate the matter internally and externally. At the sixth stage, the target experiences a material constraint, not because the law existed in theory, but because access to finance, logistics, insurance, technology, or intermediation has actually been denied or delayed. At the seventh stage, the wider market internalises the risk signal and begins to pre-emptively avoid similar exposure. This cumulative sequence shows that compliance is not an incidental technical layer. It is the central transmission channel through which sanctions acquire behavioural reality across decentralised systems of exchange[4,5,6].

The distributed character of sanctions implementation explains why compliance cannot be reduced to state enforcement alone. Public authorities adopt, interpret, coordinate, and in some cases penalise, but they do not personally review every customer file, shipping instruction, correspondent banking message, or export-control query. The daily conversion of sanctions law into operational restraint is performed overwhelmingly by firms and organisations that sit at the points where cross-border activity is initiated, routed, financed, documented, or insured. This makes compliance a form of delegated governance, although not in the sense of voluntary self-regulation. The delegation is structured by law, incentivised by liability exposure, and reinforced by reputational, contractual, and supervisory pressure. Private actors become the first line of detection, the first line of interruption, and often the first line of evidential preservation. That is why the European Parliament has emphasised that implementation heavily relies on the private sector and that the Union must provide adequate guidance to economic operators if sanctions are to be applied effectively. The same principle appears in partner jurisdictions, where general sanctions guidance describes firms as central to implementation and, in some contexts, the first line of defence against circumvention. The implication is analytically important: the sanctions regime is neither purely public nor purely private in operation. It is a hybrid governance system in which public legality depends on private transmission capacity[7,8,9].

Within the EU, the importance of compliance as a transmission mechanism is reflected in the growth of an increasingly dense guidance infrastructure. The Commission maintains a sanctions resources architecture that includes consolidated FAQs, the financial sanctions consolidated list, the EU sanctions map, the sanctions helpdesk, and the whistleblower tool. This institutional ecosystem exists because legal acts alone are insufficient for uniform implementation across complex sectors and Member States. Operators require not only knowledge of what is prohibited, but workable assumptions about ownership, control, due diligence expectations, red flags, reporting channels, and the relation

[1] European Commission. (2024a, February 19). *Guidance on due diligence*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[3] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[4] European Commission. (2023a, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] European Commission. (2026a, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[7] Ibid.
[8] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[9] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

between general rules and sector-specific risk. The consolidated FAQ architecture performs a standardising function by providing a common interpretative frame for authorities, operators, and citizens. The sanctions helpdesk lowers practical barriers to compliance, especially for firms that lack deep in-house sanctions capability. The whistleblower tool expands the informational surface through which suspected violations may reach authorities. The consolidated list improves the machine-readable and operational usability of listing decisions. Taken together, these instruments reveal that the Union itself treats compliance as a core functional condition of sanctions effectiveness, not as a peripheral technical problem[1,2,3].

A central feature of modern sanctions compliance is that it is risk-based rather than purely formalistic. The Commission's due-diligence guidance explicitly states that there is no one-size-fits-all model and that each operator must develop, implement, and routinely update a compliance programme calibrated to its business model, sectoral exposure, geography, and risk assessment. This is a major analytical point because it means sanctions implementation is not exhausted by mechanical list-checking. A firm trading low-risk goods within a limited jurisdictional footprint does not face the same exposure as a multinational bank, maritime insurer, dual-use exporter, or freight operator active in re-export corridors. Risk-based compliance therefore requires proportionality of controls, but not passivity. It demands the capacity to identify where the business is exposed to designated persons, opaque ownership structures, suspicious intermediaries, high-priority items, or diversion-sensitive routes. It also requires regular updating, because circumvention patterns evolve faster than static manuals. In this sense, compliance is dynamic and learning-based. It is closest to a system of operational vigilance structured by law, rather than a box-ticking exercise organised by formality. Where this risk-based logic is absent, the transmission of sanctions becomes either under-inclusive, through false negatives, or over-inclusive, through indiscriminate de-risking[4,5,6,7].

Table 7.1.1-1. Sanctions Compliance as a Transmission Chain from Norm to Behaviour

Stage of the chain	Principal carrier	Operational result
Legal designation or prohibition	EU institutions / partner governments	A restrictive norm is formally created
Interpretative clarification	Commission FAQs, guidance, best-practice materials	Operators receive usable assumptions for implementation
Data operationalisation	Consolidated lists, internal systems, screening tools	Legal categories become machine-readable or workflow-readable
Organisational embedding	Compliance teams, legal departments, management approval	Policies, escalation channels, and review thresholds are set
Transaction-level screening	Banks, exporters, insurers, logistics firms, platforms	Counterparties, goods, routes, and services are tested against risk
Decision and interruption	Front-line business units with compliance oversight	Freeze, reject, report, escalate, licence-check, or terminate
Market feedback and deterrence	Wider ecosystem of counterparties and intermediaries	Risk avoidance spreads beyond individual blocked cases

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Commission. (2025, November 17; last updated March 13, 2026). *Overview of sanctions and related resources*.
[3] European Commission. (n.d.). *EU sanctions whistleblower tool*.
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] European Commission. (2024, February 19). *Guidance on due diligence*.
[6] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[7] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

Authorship: prepared by the author on the basis of official EU institutional materials, United Kingdom' and United States' materials.
Sources:

- European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
- European Commission. (2024, February 19). *Guidance on due diligence*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

The behavioural significance of compliance lies not only in its ability to stop prohibited activity, but also in its capacity to reshape incentives before enforcement action becomes necessary. Once firms internalise the possibility of exposure, they begin to re-price risk, tighten onboarding, shorten acceptable counterparty chains, demand more documentary evidence, and reject ambiguous transactions at earlier stages. This anticipatory adjustment is one of the main reasons why sanctions can generate effects broader than the number of prosecuted or publicly detected violations might suggest. It turns legal rules into a climate of constraint. A customer associated with a high-risk jurisdiction, an unusual routing pattern, or a poorly explained ownership structure may find that commercial access narrows even without a formal designation. This does not mean that all such refusals are normatively desirable, because over-compliance is a real issue to be analysed separately. It means that compliance operates as a preventive system that alters expected behaviour at scale. In sanctions policy against Russia, this preventive function is especially important because many relevant transactions are time-sensitive, cross-border, and reliant on service ecosystems that can be interrupted before the target acquires the desired economic advantage. The earlier the interruption occurs, the greater the coercive efficiency of the regime. Compliance therefore converts sanctions into a system of practical friction, not just legal prohibition[1,2,3].

In the financial sphere, the transmission role of compliance is particularly visible because banking systems sit at the centre of payment execution, liquidity access, correspondent relations, and settlement reliability. Financial sanctions are made real through customer due diligence, sanctions screening, transaction monitoring, ownership-and-control analysis, internal escalation, suspicious-activity logic, and licensing checks. The effect is not limited to the freezing of listed assets. It also encompasses the refusal of account services, heightened scrutiny of payment messages, rejection of trade-finance instruments, and broader reluctance to intermediate transactions linked to sanctioned sectors or high-risk routes. Because banks occupy a nodal position in the wider economy, their compliance decisions can multiply the reach of legal measures beyond the financial sector narrowly defined. A supplier may have the goods, an insurer may be willing in principle, and a customer may exist, but if the payment chain fails, the transaction may not proceed. This is why financial institutions are often the most consequential private transmitters of sanctions pressure. The same logic explains why partner jurisdictions devote extensive guidance to financial sanctions implementation and why senior-management commitment, resourcing, and compliance authority are treated as essential components of an effective programme. In operational reality, a sanctions regime without disciplined banking compliance is a regime with weak circulatory control. The financial system is therefore not merely one

[1] European Commission. (2023, September 7). *Sanctions: Commission publishes guidance to help European operators assess sanctions circumvention risks*.
[2] European Commission. (2024, February 19). *Guidance on due diligence*.
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

sector among others; it is one of the main conduits through which sanctions law becomes material constraint[1,2,3].

The same transmission logic applies in trade and export-control settings, although the mechanics differ from banking. Here compliance acts through export classification, counterparty vetting, end-use and end-user checks, route scrutiny, document review, contract clauses, and post-sale controls. The Commission's due-diligence materials and Russia circumvention guidance make clear that operators must assess business partners, transactions, and goods, and must pay attention to circumvention red flags rather than treating formal paperwork as self-sufficient proof of legitimacy. This is critical in the Russia context because diversion often occurs through third-country intermediaries, layered logistics, or disguised end-users rather than through obviously direct shipments. Export controls and sanctions therefore depend on firms asking whether the transaction makes commercial sense, whether the routing is plausible, whether the customer profile matches the goods, and whether the documentation withstands scrutiny. Compliance in this sector is not a clerical function. It is an investigative screening function embedded within ordinary business processes. The release of G7 industry guidance with heightened-risk items, updated red flags, best practices, and public screening resources shows that authorities expect implementation to occur through operational judgement at the level of firms, not solely through border interception by the state. The exporter, distributor, freight forwarder, and service provider collectively become the mechanism that prevents restricted goods from reaching Russian military-industrial use. In that sense, trade compliance is one of the clearest examples of sanctions as decentralised control exercised through private operational checkpoints[4,5,6,7].

Beneficial ownership and ownership-and-control analysis illustrate especially well why compliance is the real transmission mechanism rather than a mere administrative annex. A sanctions list may identify a designated person by name, but the economically significant question is often whether a non-listed entity is in fact owned or controlled by that person or operates for that person's benefit. The compliance challenge is therefore not exhausted by name matching. It requires corporate-structure analysis, document verification, control-rights review, scrutiny of indirect holdings, and judgement about *de facto* influence. FATF guidance stresses that stronger beneficial-ownership transparency is essential because sanctions evaders, money launderers, and corrupt actors frequently hide behind complex legal structures, shell companies, and trusts. Partner-jurisdiction experience reinforces the same lesson. The UK's 2026 ownership-and-control review explicitly states that firms are expected, and required by law, to assess ownership and control and that industry plays a first-line defensive role in ensuring sanctions are implemented robustly and effectively. This is operationally decisive because many Russian-linked commercial networks do not rely on overtly Russian counterparties, but on layered corporate vehicles designed to fragment visibility and dilute apparent connection. Where ownership-and-control analysis is weak, the legal measure remains formally present but economically porous. Where it is strong, sanctions penetrate beyond the visible list and reach the real structure of control[8,9,10].

Anti-circumvention policy further confirms that compliance is not merely a way of obeying sanctions, but the main means of preserving their effect under conditions of adaptation. Russian circumvention

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] European Commission. (2024, February 19). *Guidance on due diligence*.
[6] European Commission. (2024, September 24). *Sanctions vis-à-vis Russia: Commission publishes G7 Industry Guidance on preventing sanctions evasion*.
[7] U.S. Department of Commerce, Bureau of Industry and Security. (2024, February 23). *Common High Priority Items List (CHPL)*.
[8] Financial Action Task Force. (2024, March 11). *Guidance on Beneficial Ownership and Transparency of Legal Arrangements*.
[9] HM Treasury, Office of Financial Sanctions Implementation. (2026b, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[10] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.

efforts have become more elaborate, opaquer, and more dependent on third-country intermediaries, layered service provision, and re-export chains. The Commission's guidance was issued precisely because the Union recognised that operators need tools to identify, assess, and understand circumvention risks in real time. Those tools include strategic risk assessment, enhanced due diligence for higher-risk exposure, and red-flag awareness concerning customers, transactions, routing, and goods. The 2024 G7 industry guidance goes further by combining heightened-risk item lists, updated red flags, best practices, and public screening resources. This shows that sanctions enforcement is increasingly typology-based rather than purely rule-recitation-based. In other words, operators are expected to look for patterns of evasion, not merely direct textual matches. The transmission mechanism of sanctions thus becomes partially intelligence-like in character, although still constrained by legal and evidential discipline. Compliance turns anti-circumvention from a declaratory political objective into a distributed pattern-recognition effort embedded in private operations. Without such compliance adaptation, sanctions lose force as soon as targets learn to route around them[1,2,3,4].

Another reason why compliance must be treated as the operational transmission layer is that sanctions implementation depends heavily on information architecture. A prohibition is useful only to the extent that operators can access relevant data, map it correctly, and integrate it into decision-making within operational time constraints. The Commission's consolidated lists, FAQs, helpdesk, and whistleblower mechanism are all instruments for reducing information failure. The consolidated list improves accessibility and operational matching. FAQs reduce interpretative asymmetry. The helpdesk lowers the entry barrier for firms, especially smaller operators, that may otherwise misapply or under-apply sanctions due to insufficient capacity. The whistleblower tool expands the system's ability to capture violation signals that would not emerge through routine compliance monitoring alone. This informational dimension matters because sanctions failure often arises not from open opposition to the policy, but from ambiguity, fragmentation, weak visibility, or slow data conversion. Compliance is the channel through which information becomes action, and action becomes interruption. In that sense, sanctions governance is partly an information-governance problem, and compliance is its main applied interface[5,6,7,8].

At the organisational level, effective transmission depends on whether sanctions compliance is embedded into governance rather than isolated in a marginal support unit. The OFAC framework is especially useful conceptually here because it identifies management commitment, risk assessment, internal controls, testing and auditing, and training as essential components of a sanctions' compliance programme. Although the report focuses on the EU track, this logic is broadly transferable and helps clarify why operational effect varies across firms exposed to similar legal rules. If senior management does not allocate resources, if compliance lacks authority, if business units can bypass controls, or if staff do not understand exposure patterns, the legal rule will remain weakly transmitted. Conversely, well-resourced compliance can identify exposure early, preserve audit trails, support defensible decisions, and align commercial practice with legal obligations. The transmission mechanism is therefore institutional before it is technological. Software matters, but only when it sits inside a governance structure that authorises escalation, tolerates transaction delay where needed, and values legal-operational discipline over short-term commercial convenience. This is why mature sanctions

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2023, September 7). *Sanctions: Commission publishes guidance to help European operators assess sanctions circumvention risks*.
[3] European Commission. (2024, September 24). *Sanctions vis-à-vis Russia: Commission publishes G7 Industry Guidance on preventing sanctions evasion*.
[4] U.S. Department of Commerce, Bureau of Industry and Security. (2024, February 23). *Common High Priority Items List (CHPL)*.
[5] European Commission. (2025b, November 17; last updated March 13, 2026). *Overview of sanctions and related resources*.
[6] European Commission. (n.d.). *EU sanctions whistleblower tool*.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[8] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

implementation is inseparable from corporate governance quality. Compliance is not just an act of checking; it is an act of organisational steering[1,2,3].

The relationship between compliance and enforcement should also be understood correctly. Compliance does not replace enforcement, but enforcement without compliance is economically shallow and administratively expensive. Public authorities cannot detect all breaches directly, particularly in complex cross-border systems involving intermediaries, dual-use goods, fragmented services, or layered ownership structures. They therefore rely heavily on firms to generate the first wave of restraint, reporting, record-keeping, and suspicious-pattern recognition. At the same time, compliance requires credible enforcement to avoid degenerating into selective convenience or symbolic procedure. The recent EU criminalisation initiative concerning violations of Union restrictive measures shows that the Union itself recognises the need to reinforce the punitive and investigative back end of the regime. Yet even criminalisation does not by itself generate operational effect. Its significance lies in strengthening the incentives under which firms maintain robust controls and in improving the consequences of deliberate evasion. Thus, enforcement is the coercive backstop, while compliance is the everyday transmission medium. A serious architecture requires both, but their functions are distinct. The law bites continuously through compliance and episodically through enforcement[4,5,6].

From the perspective of effectiveness measurement, this has an important implication. The success of sanctions cannot be inferred solely from the number of legal acts adopted, the number of persons listed, or even the number of enforcement cases concluded. It must also be assessed in terms of whether compliance systems are changing behaviour in the desired zones of exposure. Relevant indicators therefore include the quality of screening, the speed of list implementation, the reliability of ownership checks, the rate of escalations, the responsiveness to new red flags, the usability of guidance, and the capacity to preserve and share relevant information. This also means that apparent smoothness in trade or financial data may conceal intensive compliance friction beneath the surface. Transactions may be delayed, repriced, restructured, abandoned, or rerouted long before they appear in formal breach statistics. The analytical mistake is to treat enforcement outputs as the only visible trace of sanctions implementation. In reality, many of the most important sanctions effects occur in the compliance layer and remain only partially visible through aggregate enforcement data. For the Russian case, where adaptation and circumvention are substantial, this hidden layer is particularly consequential. A credible assessment of sanctions must therefore examine the quality of compliance transmission, not merely the breadth of legal drafting[7,8,9].

The Russian case also demonstrates why compliance should be treated as a pressure multiplier against a large adaptive state rather than as a narrow legal-administrative topic. Russia has not depended solely on direct bilateral transactions with the EU, but increasingly on intermediary jurisdictions, disguised procurement chains, layered logistics, and alternative service ecosystems. Under such conditions, a sanction measure that remains at the level of formal prohibition can be bypassed with relative ease. A measure that is operationalised through diligent screening, routing scrutiny, beneficial-ownership analysis, and typology-based detection becomes far harder to evade. Compliance therefore multiplies the reach of legal restrictions by extending them into the spaces where adaptation actually occurs. It follows circumvention into the grey zones of practical commerce. This is precisely why guidance

[1] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[3] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[4] European Commission. (2024, May 17). *New EU rules criminalising the violation of EU sanctions enter into force*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[7] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[8] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[9] European Commission. (2024, February 19). *Guidance on due diligence*.

documents now focus so heavily on red flags, strategic risk assessment, high-priority items, and successive due-diligence steps. The policy object is no longer just the obvious prohibited transaction. It is the broader ecosystem of risk through which Russian-linked actors attempt to reconstruct access to finance, goods, and services. Compliance is the mechanism that allows sanctions to operate within that ecosystem rather than outside it[1,2,3,4].

At the same time, it is necessary to recognise that the very strength of compliance as a transmission mechanism creates tensions that later sections of this report will address in more detail. When private actors carry substantial implementation responsibility, they may respond not only with accurate risk control but also with defensive caution. Ambiguous rules, opaque ownership, tight deadlines, and high penalty exposure may encourage broader refusal than the law strictly requires. This phenomenon does not negate the centrality of compliance. On the contrary, it confirms it. Over-compliance matters precisely because compliance is the mechanism through which sanctions acquire practical reach. If compliance were marginal, its excesses would not have systemic consequences. Because it is central, both under-compliance and over-compliance affect the real distribution of pressure, legality, and operational burden. The correct policy conclusion is therefore not to weaken compliance, but to govern it better through clearer drafting, better guidance, and more coherent supervisory expectations. Transmission quality, not merely transmission intensity, is the relevant standard[5,6,7].

Compliance also occupies an important boundary position between the legal and hybrid dimensions of the sanctions' regime. Hybrid sanctions, as argued in Part Six, operate through cross-domain disruption of enabling systems, intermediary networks, and adaptive infrastructures. Yet those hybrid measures often become effective only when compliance functions translate them into concrete denials of service, refusals of cover, route disruption, enhanced scrutiny, or partner disengagement. In that sense, compliance is not itself identical to the hybrid instrument, but it is often the mechanism through which hybrid pressure is realised. The distinction is analytically necessary. Hybrid design identifies the pressure zone, while compliance determines whether the pressure reaches it operationally. This is especially evident in areas such as shadow-fleet exposure, intermediary jurisdictions, high-priority goods, and network-based facilitation structures. The stronger the compliance conversion layer, the more difficult it becomes for adaptive Russian-linked networks to exploit fragmentation between legal design and market execution. Thus, compliance should be treated as a cross-cutting multiplier of other sanctions categories, even though it remains a distinct analytical dimension in its right[8,9].

For Brussels policy analysis, the most important strategic conclusion is that compliance determines whether sanctions remain governable under conditions of prolonged confrontation. The question for 2026–2030 is no longer simply whether the Union can adopt additional packages, but whether the accumulated sanctions architecture can be converted into consistent and sustainable operational practice across sectors and Member States. That depends on the usability of legal acts, the speed of updates, the accessibility of guidance, the quality of risk communication, and the ability of private operators to absorb obligations without collapsing into paralysis or indifference. The Commission's guidance ecosystem, the helpdesk model, the consolidated FAQ structure, and the emphasis on

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2023, September 7). *Sanctions: Commission publishes guidance to help European operators assess sanctions circumvention risks*.
[3] European Commission. (2024, September 24). *Sanctions vis-à-vis Russia: Commission publishes G7 Industry Guidance on preventing sanctions evasion*.
[4] U.S. Department of Commerce, Bureau of Industry and Security. (2024, February 23). *Common High Priority Items List (CHPL)*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[8] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[9] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

enhanced due diligence all point in the same direction. Sanctions policy is now a field of continuous operational governance, not a sequence of isolated political announcements. Compliance is the main medium through which this continuous governance is exercised. It links law to markets, policy to transactions, and geopolitical intent to everyday commercial behaviour. Without it, sanctions remain declaratory. With it, they become a durable regime of structured constraint[1,2,3,4].

The point can therefore be stated in a final and concentrated form. Compliance is the operational transmission mechanism of sanctions because it is the institutional process that carries restrictive norms from the level of legal adoption to the level of distributed behavioural modification. It performs this function through screening, due diligence, ownership analysis, escalation, refusal, reporting, licensing checks, and the continual updating of risk-sensitive controls. It is exercised by private actors, but under public law and in interaction with public authorities. It produces both direct interruption and anticipatory deterrence. It is indispensable in finance, trade, logistics, insurance, and service provision, and it becomes even more central when circumvention is adaptive and networked, as in the Russia case. It is supported by guidance, lists, helpdesks, and reporting tools because the Union itself recognises that sanctions only work when operators can convert rules into decisions. It also requires credible enforcement and better data architecture, because transmission weakens where certainty, capacity, or incentives are poor. For all these reasons, compliance should not be described as a technical supplement to sanctions policy. It is one of the principal mechanisms through which sanctions acquire real-world force[5,6,7,8,9].

7.1.2. The Governance Logic of Compliance: From Legal Obligation to Risk-Based Control

The governance logic of sanctions compliance begins with a basic but often misunderstood point: a legal prohibition does not automatically generate controlled behaviour. It generates an obligation, but the obligation must still be interpreted, internalised, operationalised, and monitored within the institutions that actually move money, goods, services, data, and contractual commitments across borders. For that reason, compliance governance should be analysed as the architecture that converts a norm into a control environment. The transition is not linear in a purely formal sense, because firms do not simply "apply the law" as a judge would. They construct risk-sensitive procedures that allow the law to be recognised at decision points where transactions are initiated, approved, processed, modified, delayed, escalated, or rejected. In sanctions policy, this means that the object of governance is not only legal obedience but operational foresight. It is not enough to know that a transaction would be unlawful if completed. The system must be designed so that the transaction is identified before completion, paused if necessary, assessed against available evidence, and recorded in a manner that supports defensibility and possible supervisory review. This is why modern sanctions compliance is built less around abstract prohibition and more around organised anticipatory control. The legal act remains the starting point, but the practical regime is a sequence of risk-based governance decisions embedded in ordinary commercial processes. In the EU and partner practice alike, guidance materials increasingly reflect

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Commission. (2025, November 17; last updated March 13, 2026). *Overview of sanctions and related resources*.
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[4] European Commission. (2024, February 19). *Guidance on due diligence*.
[5] Ibid.
[6] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[8] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[9] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

exactly this model, emphasising structured due diligence, internal controls, escalation, and documentation rather than mere awareness of restrictive measures[1,2,3].

This governance logic is best understood as a translation from rule-based obligation to risk-based control. Rule-based obligation answers the question of what is forbidden, restricted, licensed, exempted, or reportable. Risk-based control answers a different question: where, in the firm's activities, is exposure most likely to arise, and what organisational tools are necessary to detect and manage it? The second question is not derivative in a trivial sense. It requires a firm to assess business lines, jurisdictions, customer categories, product types, distribution channels, intermediaries, payment flows, transport routes, service interfaces, and document reliability. The OFAC compliance framework formulates this explicitly by placing risk assessment alongside management commitment, internal controls, testing, and training as essential components of an effective sanctions' compliance programme. The Commission's due-diligence guidance adopts the same basic logic, stating that there is no one-size-fits-all approach and that each operator must calibrate its controls to its own sanctions' exposure. This means that governance in the sanctions field is not exhausted by legal classification. It includes organisational mapping, prioritisation, and periodic recalibration. Firms are expected to identify their own vulnerability points and to design controls proportionate to those points. A mature compliance system therefore behaves less like a static legal manual and more like a structured risk-governance framework. That is the deeper logic by which sanctions move from formal obligation to workable control[4,5].

Due diligence is the first major institutional expression of that transition. In legal terms, due diligence is not always described as an autonomous sanction. In governance terms, however, it is the practical medium through which exposure is investigated before an irreversible step is taken. The Commission's Russia-related guidance and due-diligence materials make clear that operators are expected to examine business partners, transactions, goods, and routes with a degree of seriousness proportionate to the risk at issue. This means verifying identity, commercial rationale, ownership structure, delivery pathways, end-use claims, and the consistency of accompanying documents. Due diligence therefore functions as a pre-transactional filter and as a continuing discipline of verification. It is especially important where sanctions evasion relies on fragmented chains in which no single data point appears conclusive in isolation. A legitimate-looking invoice may sit beside an implausible shipping route, an apparently acceptable customer may sit within a suspicious ownership structure, and a non-listed counterparty may be acting for the benefit of a designated person. Due diligence is the process by which those fragments are brought into analytical relation. Without it, the legal obligation remains too coarse to govern complex transactions. With it, the firm creates an evidence-based basis for acting before exposure crystallises into breach[6,7,8].

Screening is the second major control layer, but it should not be reduced to simplistic list matching. In many organisations, screening begins with basic automated comparison of names, identifiers, vessel information, account data, or other structured fields against sanctions lists. Yet the governance value of screening depends on design choices that go far beyond software acquisition. A screening system must reflect the frequency of updates, the logic of fuzzy matching, the treatment of transliteration differences, the handling of false positives, the relationship between customer screening and transaction screening, and the authority to halt processing while an alert is reviewed. Screening is therefore not only a technical

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] European Commission. (2024, February 19). *Guidance on due diligence*.
[4] Ibid.
[5] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[6] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[7] European Commission. (2024, February 19). *Guidance on due diligence*.
[8] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.

instrument but an institutional workflow. It requires governance over thresholds, responsibilities, review quality, and escalation timing. OFSI's 2026 general guidance and OFAC's compliance framework both point toward this broader understanding by linking screening to compliance obligations, ownership analysis, reporting, and internal controls. The same logic appears in EU practice, where consolidated lists and consolidated FAQs exist precisely because screening requires usable, accessible, updatable information rather than merely formal acts in the *Official Journal*. Screening, then, is the front-end control through which a broad legal regime becomes operationally searchable. But its quality depends on the governance arrangements around it, not simply on its existence[1,2,3].

Internal controls are what transform screening and due diligence from isolated actions into a durable compliance system. A firm may possess a list-screening tool and still remain poorly governed if there is no clear policy architecture defining who screens, when screening occurs, what documentation must be collected, what constitutes an alert, who can override a warning, and what happens when relevant information is incomplete. OFAC's framework is especially influential here because it formalises the idea that internal controls are an indispensable pillar of sanctions governance. Controls are needed to ensure that policies are not merely aspirational, that process ownership is assigned, that gaps are tested, and that business operations do not silently bypass compliance. In the EU environment, this logic is reinforced by the Commission's insistence on tailored due diligence and by the growing body of FAQs designed to reduce interpretative inconsistency at the operational level. Internal controls also create temporal discipline. They define at what stage of a customer relationship or transaction the review must occur, how often screening must be refreshed, and what events trigger enhanced review. Such controls turn broad sanctions rules into repeatable and auditable conduct. Without them, the governance of compliance remains discretionary and fragile. With them, legal obligation is converted into institutional routine[4,5,6].

Escalation procedures form the next indispensable layer because sanctions risk often presents itself through ambiguity rather than certainty. A transaction may not obviously match a listed person, but the ownership structure may be opaque, the route commercially implausible, the goods diversion-sensitive, or the document package internally inconsistent. In such cases, governance must ensure that uncertainty does not default automatically to transaction completion. An effective compliance system therefore requires escalation channels that move a case from front-line operations to legal, compliance, senior management, or specialised review when defined triggers are met. Escalation is not a sign of failure. It is the mechanism by which organisations preserve decision quality under uncertainty. It prevents business units from resolving complex sanctions questions through speed, habit, or commercial pressure alone. It also helps distinguish between manageable risk and unacceptable exposure. OFAC's framework, as well as partner guidance in the UK, implicitly relies on this logic because risk-based control cannot function if every alert is either ignored at the front line or paralysed indefinitely without authority to decide. Escalation creates structured judgement. It is the governance bridge between automated signals and defensible human decision-making[7,8].

Licensing checks illustrate particularly clearly how sanctions governance moves beyond prohibition into calibrated control. Many sanctions regimes contain exemptions, derogations, specific licences, general licences, or other legal pathways through which conduct that would otherwise be restricted may

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026a, January 28). *UK financial sanctions general guidance*.
[3] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[4] European Commission. (2024, February 19). *Guidance on due diligence*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[7] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[8] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

proceed under defined conditions. This does not weaken the governance model. On the contrary, it complicates it in a legally significant way. Firms must not only know what is prohibited; they must know when a transaction may be authorised, by whom, on what evidence, with what record-keeping duties, and subject to what limits. OFSI's general guidance expressly positions licensing and compliance issues together, while its annual review emphasises the operational significance of improving transparency and responsiveness in licensing. In the EU context, the extensive consolidated FAQs perform a parallel function by clarifying how derogations and permissions should be interpreted under the Russia-related regulations. Licensing checks therefore become a core governance activity. They ensure that legitimate humanitarian, legal, contractual, or administrative exceptions are processed through lawful channels rather than through informal guesswork or excessive refusal. A mature compliance architecture must therefore distinguish between prohibited, permissible, licensable, and reportable conduct. That distinction is one of the places where legal obligation most visibly becomes risk-based operational control[1,2,3].

Beneficial-ownership verification is perhaps the clearest example of why risk-based control cannot stop at formal counterparties. In many sanctions-related transactions, the immediate legal person appearing in a contract, invoice, account record, or shipping document is not the economically relevant actor. The real question is whether that entity is owned, controlled, or significantly influenced by a designated person or by a network established to conceal sanctions nexus. FATF's work on beneficial ownership and transparency directly addresses this problem by emphasising that opaque corporate and legal arrangements enable sanctions evaders and other illicit actors to obscure control and beneficial interest. OFSI's 2026 ownership-and-control review underscores the same point, making explicit that firms are expected by law to assess ownership and control rather than relying only on surface-level list screening. Governance in this field therefore requires corporate-structure analysis, review of shareholder information, scrutiny of trusts and nominees where relevant, examination of indirect holdings, and structured judgement about de facto influence. This is not merely a legal nicety. It is the means by which compliance reaches beyond nominal legal form into actual control reality. For Russia-related exposure, this is decisive because circumvention frequently depends on layered, cross-jurisdictional, and partially concealed structures. A compliance system that cannot perform meaningful beneficial-ownership verification is not risk-based in any serious sense. It is only formally compliant at the surface level[4,5,6].

Record-keeping is often underestimated because it lacks the dramatic visibility of asset freezes or rejected shipments, yet it is one of the core pillars of sanctions governance. A risk-based system cannot function merely through one-off judgement. It must be able to explain, retrospectively and systematically, why a customer was onboarded, why a transaction was stopped, why an alert was cleared, why a licence was considered sufficient, and what information was available at the time. Record-keeping therefore serves several governance functions simultaneously. It preserves institutional memory, supports internal consistency, enables testing and audit, facilitates supervisory review, and protects the organisation when a decision is later questioned. UK guidance explicitly links sanctions obligations with reporting and record-related responsibilities, including in relation to licensing and frozen assets. Trade-sanctions guidance likewise indicates that information requests and record-keeping duties are not ancillary but enforceable parts of the regime. In the EU sphere, the same logic is reflected indirectly in the importance attached to due diligence, reporting, and evidence-based implementation. Record-keeping turns compliance from a series of ephemeral choices into an

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] Financial Action Task Force. (2024, March 11). *Guidance on Beneficial Ownership and Transparency of Legal Arrangements*.
[5] Financial Action Task Force. (2023, March 10). *Guidance on Beneficial Ownership of Legal Persons*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.

accountable governance process. Without documentary traceability, risk-based control quickly becomes unprovable, uneven, and difficult to defend[1,2,3].

The logic of risk-based governance also requires that compliance controls be differentiated across sectors rather than uniformly copied. The relevant risks of a bank, a maritime insurer, a freight forwarder, a dual-use exporter, a crypto-service provider, and a professional advisory firm are not identical. This is precisely why both OFAC and OFSI have supplemented general frameworks with sector-sensitive guidance. OFAC has issued targeted materials for instant payment systems, virtual currency businesses, and the maritime sector, each of which recognises that the architecture of exposure differs with the structure of the service. The governance lesson is clear. A credible sanctions compliance system must be risk-based not only in the abstract but in relation to the operational ecology of the sector concerned. Screening frequency, due-diligence triggers, typology awareness, documentary demands, and escalation thresholds may legitimately differ across contexts. However, the underlying governance logic remains constant. The firm must identify where sanctions exposure is likely to arise and build controls responsive to that exposure. This is why "copy-and-paste compliance" is structurally weak. It mimics policy language without governing the actual risk environment in which the business operates[4,5,6].

In the trade-control context, the shift from legal obligation to risk-based control is especially visible in end-use and end-user due diligence. A legal text may prohibit export, re-export, transfer, or brokering of specific goods or services under specified conditions. Yet in practice, the governance challenge lies in detecting when formally lawful-seeming transactions conceal diversion risk. The Commission's Russia circumvention guidance, the enhanced due-diligence document for common high-priority items, and BIS materials all indicate that operators must move beyond commodity classification alone. They must assess whether the customer profile fits the goods, whether the destination is plausible, whether routing signals diversion risk, whether documentation is coherent, and whether the transaction contains red flags associated with military-industrial procurement or sanctions evasion. This is a governance model of pattern recognition built on legal obligation. The law tells firms what exposure matters. Risk-based control tells them how to search for it in the ordinary flow of trade. For Russia-related sanctions, this has become indispensable because the most consequential violations are often not openly direct but strategically disguised. End-use diligence therefore becomes one of the principal means by which trade restrictions acquire practical force[7,8,9].

The same pattern appears in financial compliance, where the governance objective is no longer simply to identify listed names but to control the financial pathways through which restricted actors, sectors, or transactions might still obtain access. OFSI's general guidance and OFAC's framework both place heavy emphasis on risk awareness, compliance resourcing, and internal procedures capable of addressing actual exposure. The operational question is whether payments, account relationships, correspondent channels, trade-finance instruments, insurance-linked transfers, or service fees present sanctions nexus. This requires institutions to combine screening with transaction monitoring, customer due diligence, adverse-information review, and event-driven re-assessment. It also requires a governance model that can manage urgency without sacrificing control, since payment systems

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[2] HM Government. (2026, March 12). *Russia sanctions: statutory guidance*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] U.S. Department of the Treasury, Office of Foreign Assets Control. (2021, September 21). *Sanctions Compliance Guidance for the Virtual Currency Industry*.
[5] U.S. Department of the Treasury, Office of Foreign Assets Control. (2021). *Sanctions Compliance Guidance for Instant Payment Systems*.
[6] U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.
[7] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[8] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*
[9] U.S. Department of Commerce, Bureau of Industry and Security. (2024, February 23). *Common High Priority Items List (CHPL)*

frequently operate under high speed and high volume. The emergence of guidance for instant payment systems is especially revealing in this respect. Authorities recognise that innovation in financial infrastructure does not remove sanctions obligations. It intensifies the need to redesign controls so that speed does not become a vector of evasion or inadvertent breach. Thus, the governance logic of sanctions compliance is inseparable from the evolution of operational tempo in modern finance[1,2,3].

Testing, auditing, and review are central to this governance logic because sanctions exposure is not static. A compliance system that was adequate when first designed may become weak as business models expand, product offerings change, software ages, ownership structures become opaquer, or circumvention typologies evolve. OFAC's framework explicitly treats testing and auditing as essential components of a sanctions' compliance programme. This is not just good governance in general. It is essential in sanctions policy because the consequences of unnoticed control deterioration can be severe, both legally and strategically. Regular review allows firms to detect false negatives, unmanageable false positives, unclear escalation routes, documentation gaps, inconsistent approvals, and training failures. It also allows management to identify whether the control environment still aligns with the actual pattern of risk. A risk-based model without review becomes merely historical. It reflects an earlier risk map rather than the present one. Continuous review therefore completes the governance cycle: legal rule, risk identification, control design, implementation, testing, correction, and re-implementation. That cycle is what distinguishes a living compliance architecture from a static policy binder[4,5].

Training serves a similarly structural function because risk-based governance depends on decision quality at multiple levels of the organisation. Front-office staff, onboarding teams, trade operations personnel, logistics coordinators, legal reviewers, finance departments, and senior approvers do not encounter sanctions risk in the same form. Yet all of them may control a part of the transaction chain at which exposure becomes visible or should have become visible. Training is therefore not reducible to awareness sessions on the existence of sanctions. In governance terms, it is the distribution of operational literacy across the organisation. Staff must know what red flags look like in their own workflow, what must be documented, when escalation is mandatory, and what cannot be resolved by commercial judgement alone. OFAC again treats training as an essential component, and the broader guidance environment in the EU and UK points in the same direction even when expressed through due-diligence and reporting expectations rather than through a single unified compliance doctrine. Training matters because even well-designed controls fail when users do not understand the logic behind them. A risk-based architecture is only as effective as the interpretative competence of the people expected to use it[6,7,8].

Another important feature of the governance logic is that it seeks not total elimination of uncertainty, but controlled management of uncertainty. Sanctions compliance regularly operates in situations where evidence is partial, legal definitions require interpretation, and commercial facts do not align neatly with formal categories. Risk-based control does not promise mathematical certainty in such settings. It creates procedures for acting responsibly despite imperfect information. That is why due diligence, escalation, record-keeping, and review matter so much. They do not eliminate ambiguity, but they make decisions disciplined, explainable, and more resistant to both recklessness and arbitrariness. This point is particularly important in the Russia context, where evasive behaviour often depends on maintaining

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2021). *Sanctions Compliance Guidance for Instant Payment Systems*.
[3] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[4] Ibid.
[5] European Commission. (2024, February 19). *Guidance on due diligence*.
[6] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[7] European Commission. (2024, February 19). *Guidance on due diligence*.
[8] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

ambiguity long enough for a transaction to clear. Governance is therefore successful not when it produces omniscience, but when it prevents ambiguity from defaulting into permissive execution. A good system converts uncertainty into a trigger for enhanced scrutiny rather than a reason for administrative passivity. That is one of the core features of risk-based control as a governance model[1,2].

Table 7.1.2-1. Governance Transition from Legal Obligation to Risk-Based Control

Governance layer	Core question	Principal instruments	Operational purpose
Legal obligation	What is prohibited, restricted, licensed, exempted, or reportable?	Regulations, listings, FAQs, statutory guidance	Establish the normative perimeter
Risk identification	Where is the firm exposed?	Risk assessment, business-line mapping, geographic and sectoral analysis	Locate sanctions-sensitive activity
Preventive verification	Is the counterparty, route, transaction, or use-case acceptable?	Due diligence, screening, BO/UBO checks, end-use review	Detect exposure before execution
Decision control	Who decides when risk is uncertain or elevated?	Escalation channels, approval matrices, legal/compliance review	Prevent uncontrolled or premature execution
Conditional permissibility	Can the activity proceed lawfully under authorisation?	Licensing checks, derogation assessment, reporting duties	Distinguish prohibited from authorised conduct
Accountability and resilience	Can the decision be defended, audited, and improved?	Record-keeping, testing, audit, training, periodic review	Sustain consistency and corrigibility

Authorship: prepared by the author on the basis of official EU institutional materials and United States' materials.
Sources:

- European Commission. (2023, September 7). Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention.
- European Commission. (2024, February 19). Guidance on due diligence.
- European Commission. (2026, March 13). Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). UK financial sanctions general guidance.
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). A Framework for OFAC Compliance Commitments.
- Financial Action Task Force. (2024, March 11). Guidance on Beneficial Ownership and Transparency of Legal Arrangements.

From a governance perspective, public guidance performs a function that is more substantive than explanatory. It does not merely restate law for convenience. It reduces implementation entropy across thousands of private and public actors that must act on the same sanctions' framework under time pressure and with uneven expertise. The existence of extensive EU FAQs, due-diligence guidance, and anti-circumvention documents indicates that authorities themselves recognise that legal obligation alone is too thin a medium for uniform application. Public guidance helps translate regulatory intent into operational assumptions. It narrows the zone in which divergent interpretations arise, clarifies what evidence matters, and signals what forms of risk deserve heightened attention. In that sense, guidance is part of governance, not a supplement to it. It shapes how firms convert law into internal procedure. This also explains why delayed or fragmented guidance can weaken sanctions policy even when the legal

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

texts themselves are unchanged. The governance quality of a sanctions' regime depends partly on whether the law is made operationally legible to those who must implement it every day[1,2,3].

The public–private relationship is therefore built into the governance logic of compliance itself. States and supranational institutions determine the normative framework, but firms and regulated intermediaries' control much of the operational space in which sanctions succeed or fail. This does not make private actors sovereign over sanctions policy. It makes them indispensable carriers of implementation. The governance question is how to structure that role so that private actors neither under-apply the law through negligence nor over-apply it through indiscriminate defensive withdrawal. Risk-based control is the chosen answer because it permits differentiated management of exposure while preserving the legal core of the regime. But that answer only works if public authorities provide enough clarity, accessibility, and supervisory coherence to make reasoned private implementation possible. The more complex the circumvention environment becomes, the more this public–private governance relationship matters. In the Russia case, where third-country intermediaries, proxy entities, and fragmented routing have become central to evasion, the private sector often sees suspicious patterns before the state does. A well-governed sanctions regime therefore treats firms not only as potential violators but as institutional partners in early detection and controlled interruption[4,5].

This governance model also explains why sanctions compliance is inseparable from proportionality. A risk-based regime is not supposed to require the same depth of inquiry for every transaction, every customer, and every product. It is designed to allocate scarce compliance resources toward the areas of greatest exposure. OFAC has articulated this principle directly in Russia-related advisory materials, encouraging institutions to deploy compliance resources toward products, services, business lines, and locations most likely to facilitate activity involving Russia's military-industrial base. The same logic underlies EU guidance on enhanced due diligence and common high-priority items. Proportionality is therefore not a relaxation of governance. It is a condition of governance effectiveness. Systems that attempt to treat all activity as equally risky often produce alert fatigue, weak prioritisation, and deterioration in decision quality. By contrast, systems that identify where risk is concentrated can act more quickly and more credibly where it matters most. The transition from legal obligation to risk-based control is thus also a transition from abstract universality to operational prioritisation[6,7].

At the same time, risk-based control is not a licence for loose discretion or purely commercial balancing. That danger is precisely why governance structures must be documented, reviewable, and anchored in legal obligation. A firm cannot justify weak due diligence merely by saying that it judged the risk to be low. Nor can it legitimise selective blindness toward suspicious intermediaries by invoking commercial practicality. Risk-based governance demands reasoned calibration, not opportunistic downgrading of controls. This is another reason why record-keeping, testing, and supervisory expectations matter so much. They make risk-based control contestable and therefore governable. In effect, they prevent the language of proportionality from being misused as a euphemism for convenience. A serious sanctions regime must therefore maintain a dual commitment: flexible enough to respond to differentiated risk,

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2024, February 19). *Guidance on due diligence*.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[5] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[6] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[7] U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, June 12). *Sanctions Advisory*.

but disciplined enough to prevent flexibility from collapsing into inconsistency or evasion tolerance. That balance is one of the central governance tasks for the 2026–2030 sanctions environment[1,2,3].

For the Russian sanctions track specifically, the evolution from legal obligation to risk-based control has been driven by the practical limits of static prohibition in an adaptive environment. As Russia and Russia-linked networks expanded use of third-country hubs, layered service provision, opaque ownership structures, and disguised procurement channels, the older model of simple prohibition plus after-the-fact enforcement became increasingly insufficient. Authorities responded by building a denser compliance governance ecosystem centred on enhanced due diligence, typology recognition, beneficial-ownership transparency, licensing clarity, and better information architecture. This shift is not cosmetic. It marks the recognition that sanctions policy against a large adaptive target must be implemented as a dynamic control system. The legal norm remains essential, but it is no longer the decisive operational variable on its own. What matters equally is the quality of the governance chain that surrounds it. That chain determines whether law remains declaratory or becomes behaviourally effective across the infrastructures through which Russia seeks to preserve external access. In this sense, the governance logic of compliance is not merely administrative theory. It is one of the central conditions of sanctions effectiveness in prolonged geopolitical confrontation[4,5,6].

The main conclusion is therefore clear. The governance logic of compliance consists in converting legal obligation into a differentiated, documented, auditable, and adaptable control environment. It does so through due diligence, screening, internal controls, escalation procedures, licensing checks, beneficial-ownership verification, record-keeping, training, and periodic review. Each of these elements answers a different operational question, but together they form a coherent governance architecture. That architecture is risk-based because modern sanctions exposure is distributed unevenly and concealed strategically. It is still law-bound because controls must remain anchored in normative obligation rather than commercial preference alone. For the EU sanctions regime, and especially for the Russia track, this model has become indispensable. It is the practical means by which restrictive measures are made usable by firms, governable by authorities, and effective against increasingly adaptive patterns of circumvention. A sanctions regime that stops at prohibition is incomplete. A sanctions regime that builds a credible risk-based control architecture begins to operate as a durable system of real-world constraint[7,8,9,10] .

7.1.3. Public–Private Interface in Sanctions Implementation

The public–private interface in sanctions implementation is not a secondary organisational detail but one of the constitutive features of the modern sanctions' regime. Restrictive measures are adopted by public authorities, interpreted through public law, and ultimately backed by public enforcement powers. Yet their daily practical effect is generated at the points where private actors decide whether to onboard a customer, process a payment, release cargo, insure a vessel, execute a contract, or continue a service relationship. The sanctions system therefore operates through a hybrid chain of authority and execution rather than through a simple command-and-control model. Public institutions define the normative

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] European Commission. (2024, February 19). *Guidance on due diligence*.
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] Financial Action Task Force. (2024, March 11). *Guidance on Beneficial Ownership and Transparency of Legal Arrangements*.
[6] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[7] Ibid.
[8] European Commission. (2024, February 19). *Guidance on due diligence*.
[9] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[10] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

perimeter, but private operators convert that perimeter into operational decisions. This makes sanctions implementation a field of co-produced governance in which state and market actors perform different but interdependent functions. The state cannot achieve implementation alone because it does not sit inside every transaction. Private actors cannot govern autonomously because their role derives from legal obligations, supervisory expectations, and enforcement risk. The real architecture is therefore relational. Compliance is shaped in the space where public mandate and private operational capacity meet[1,2,3].

In the EU context, this interface is structurally multi-level. The Union adopts sanctions through the CFSP and, where necessary, through directly applicable regulations, but the implementation and enforcement of those sanctions rest primarily with the Member States. The Commission's own sanctions overview states that investigation of potential non-compliance cases falls to the Member States and their national competent authorities, while the Commission monitors implementation and enforcement across the Union. The same materials also stress that Member States are responsible for identifying breaches and imposing penalties. This division of labour means that the public side of the interface is already internally plural before the private sector even enters the picture. It includes EU institutions that design, coordinate, and clarify the regime, and national authorities that authorise, investigate, and penalise within domestic legal systems. Private operators therefore do not interact with a single "state" actor, but with a layered governance structure. This complexity partly explains why guidance, coordination, and common best practices have become so important. Without them, the interface would fracture into multiple national implementation environments and generate uneven signals for firms operating cross-border. Public–private implementation in the EU is thus inseparable from public–public coordination inside the Union itself[4,5,6].

At Union level, the Commission occupies a central interface-management role rather than a purely legislative or symbolic one. According to the Commission's sanctions overview, DG FISMA monitors the implementation and enforcement of EU sanctions across all Member States and increasingly supports Member States by answering interpretation questions raised by national competent authorities as well as economic and humanitarian operators. That formulation is highly revealing. It shows that the Commission is not merely producing abstract policy statements. It is actively sustaining a common interpretative space in which both authorities and operators can work. The consolidated FAQ architecture performs the same interface function. It provides a shared frame for national authorities, businesses, and other stakeholders dealing with legally complex and fast-evolving restrictions. The EU Sanctions Helpdesk extends this operational support even further by offering free personalised assistance to firms, particularly SMEs, undertaking sanctions due diligence. These mechanisms illustrate that the Union now treats implementation not as a purely downstream enforcement matter but as an ongoing governance relationship with market actors. The Commission is therefore best understood as an interface stabiliser. It helps reduce interpretative fragmentation between law on paper and compliance in practice[7,8,9].

National competent authorities remain the most immediate public interlocutors for private operators. The Commission's contacts page states explicitly that the primary responsibility for the implementation of EU sanctions rests with the Member States and that EU operators looking for guidance on specific issues should first and foremost reach out to their national competent authority. This is one of the

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[2] European Commission. (n.d.). *Overview of sanctions and related resources*
[3] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*
[4] European Commission. (n.d.). *Overview of sanctions and related resources*.
[5] European Commission. (n.d.). *Contacts on EU sanctions*.
[6] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[7] European Commission. (n.d.). *Overview of sanctions and related resources*.
[8] European Commission. (2025, June 11). *Sanctions implementation*.
[9] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

clearest institutional signals in the current architecture. It confirms that the interface is not designed around direct centralised micro-management from Brussels. Instead, firms are expected to operate primarily through national legal-administrative channels, even while the broader framework remains European. National competent authorities are therefore the core public nodes through which licensing, derogations, reporting, interpretative queries, and enforcement follow-up are organised. Their practical accessibility matters enormously for compliance quality. Where NCAs are responsive, clear, and coordinated, firms are more likely to escalate difficult cases rather than either ignore them or default to indiscriminate de-risking. Where NCAs are slow, opaque, or inconsistent, the public–private interface becomes less predictable and more defensive. The effectiveness of the EU sanctions regime thus depends substantially on the quality of these national contact points and not only on the content of Union regulations[123].

The Council's 2024 Best Practices document makes this multi-actor structure even more explicit by describing implementation as a coordinated process across numerous public bodies and by assigning a recognised role to economic operators and citizens. The document includes a dedicated section on the "role of economic operators and citizens" and states that economic operators are obliged to provide information facilitating compliance, to report indications that funds or economic resources may have been made available without authorisation, and to cooperate with competent authorities in the verification of information. This is not a marginal procedural note. It formalises the private sector as part of the implementation chain rather than as a passive object of public supervision. The same document also provides that competent authorities may exchange relevant information with the Commission, the Council, the EEAS, competent authorities of other Member States, law enforcement bodies, courts, investigating and prosecuting authorities, and, where necessary, credit and financial institutions. In other words, the public–private interface is embedded in a broader information-sharing web that stretches well beyond a bilateral regulator-firm relationship. Sanctions implementation is presented here as a coordinated ecosystem. That ecosystem has public leadership, but it depends on private informational input and operational cooperation to function effectively[4].

A particularly important part of that public side is national inter-agency coordination. The Council's Best Practices state that Member States should ensure efficient national coordination and communication mechanisms between all relevant government agencies, bodies, and services with competence in restrictive measures, including ministries, FIUs, financial supervisors, intelligence and security services, judicial authorities, prosecutors, and other law-enforcement bodies as appropriate. This formulation matters because it shows that implementation problems are rarely confined to one bureaucratic silo. A sanctions issue may begin as a compliance alert in a bank, appear as a suspicious routing pattern in customs data, develop into a criminal inquiry, and later generate prosecutorial or judicial action. If those state actors do not coordinate, the private sector receives fragmented signals and the regime loses coherence. The Council also recommends an intelligence-driven and risk-based approach and broader information exchange with other Member States, the Commission, the EEAS, Europol, Eurojust, FATF, and relevant UN bodies. This means that the public–private interface is only one layer of a larger coordination matrix. Firms stand at the edge of a state architecture that must itself be joined up if private reporting and compliance are to produce systemic effect. Sanctions implementation is therefore neither purely national nor purely European in its public dimension. It is an integrated field of nested authorities and cooperative channels[5].

Customs authorities illustrate especially well why sanctions implementation cannot be described as purely financial or purely legal. The Commission's customs page on EU measures following the Russian invasion of Ukraine explains that many sanctions measures have direct implications for the work of EU

[1] European Commission. (n.d.). *Contacts on EU sanctions*.
[2] European Commission. (n.d.). *Overview of sanctions and related resources*.
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[4] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[5] Ibid.

customs authorities, importers, and exporters. This reveals a classic interface structure. Public authorities control border release, customs status, and enforcement capacity, but they rely heavily on declarations, documents, classifications, and operational behaviour provided by traders, brokers, freight operators, and importers. The 2023 Commission guidance note on stopped goods makes the point even more concretely by stating that customs administrations in Member States are implementing various sanctions and, in some cases, have stopped goods subject to import and export prohibitions. The guidance also makes clear that customs must carefully assess whether release of blocked goods would create a circumvention risk. This is not a unilateral state act detached from private activity. It is a legally structured interaction in which customs, traders, and related operators must exchange information under conditions of uncertainty and time pressure. The customs layer therefore embodies the public–private interface in material form: goods, documents, declarations, and control decisions intersect at the border. That makes customs authorities among the most visible public executors of sanctions, but still not independent of private compliance quality[1,2].

The financial sector provides another crucial interface, but here the interaction is more continuous and less episodic than at customs. Banks, payment institutions, and other financial intermediaries occupy central positions in sanctions implementation because they process flows that are both rapid and deeply embedded in cross-border commercial life. Public authorities impose the legal obligation, but private institutions decide whether an alert is escalated, whether a transaction is paused, whether an account is frozen, whether a beneficial-owner check is sufficient, and whether a report is made. This explains why both the UK and EU-related supervisory frameworks place such emphasis on governance, internal controls, and reporting duties. It also explains why the EBA's 2024 guidelines are so important. The EBA stated that, for the first time, it was setting common EU standards on governance arrangements and policies, procedures, and controls that financial institutions should have in place to comply with Union and national restrictive measures. That step is essentially a form of interface engineering. It attempts to reduce divergence in how supervised firms operationalise public sanctions obligations. Financial sanctions implementation is therefore not only about legal restrictions on funds. It is about the supervisory structuring of private compliance conduct[3,4,5].

The EBA materials also show that the public–private interface increasingly operates through supervisory standard-setting rather than through ad hoc enforcement alone. The final guidelines are addressed both to competent authorities and to financial institutions, and they are designed to be used by supervisors when assessing internal policies, procedures, and controls adopted by firms. This dual addressee structure is analytically important. It means that the interface is not just a line between state and firm; it is a shared governance space in which authorities define expectations for how firms should organise themselves internally. The same EBA report notes that competent authorities had reported common deficiencies in screening systems, including outdated or incorrect lists, overreliance on vendors, weak understanding of those systems, inadequate frequency of screening, and limited fuzzy matching. It also records that technical screening alone is insufficient and must be complemented by strong processes relating to customers and beneficial owners. These are classic interface findings. They show that implementation problems arise where supervisory expectation, technical infrastructure, and institutional practice meet. The state does not merely punish private failure after the fact. It increasingly shapes the internal architecture through which private compliance is performed[6,7].

[1] European Commission, Directorate-General for Taxation and Customs Union. (n.d.). *EU measures following the Russian invasion of Ukraine*.
[2] European Commission. (2023, September). *Guidance note to Member States on stopped goods as a result of the sanctions*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[5] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[6] Ibid.
[7] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

Financial Intelligence Units add a further layer to this interface because they convert private reporting into public intelligence. The Commission's 2025 article on the 'Next-Generation' FIU.net states that the system gives FIUs and Europol improved capacity for information exchange and cross-matching, and that cross-border reporting enables FIUs to distribute suspicious transaction reports filed by obliged entities registered in one country but providing services in others. This is highly relevant for sanctions implementation even where the formal legal basis arises from AML/CFT structures. It demonstrates that firms are not merely expected to comply silently. They are also expected to generate intelligence signals that public authorities can analyse and share across borders. FIUs thus occupy a mediating position between private gatekeepers and investigative or prosecutorial authorities. They are part of the state, but their informational inputs frequently originate in private compliance systems. In sanctions terms, this matters because circumvention often manifests first as an unusual pattern rather than an immediately provable breach. The FIU layer helps transform suspicion into cross-border financial intelligence. Public–private implementation in this area is therefore iterative: firms detect anomalies, FIUs analyse and disseminate, and other authorities pursue follow-up[1,2].

The emerging role of AMLA further institutionalises this interface in the financial sector. According to the Commission's 2024 AML/CFT Questions and Answers, AMLA will check compliance with sanctions-related measures by the riskiest cross-border groups in the financial sector and will contribute to a common supervisory approach to verification of compliance with sanctions-related requirements. The same document adds that AMLA will provide critical input to the understanding and mitigation of risks of sanctions evasion or non-implementation at Union level. This is a significant development because it links sanctions implementation more closely to the broader European supervisory architecture for financial integrity. It also suggests that sanctions compliance is being normalised as a matter of supervisory governance rather than treated only as an exceptional foreign-policy overlay. AMLA does not replace national authorities or firm-level compliance functions. Instead, it strengthens convergence and risk visibility across jurisdictions and groups whose activities are inherently cross-border. That is precisely what a complex public–private interface requires. As sanctions implementation becomes more networked, central supervisory coordination becomes more valuable[3,4].

Private actors, for their part, should be understood as operational gatekeepers rather than as mere compliance subjects. Banks, exporters, insurers, shipping firms, payment providers, platforms, and professional intermediaries are situated at points where sanctions can actually interrupt a transaction or be bypassed. This is why the Council Best Practices assign information and cooperation duties to economic operators, and why the Commission's sanctions support tools are designed not only for public authorities but also for businesses. Private firms control transaction initiation, documentary collection, customer onboarding, route selection, service continuation, and payment execution. The state generally does not perform these tasks itself. It relies on the fact that firms occupy the chokepoints through which restricted activity must often pass. That reliance is not informal or accidental. It is built into the architecture of sanctions as a system of distributed implementation. In this sense, private actors are not substitutes for state enforcement but indispensable executors of first-instance operational control. Without them, most sanctions regimes would become vastly more expensive to police and far less effective in real time[5,6,7].

Corporate compliance teams are the institutional location where this private role is organised and translated into repeatable practice. They mediate between legal texts, business incentives, technical

[1] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[2] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[3] European Commission. (2024, April 24). *Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[6] European Commission. (2025, June 11). *Sanctions implementation*.
[7] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

screening tools, and external regulatory expectations. In governance terms, they are internal interface managers. They receive rules and guidance from public institutions, but they must re-express those rules in policies, escalation channels, screening logic, client-acceptance criteria, and documentation standards intelligible to commercial staff. Their work is therefore neither purely legal nor purely operational. It is a form of organisational translation. This is why recent EU and partner guidance increasingly stresses internal policies, procedures, controls, training, and testing. The public–private interface is not located only at the boundary between regulator and firm. It also runs through the inside of the firm, where public requirements are converted into business process. If that internal translation fails, the external legal rule remains weakly implemented. Compliance teams are thus a crucial intermediary layer within the broader interface architecture[1,2,3].

The EU Sanctions Helpdesk is especially important because it lowers the threshold for private-sector participation in implementation. The Commission's 2025 article explains that the helpdesk offers free personalised support to companies performing sanctions due-diligence checks and invites firms to submit either general sanctions questions or detailed due-diligence requests. The related contacts page also states that SMEs can receive personalised support through the Helpdesk. This is more than a convenience service. It is a governance instrument designed to strengthen interface usability, especially for firms that lack large in-house compliance teams. Large banks and multinational exporters may be able to absorb interpretative complexity internally. Smaller operators often cannot. If support is absent, those firms may either disengage excessively from legitimate business or underinvest in controls because the compliance burden appears too opaque. The Helpdesk therefore broadens the implementational capacity of the private side of the interface. It makes the sanctions regime more socially and economically governable by improving access to compliant participation rather than relying solely on post hoc deterrence[4,5,6].

Table 7.1.3-1. Public–Private Interface in EU Sanctions Implementation

Interface actor	Primary role	Type of interaction with other actors	Implementation significance
European Commission / DG FISMA	Monitoring, guidance, interpretative support, helpdesk, whistleblower intake	Supports Member States; answers operator queries; refers credible information to Member States	Stabilises Union-wide interpretation and reduces fragmentation
National competent authorities	Licensing, derogations, interpretation, enforcement, penalties	Main contact point for operators; coordinate with Commission and other NCAs	Core national public interface for firms
Customs authorities	Border implementation of import/export prohibitions	Interact with traders, brokers, importers, exporters, and Commission guidance	Convert sanctions into control over goods movement
Financial supervisors / EBA / AMLA	Supervisory standards, control assessment, convergence	Shape firms' internal controls and cross-border supervisory expectations	Harmonise compliance quality in finance
FIUs / FIU.net / Europol-linked channels	Intake, analysis, and exchange of suspicious financial information	Receive private-sector signals and disseminate intelligence across borders	Transform compliance alerts into actionable intelligence

[1] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[4] European Commission. (2025, June 11). *Sanctions implementation*.
[5] European Commission. (n.d.). *Contacts on EU sanctions*.
[6] European Commission. (n.d.). *Overview of sanctions and related resources*.

Interface actor	Primary role	Type of interaction with other actors	Implementation significance
Regulated firms and corporate compliance teams	Screening, due diligence, escalation, reporting, service denial	Translate public rules into internal controls and operational decisions	First-line execution of sanctions pressure
Whistleblowers / citizens / other stakeholders	Violation reporting	Provide information to Commission and relevant authorities	Expand detection beyond formal institutional channels

Authorship: prepared by the author on the basis of official EU institutional materials
Sources:

- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Commission. (n.d.). *Contacts on EU sanctions*.
- European Commission. (2025, June 11). *Sanctions implementation*.
- European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
- European Commission. (2024, April 24). *Questions and answers: Anti-money laundering and countering financing of terrorism (AML/CFT)*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

The Commission's whistleblower mechanism further widens the interface by allowing individuals aware of possible violations to submit information anonymously. The contacts page specifies that if the Commission considers the information credible and well documented, it will refer it to the relevant Member State or Member States together with its legal interpretation. This is a striking example of interface governance. The state is not waiting only for formal reports from regulated firms or for investigative authorities to discover breaches independently. It is constructing channels through which private and quasi-private knowledge can enter the enforcement system. The Commission also does not simply transmit raw information mechanically. It adds legal interpretation, thereby linking intelligence input with regulatory framing. This strengthens the connection between detection and action. It also demonstrates that sanctions implementation includes managed informational intermediation, not just command and compliance. Public–private interaction thus extends beyond the regulated firm and into the broader social environment of observability and reporting[1,2].

Licensing and derogations offer another clear example of why the interface is not reducible to enforcement. In many sanctions' regimes, the relevant public question is not simply whether to punish violation but whether and how to authorise specific conduct under legally defined exceptions. The Council Best Practices emphasise that competent authorities should inform other competent authorities and the Commission of rejected authorisation requests where the regulation so requires, and should still aim to notify rejected requests even where there is no explicit obligation, in order to minimise distortions of competition in the internal market. This reveals two important features of the interface. First, firms interact with public authorities not only as potential violators but as applicants seeking lawful pathways through prohibited space. Second, public actors themselves must coordinate their handling of those applications so that private parties do not forum-shop or receive materially divergent treatment across Member States. Licensing therefore transforms the interface into a channel of negotiated legality.

[1] European Commission. (n.d.). *Contacts on EU sanctions*.
[2] European Commission. (n.d.). *Overview of sanctions and related resources*.

It is not a relaxation of sanctions but a structured means of ensuring that exceptional permissions remain governable, transparent, and consistent[1,2,3].

This public–private structure also explains why implementation quality depends heavily on trust and usability. If firms regard public guidance as unclear, delayed, or internally inconsistent, they will often respond defensively by over-blocking, withdrawing services, or relying excessively on third-party screening vendors without sufficiently understanding their outputs. The EBA's 2024 report notes precisely such supervisory concerns, including overreliance on vendors and poor understanding of screening systems by firms. That is not merely a private deficiency. It is evidence of interface weakness. A well-designed interface should allow private actors to understand expectations clearly enough to make reasoned and reviewable decisions. A poorly designed interface amplifies both false negatives and false positives. The same is true when national authorities vary too sharply in responsiveness or interpretation. Public–private sanctions governance therefore requires more than legal authority. It requires interface credibility, meaning that the private sector sees escalation, consultation, and reporting as workable rather than futile. Without that credibility, implementation either deteriorates or becomes excessively defensive[4,5].

The reason compliance cannot be regarded as purely state enforcement is therefore practical as well as conceptual. States do not control the full informational and operational surface on which sanctions exposure appears. They do not originate every customer file, own every transaction-monitoring system, inspect every logistics decision in real time, or see every ownership anomaly before a deal is executed. Much of this visibility resides with firms. The Council Best Practices explicitly recognise this by requiring operators to provide information and cooperate in verification, while the Commission's tools are built to assist and receive inputs from operators. Compliance is thus distributed by design. The state provides legal force and coercive backing, but the private sector provides much of the early detection, operational interruption, and evidence generation. That does not privatise sanctions policy. It means that sanctions policy functions through a layered implementation ecology in which public enforcement alone would be insufficiently granular, slow, and costly. State enforcement is indispensable, but it is not self-sufficient[6,7,8].

This becomes even clearer in the Russia sanctions context because circumvention has been adaptive, transnational, and often networked through intermediaries. The Commission's anti-circumvention guidance and related due-diligence materials were issued precisely because authorities recognised that private operators needed help identifying patterns that did not always present as direct legal matches. Third-country routing, shadow ownership, obscure intermediaries, and fragmented service provision do not always first appear in public case files. They often appear in private transactional ecosystems as anomalies, implausible instructions, or documentary inconsistencies. The public–private interface is therefore a site of distributed intelligence, not merely distributed obedience. Firms detect signals because they are close to transactions. Public authorities contextualise, verify, coordinate, and enforce because they possess legal mandate and broader information powers. The two sides are not interchangeable, but neither can succeed alone under contemporary circumvention conditions. In

[1] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[7] European Commission. (n.d.). *Overview of sanctions and related resources*.
[8] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

practical terms, sanctions implementation against Russia has evolved into a shared detection-and-interruption environment[1,2,3].

Yet this interface also generates structural tensions. Private actors may over-comply to protect themselves against legal and reputational risk. National authorities may diverge in practice even when the formal rule is the same. Supervisors may push firms toward stronger controls, while operators experience alert overload and uncertainty over when reporting is actually required. The EBA's final report records consultation feedback warning that a requirement to report every suspicion of possible circumvention could flood competent authorities with incomplete or irrelevant information, and the EBA acknowledged that there is no general legal obligation of that kind across all circumstances. This exchange is instructive. It shows that interface design must balance information intake against usability and proportionality. Too little reporting weakens detection. Too much undifferentiated reporting can degrade analytical capacity on the public side and compliance efficiency on the private side. The public–private interface is therefore not simply about adding more obligations. It is about calibrating interaction so that information, scrutiny, and control remain decision-useful[4].

From a strategic perspective, the central policy lesson is that sanctions implementation should be treated as a system of managed interaction rather than a unilateral act of sovereign imposition. EU institutions, NCAs, customs, FIUs, supervisors, prosecutors, firms, and corporate compliance teams all occupy different positions in the same implementation chain. The quality of their interaction determines whether sanctions remain credible, navigable, and effective under prolonged geopolitical strain. Better guidance, faster interpretation, higher-quality supervisory convergence, more usable support for firms, and stronger channels for cross-border intelligence exchange all improve the interface. The opposite tendencies—fragmentation, opacity, inconsistent national practice, and private-sector fatigue—degrade it. The EU's recent institutional developments point strongly toward the first model. Helpdesks, FAQs, whistleblower tools, EBA guidelines, stronger supervisory convergence, AMLA-related powers, customs guidance, and FIU.net modernisation all show a move toward a more structured interface architecture. This is not bureaucratic overgrowth. It is the practical recognition that sanctions now operate through networks of interaction rather than through isolated legal commands. The public–private interface is therefore not incidental to sanctions implementation. It is one of its principal operating conditions[5,6,7,8].

The broader conclusion is thus straightforward. Sanctions compliance is not purely state enforcement because the state does not occupy all the operational sites where compliance must occur. Nor is it private self-regulation because private action derives from public norms, public supervision, and public penalty frameworks. It is a hybrid implementation order built on reciprocal dependence. Public authorities need private visibility, transaction-level control, and reporting capacity. Private firms need public clarity, licensing pathways, interpretative support, and coherent supervisory expectations. The more adaptive the circumvention environment becomes, the more this reciprocal structure matters. In the Russia-related sanctions field, that reality is now unmistakable. Effective implementation depends less on the abstract existence of sanctions than on the quality of the public–private interface through which they are carried into actual market behaviour. That interface is therefore not a technical sidebar

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2024, February 19). *Guidance on due diligence*.
[3] Financial Action Task Force. (2025, June 9). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] European Commission. (2025, June 11). *Sanctions implementation*.
[6] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[7] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[8] European Commission. (2024, April 24). *Questions and answers: Anti-money laundering and countering financing of terrorism (AML/CFT)*.

to sanctions policy. It is one of the decisive determinants of whether sanctions remain legally credible and operationally effective over time[1,2,3].

7.1.4. Compliance, Legal Certainty, and Policy Credibility

Compliance effectiveness depends not only on the existence of sanctions law but on the degree of legal certainty with which that law can be operationalised. In sanctions governance, legal certainty should not be understood in an absolutist sense, as though every possible transaction pattern could be resolved in advance by fully determinate rules. In practice, sanctions regimes are revised frequently, contain multiple derogations and licensing pathways, and must respond to adaptive circumvention strategies. What matters, therefore, is not immutable certainty but usable certainty. Operators need to know where the legal boundary lies, which questions require escalation, which data points are decisive, and which public channels can be relied upon when ambiguity remains. This is why guidance, FAQs, consolidated lists, and best-practice materials are not peripheral additions to sanctions policy. They are part of the architecture through which a dynamic legal regime becomes operationally legible. Without that architecture, the regime remains formally valid but practically unstable. With it, compliance can be structured as a disciplined and defensible process rather than as improvisation under threat of penalty. In this sense, legal certainty is one of the enabling conditions of sanctions implementation rather than a post hoc legal luxury[4,5,6].

The Commission's own framing makes this point with unusual clarity. The Russia sanctions FAQs are described as being drafted by the Commission services to support national authorities, EU operators, and citizens in the interpretation and implementation of the relevant regulations, while also stating that only the Court of Justice of the European Union is competent to interpret EU law. That formulation captures the precise balance on which legal certainty in sanctions policy rests. The FAQs do not replace formal law, and they do not amount to judicially binding interpretation. Yet they still perform an essential operational function by narrowing the zone of uncertainty within which firms and authorities must act. In other words, they provide structured interpretative assistance without displacing the hierarchy of legal authority. This is exactly the type of "safe operating assumption" that sanctions governance requires. Operators do not need every ambiguity eliminated before they act, but they do need a public interpretative environment that makes prudent, proportionate, and reviewable action possible. Legal certainty in sanctions policy is therefore produced partly through formal law and partly through disciplined guidance that remains clearly subordinate to formal law[7,8].

This layered model of certainty is particularly necessary because the EU sanctions regime is implemented through a dispersed network of public and private actors. Banks, exporters, insurers, customs brokers, logistics providers, platforms, and advisers do not operate inside a single administrative chain of command. They function through separate internal systems, different risk appetites, and divergent sectoral exposures. In such an environment, legal certainty must be socially distributed rather than merely legislatively declared. The Commission's overview of sanctions resources explicitly links implementation quality to guidance, the sanctions helpdesk, the consolidated list, the EU sanctions map, and the whistleblower tool. That resource architecture exists because the law alone cannot create uniform operational understanding across heterogeneous sectors. The Helpdesk article

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[2] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[3] European Commission. (n.d.). *Overview of sanctions and related resources*.
[4] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[5] European Commission. (n.d.). *Overview of sanctions and related resources*.
[6] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[8] European Commission. (n.d.). *Frequently asked questions — Sanctions against Russia*.

of June 2025 makes the same point in practical terms by stressing that SMEs often need tailored legal support in order to understand what sanctions changes actually mean for commercial decisions. Legal certainty, therefore, is not only a matter of drafting. It is also a matter of access, usability, and institutional support. A sanctions regime that is formally coherent but operationally inaccessible will still generate weak or distorted compliance outcomes[1,2,3].

The relevance of legal certainty becomes even clearer when one considers the alternative. Where definitions are unclear, lists are difficult to use, derogation procedures are opaque, or interpretative updates arrive too slowly, firms tend to respond in one of two ways. Some under-comply by treating ambiguity as a reason not to intervene until violation is obvious. Others over-comply by blocking lawful activity, withdrawing services, or refusing legitimate transactions because the legal risk of a mistaken permissive decision appears too high. Both responses weaken policy quality. The first creates enforcement gaps and circumvention opportunities. The second produces unnecessary friction, market distortion, and private-law tension. This is why the European Parliament's 2023 study recommended that the EU ensure adequate guidance for economic operators and agree on a joint definition of competent national authority. It is also why the Council's 2024 Best Practices stress co-ordination and communication mechanisms across competent bodies and recommend notifying rejected authorisation requests to minimise the risk of distorting competition in the internal market. Legal certainty, then, is not only a compliance aid. It is a tool for preventing fragmentation and uneven burden allocation inside the coalition itself[4,5].

The EBA's 2024 guidelines reinforce this diagnosis by showing how uncertainty and inconsistency materialise at the level of internal systems. The guidelines specify the internal policies, procedures, and controls that financial institutions should put in place to ensure the effective implementation of Union and national restrictive measures, and they are addressed both to institutions and to competent authorities that assess those institutions. The EBA also records common supervisory concerns: outdated or incorrect lists, overreliance on external screening vendors, poor understanding of screening systems, inadequate calibration, inadequate frequency of screening, and limited fuzzy matching. These findings are highly significant for the present section because they demonstrate that legal certainty is not merely conceptual. It depends on whether the information and control environment are sufficiently clear, updated, and intelligible to support correct use. Where public expectations are vague or inconsistently translated, technical systems drift into unreliable operation. The EBA's insistence that screening alone is insufficient and must be complemented by stronger customer and beneficial-owner processes reveals the same logic. Certainty must extend beyond simple list access to the wider due-diligence framework in which decisions are made. In sanctions compliance, legal certainty is therefore partly infrastructural: it resides in the quality of the control environment as much as in the wording of the underlying legal act[6].

Definitions are a particularly sensitive part of this certainty architecture because they determine the scope of practical obligation. A sanctions regulation may prohibit dealings with listed persons, entities owned or controlled by them, or specified classes of goods, services, or financial instruments. But the operational challenge lies in what counts as "ownership", "control", "making available", "economic resources", "brokering", "indirect supply", or "benefit". If these concepts are too abstract at the level of practical use, then firms are left to improvise their own meaning under conditions of liability exposure. That is precisely why the Commission's FAQs remain so important. They do not create new law, but they give operators and national authorities a common interpretative vocabulary. A common vocabulary does

[1] European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] European Commission. (2025, June 11). *Sanctions implementation*.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[5] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

not eliminate all disputes, but it narrows the range of plausible divergence and thereby improves predictability. In turn, predictability reduces the odds that one Member State, one supervisor, or one sector will apply materially different operational assumptions from another. Legal certainty in sanctions policy is therefore inseparable from definitional discipline. Poor definitions externalise the burden of interpretation onto the market; better definitions and guidance internalise it within the governance structure of the regime[1,2,3].

Consolidated lists perform a similarly foundational role because certainty in sanctions compliance requires a reliable object of reference. The Commission's sanctions resources page states that the consolidated list of persons, groups, and organisations subject to EU financial sanctions is managed and updated whenever necessary and reflects the officially adopted texts published in the *Official Journal* of the European Union. The same page notes that EUR-Lex provides official and comprehensive access to EU legal documents and is updated daily. These two features matter greatly. First, they reduce the gap between formal adoption and operational visibility. Second, they create a public infrastructure of version control, which is indispensable in a regime characterised by repeated amendments and targeted additions. Operators need not only access to the law, but access to the current law in a format that can be used in screening, escalation, audit, and review. The same logic can be seen in partner jurisdictions. The UK sanctions list is maintained as a public, searchable resource and was updated as recently as 16 March 2026, while UK FAQs display a detailed amendment trail showing additions and revisions across 2025 and 2026. These examples support a broader conclusion: update discipline is a core ingredient of legal certainty because stale certainty is operationally equivalent to uncertainty[4,5,6].

The importance of update discipline becomes even more obvious when sanctions are used against a large adaptive target such as Russia. In that setting, operational relevance decays quickly if public guidance fails to keep pace with new derogations, changed price caps, altered reporting requirements, new evasion typologies, or amended sectoral restrictions. The Commission's Helpdesk article presents this problem from the perspective of SMEs that must decide whether altered sanctions environments permit a return to "business as usual" or require continued caution. The article explicitly links changing geopolitical conditions to the need for comprehensive FAQs and tailored support. This is a significant institutional acknowledgement. It means that certainty must be maintained actively rather than assumed once a regulation is published. In that sense, update discipline is not only a communications task. It is an element of enforcement design. A regime that updates its law but not its usable guidance invites divergence, delay, and preventable mistakes. A regime that updates both simultaneously stands a better chance of preserving coherent behaviour across the coalition[7,8].

The sanctions helpdesk illustrates how certainty can be operationally widened beyond large firms with sophisticated internal legal teams. The Commission describes the Helpdesk as an essential part of the Union's efforts to help European operators, particularly SMEs, comply with sanctions worldwide, and notes that it offers personalised help for sanctions due-diligence checks. This is highly relevant for policy credibility. A sanctions regime that can only be navigated by major multinationals is likely to create resentment, market exit, and asymmetric implementation burdens across the Union. By contrast, a regime that provides practical support to smaller operators is more likely to sustain lawful participation and reduce unnecessary de-risking. The Helpdesk therefore does more than answer questions. It broadens the social base of implementable compliance. It also reduces the chance that uncertainty will be solved privately through crude self-protective assumptions. In a coalition system, legal certainty

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Commission. (n.d.). *Frequently asked questions — Sanctions against Russia*.
[3] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[4] Foreign, Commonwealth & Development Office. (2020, updated 2026). *The UK Sanctions List*.
[5] Office of Financial Sanctions Implementation. (2024, updated 2026). *UK Financial Sanctions FAQs*.
[6] European Commission. (n.d.). *Overview of sanctions and related resources*.
[7] Ibid.
[8] European Commission. (2025, June 11). *Sanctions implementation*.

must be usable by the median operator, not only by elite compliance departments. That is one of the reasons why support architecture contributes directly to policy credibility[1,2].

The connection between legal certainty and market-level fairness is also central. The Council's Best Practices recommend that competent authorities notify rejected authorisation requests in order to minimise the risk of distorting competition in the internal market. That recommendation is easy to overlook, but it has major implications. It recognises that uneven interpretation or uneven information-sharing can shift commercial burdens arbitrarily across Member States and operators. One firm may receive timely clarity, another may remain trapped in uncertainty; one authority may license pragmatically, another may block excessively; one jurisdiction may absorb compliance cost while another benefits from looser practical assumptions. Such divergence is not only a technical issue. It affects the internal legitimacy of the sanctions' regime among participating states and firms. Where actors perceive the system as unpredictably unequal, long-term adherence becomes harder to sustain. Legal certainty is therefore connected not only to legality but to distributive credibility inside the coalition. A regime seen as coherent and even-handed is easier to maintain politically and economically than one experienced as patchy or arbitrary[3,4].

Comparative partner practice confirms the same general logic. The UK cross-government review of sanctions implementation and enforcement in May 2025 stated that strong enforcement is critical to impact, but also that this requires supporting the private sector to understand and comply with sanctions. The review further noted the importance of harnessing systemic efficiencies, improving information sharing, and minimising the administrative burden of compliance. OFSI's 2024–25 annual review then framed its own objective as ensuring that sanctions remain targeted and impactful while enabling businesses to operate with confidence and providing a growth-friendly regulatory environment. It reported prioritising clear communications, targeted guidance, responsive licensing, improved website accessibility, and practical updates through FAQs and alert services. A related explanatory memorandum for the 2024 amendments stated explicitly that codifying reporting obligations would provide "certainty and clarity" to persons that must comply while also strengthening the basis for enforcement. These partner-jurisdiction materials are analytically useful not because the EU should copy them wholesale, but because they show that mature sanctions systems increasingly treat clarity, transparency, and timely guidance as components of effectiveness rather than as concessions to business convenience. Legal certainty strengthens coercive policy when it makes disciplined compliance sustainable[5,6,7,8].

There is another reason why legal certainty matters for policy credibility: it affects whether firms view the regime as governable rather than merely punitive. OFSI's 2024–25 annual review states that businesses should be able to operate "with clarity and confidence", while its FAQ and guidance ecosystem is designed to give short-form technical information and updated operational instructions. This does not mean that the state promises commercial comfort. It means that a sanctions regime that aspires to long-term effectiveness must remain intelligible enough for legitimate actors to stay inside the law. The alternative is a policy environment in which operators either withdraw from exposed sectors entirely or continue only through highly defensive, low-trust behaviour. Both outcomes can weaken sanctions. Total withdrawal may be acceptable or even intended in some domains, but indiscriminate exit from lawful and strategically useful activity can hollow out coalition capacity. Legal certainty therefore

[1] European Commission. (2025, June 11). *Sanctions implementation*.
[2] European Commission. (n.d.). *Overview of sanctions and related resources*.
[3] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[4] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[5] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[6] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[7] HM Government. (2024). *The Sanctions (EU Exit) (Miscellaneous Amendments) (No. 2) Regulations 2024: Explanatory Memorandum*.
[8] Office of Financial Sanctions Implementation. (2026, February 9). *Financial sanctions enforcement: assessment and monetary penalties*.

supports not merely obedience, but calibrated obedience. That makes the regime more precise, less distortive, and more credible in the eyes of those expected to implement it. A sanctions policy that cannot be navigated predictably becomes harder to defend as a disciplined instrument of statecraft[1,2,3].

This same point applies within the EU financial sector, where certainty increasingly depends on supervisory convergence. The EBA guidelines are important not simply because they ask firms to have internal policies and controls, but because they provide a common reference point for competent authorities assessing those controls. In a multi-jurisdictional Union, supervisory convergence itself becomes part of legal certainty. If the same transaction logic is treated materially differently by different competent authorities, then firms are left navigating a formally common but practically fragmented regime. The EBA's attempt to establish common standards therefore contributes not only to compliance quality but to the credibility of the single market under sanctions conditions. It helps communicate that sanctions will be implemented through a common expectation set rather than through radically divergent national philosophies. This is especially important where institutions operate across borders and need assurance that compliance investments made in one part of the Union will not be rendered obsolete by incompatible supervisory practice elsewhere. Legal certainty, in this sense, is partly a convergence good. It is produced not only by texts and FAQs, but also by aligned supervisory treatment[4,5].

At the same time, legal certainty in sanctions policy should never be conflated with complete liability insulation. The Commission's FAQ page explicitly reminds users that only the Court of Justice can interpret EU law. The same caution appears in partner practice, where OFSI states that FAQs and guidance do not amount to legal advice and should be treated as supplementary to primary guidance. These caveats are not defects. They are an honest recognition of the constitutional and legal limits of administrative guidance. However, they do not deprive guidance of value. On the contrary, they clarify its correct function: to support implementation without usurping adjudication. In sanctions governance, that clarity about the status of guidance is itself part of legal certainty. Operators need to know both what guidance can do and what it cannot do. A regime in which soft-law materials silently claim more authority than they possess would create a different kind of uncertainty. Legal certainty is strengthened when guidance is robust, accessible, and timely, but also transparent about its own legal status[6,7].

The EBA consultation record further shows why operators demand clearer operational assumptions in high-friction areas. In the final report, respondents argued that interim freezing or rejection where information is insufficient should be set forth in legal EU requirements in order to prevent civil liability for financial institutions, especially given the high number of false positives that screening systems can generate. This is a revealing concern. It shows that, from the operator's perspective, uncertainty is not only about whether a person is listed. It is also about what the firm is expected or allowed to do while uncertainty is being resolved. In other words, legal certainty must extend to procedural posture, not merely substantive scope. Firms need to know when they may pause, when they must escalate, what follow-up due diligence is expected, and how temporary restraint interacts with potential private liability. Where these interim expectations are unclear, implementation becomes slower, more defensive, and less even. This does not necessarily mean that formal safe harbours are always required, but it does mean that the governance regime must provide clearer procedural signalling than a bare prohibition can

[1] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[2] Office of Financial Sanctions Implementation. (2024, updated 2026). *UK Financial Sanctions FAQs*.
[3] Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] European Commission. (n.d.). *Frequently asked questions — Sanctions against Russia*.
[7] Office of Financial Sanctions Implementation. (2024, updated 2026). *UK Financial Sanctions FAQs*.

supply. Legal certainty in sanctions compliance is therefore partly about decision sequencing, not just decision outcomes[1].

Table 7.1.4-1. Operational Components of Legal Certainty in Sanctions Compliance

Component of legal certainty	Public instrument or channel	Compliance function	Credibility effect if strong	Risk if weak
Normative accessibility	Official Journal, EUR-Lex, sanctions map	Ensures operators can identify current law and legal acts	Signals procedural seriousness and institutional competence	Stale or incomplete legal awareness
Interpretative support	Consolidated FAQs, topic-specific FAQs, best-practice notes	Narrows ambiguity around definitions, scope, and derogations	Improves predictability and reduces arbitrary divergence	Over-compliance, under-compliance, conflicting interpretations
Operable designation data	Consolidated lists, searchable sanctions databases	Allows screening, alert triage, escalation, and audit	Strengthens confidence that designations can be implemented in practice	Technical failure, list mismatch, delayed screening updates
Decision support for operators	Sanctions helpdesk, national competent authorities	Provides workable assumptions for concrete cases and due diligence	Keeps SMEs and mid-sized operators inside the compliance system	Market exit, defensive de-risking, uneven burden on smaller firms
Convergence mechanisms	EBA guidelines, Council best practices, supervisory dialogue	Harmonises expectations across Member States and sectors	Sustains internal market fairness and coalition cohesion	Fragmented enforcement and forum-shopping incentives
Update discipline	FAQ revisions, alert services, list updates, guidance refreshes	Maintains alignment with evolving packages, caps, and typologies	Preserves long-term trust in the sanctions regime's governability	Implementation lag, confusion, fatigue, and credibility erosion

Authorship: prepared by the author on the basis of official EU institutional materials
Sources:

- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Commission. (2025, June 11). *Sanctions implementation*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.

From here, the link to policy credibility becomes clearer. A sanctions regime is credible not only when it threatens penalties, but when participants believe it can be implemented consistently over time. Credibility has an external and an internal dimension. Externally, targets and facilitators must believe that the coalition can keep restrictions operationally intact even as they adapt. Internally, Member States, supervisors, and firms must believe that the regime remains governable and that compliance burdens are distributed in a reasonably intelligible way. Guidance ecosystems, list maintenance, update discipline, and co-ordinated best practices support both dimensions at once. They communicate that the coalition is not merely announcing restrictions but maintaining a live implementation architecture behind them. The opposite pattern—unclear rules, lagging updates, opaque licensing, inconsistent

[1] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

supervisory treatment—signals fragility. Over time, such fragility can erode confidence not only among firms but among coalition members themselves. The policy implication is that credibility is maintained through administrative reliability as much as through political resolve[1,2,3].

This is where the concept of coalition durability becomes analytically useful. Coalition durability is partly a political variable, but it is also a function of implementation manageability. Where firms can comply with relative clarity, where authorities have common reference points, and where updates are timely enough to prevent interpretative drift, sanctions are easier to sustain over multiple years. By contrast, if compliance becomes an opaque exercise in constant guesswork, the administrative and political cost of maintaining the regime rises. Smaller operators become fatigued first, then supervisors and NCAs face inconsistent reporting and recurrent clarifications, and eventually political actors confront demands for simplification, carve-outs, or selective relaxation. The UK cross-government review's emphasis on improving information sharing and minimising the administrative burden of compliance speaks directly to this risk. So does the Commission's decision to develop a Helpdesk aimed especially at SMEs. By inference, predictability supports durability because it reduces the cumulative friction of participation in the sanctions' regime. A coalition can more easily sustain a demanding policy when that policy is hard in substance but legible in operation[4,5,6,7].

For the EU sanctions track against Russia, this conclusion is especially important because the regime is already cumulative, multi-package, and functionally cross-sectoral. Such a regime cannot rely indefinitely on initial political momentum alone. It requires a maintenance layer that preserves interpretative coherence, keeps lists and FAQs current, aligns supervisory expectations, and offers operators clear channels for escalation and support. The institutional evidence now points strongly in that direction. The Commission's resource architecture, the Helpdesk, the consolidated FAQs, the Council's best-practice framework, and the EBA's common guidelines all indicate that the Union increasingly understands legal certainty as a strategic compliance asset. This should not be read as technocratic embellishment. It is part of how sanctions remain durable under conditions of repeated amendment and adaptive circumvention. The more extensive the sanctions regime becomes, the more important this certainty layer becomes. In prolonged confrontation, credibility does not rest on headline package numbers alone. It rests on whether the coalition can continue to implement those packages without disintegrating into fragmentation, fatigue, or arbitrary divergence[8,9,10,11].

The main conclusion is therefore straightforward. The effectiveness of sanctions compliance is inseparable from legal certainty, and legal certainty is inseparable from policy credibility. Guidance, FAQs, consolidated lists, definitions, decision-support channels, and disciplined updating do not merely make sanctions easier to understand. They make them more governable, more even in their application, and more sustainable over time. In the EU context, these instruments help bridge the gap between formal law and distributed implementation across Member States and private operators. In comparative partner practice, similar developments confirm that clarity, accessibility, and responsive licensing are increasingly treated as components of sanctions effectiveness rather than as external conveniences. A credible sanctions regime is one that can impose costs on the target while maintaining procedural reliability for those expected to implement it. In that sense, predictability is not the opposite

[1] European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[3] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] European Commission. (2025, June 11). *Sanctions implementation*.
[5] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[6] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[7] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[8] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[9] European Commission. (n.d.). *Overview of sanctions and related resources*.
[10] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[11] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

of pressure. It is one of the conditions under which pressure can be maintained. For the Russia-related sanctions architecture, this means that legal certainty should be treated not as a narrow juristic concern but as a core pillar of long-term compliance resilience and coalition durability[1,2,3].

7.2. Core Compliance Instruments

7.2.1. Screening, Listing Checks, and Beneficial-Ownership Verification

Screening, listing checks, and beneficial-ownership verification form the first operational layer through which sanctions become actionable in day-to-day market practice. A sanctions regime may be legally sophisticated, but it will remain weak in execution if firms cannot identify whether a counterparty, a related person, a vessel, an intermediary, or a transaction participant falls within the relevant prohibition. For that reason, these instruments should not be treated as mere technical preliminaries. They are the entry controls through which the compliance architecture begins to sort lawful from unlawful exposure. Their function is both preventive and classificatory. They prevent prohibited dealings before execution, and they classify the level of sanctions risk before the business process moves further downstream. In operational terms, this means that screening and ownership analysis are not auxiliary to compliance governance. They are the mechanisms by which compliance first acquires a concrete object. That object may be a person, an entity, a transaction, an ownership chain, a payment message, or a shipment participant, but without identifiable objects there can be no reliable sanctions control[4,5,6].

The starting point for this instrument layer is the sanctions list itself, but the list should be understood as an operational object rather than a static legal annex. The Commission's sanctions resources page states that DG FISMA manages the consolidated list of individuals, groups, and organisations subject to EU financial sanctions and updates it whenever necessary, while EUR-Lex provides official and comprehensive access to the underlying legal acts and is updated daily. This dual structure is significant. The *Official Journal* and EUR-Lex provide legal authority, while the consolidated list provides operational usability. The list is therefore part of the transmission mechanism that connects formal designation with actual screening practice. A similar logic is visible in the UK framework, where the FCDO publishes the UK Sanctions List and OFSI guidance explains both how the list is to be used and how quickly new listings or amendments are intended to be reflected. The existence of these maintained list infrastructures shows that governments themselves recognise that legal designations must be rendered searchable, updateable, and intelligible if they are to have real effect in private-sector systems[7,8].

Yet a list on its own does not solve the identification problem. The key operational distinction is between a name match and a target match. OFSI's guidance explains this with unusual clarity by stating that a match between the name of a person, entity, or ship and an entry on the list does not necessarily mean that the party in question is actually the sanctioned target. Operators must compare all available identifying information, including aliases, dates of birth, addresses, nationality, passport or ID details, and other markers, before concluding that the relevant person or entity is the listed one. OFAC's FAQ on

[1] European Commission. (2025, June 11). *Sanctions implementation*; European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[3] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] European Commission. (n.d.). *Overview of sanctions and related resources*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[7] European Commission. (n.d.). *Overview of sanctions and related resources*.
[8] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

valid matches follows the same logic in even more procedural terms. It directs users to distinguish whether the hit is truly against an OFAC list, to assess whether the type of subject matches, to review the degree of name correspondence, and then to compare all available identifying data before treating the result as actionable. This distinction matters greatly because poor screening governance can generate both false negatives and false positives. If matching criteria are too lax, sanctioned targets may slip through. If they are too crude, lawful business may be frozen or delayed without sufficient cause[1,2].

This is why high-quality screening depends on the attributes attached to a designation rather than on the name field alone. OFSI notes that the UK Sanctions List contains a range of information to aid identification, including primary names, aliases, dates of birth, places of birth, nationalities, passport details, national ID details, addresses, and official roles. The EBA guidelines reflect the same principle in a more systematised compliance format. They require PSPs and CASPs to define the types of data they will screen and to consider all data they hold about their customers, including information obtained through customer due diligence and travel-rule compliance. The guidelines also specify that screening should cover not only names but, where available, aliases, trade names, wallet addresses, and other relevant identifiers. In other words, sanctions screening is moving away from single-field comparison and toward multi-field identity resolution. This is a critical development because Russia-related evasion and circumvention often exploit the gaps between nominal identifiers, transliterations, beneficial owners, and operational intermediaries. A list-checking process that ignores those secondary fields remains formally present but functionally thin[3,4].

The question of transliteration and fuzzy matching is therefore not a mere software issue but a central element of screening design. The EBA guidelines require financial institutions to use screening systems capable of algorithm-based matching where the content screened is not identical but its spelling, pattern, or sound is a close match to the data contained in the screening dataset. They also require institutions to calibrate the degree of fuzzy matching in their systems and to document the rationale for those calibration choices. The EBA is explicit that calibration must be neither too sensitive nor insufficiently sensitive. If the system is too loose, it will miss designated persons, entities, or bodies. If it is too strict, it will generate an excessive volume of false positives and degrade operational quality. This is especially relevant in Russia-related sanctions because names may appear in different alphabets, under variant transliterations, or through partially incomplete data records. Effective screening therefore requires controlled approximation rather than exact literalism. A compliance system that insists only on exact identity of spelling will often fail in precisely the cases where sanctions evasion relies on transliterative and documentary variation[5].

The EBA's supervisory findings reinforce the practical importance of this point. In its final report, the Authority notes that competent authorities reported common deficiencies in screening systems, including outdated or incorrect lists, overreliance on vendor systems, poor understanding of those systems by firms, inadequate screening frequency, and only limited fuzzy matching. These observations are highly instructive because they show that the problem is not simply the absence of screening. It is the weakness of screening governance. A bank or crypto-asset service provider may have a screening engine in place and still be badly exposed if it does not understand what data are being screened, how often the lists are updated, how alerts are generated, and how calibration interacts with false-positive volumes. Screening effectiveness therefore depends on human governance as much as on technical tools. The use of external screening software does not relieve the institution of responsibility. It merely

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2015, January 30). *How do I determine if I have a valid OFAC match?*
[3] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] Ibid.

changes the way responsibility must be exercised. In this field, outsourcing weak judgement is not equivalent to building strong control[1].

A further reason why screening should be treated as a core compliance instrument is that it is not limited to onboarding. The EBA guidelines require PSPs and CASPs to screen their entire customer database regularly and to determine the frequency of screening on the basis of their restrictive-measures exposure assessment. They also require trigger events to be specified in internal policy. These include the entry into force of a new restrictive measure, a new designation, a change in existing sanctions, onboarding or the start of a business relationship, significant changes in customer due-diligence data, and reasonable grounds to suspect circumvention. This is a major governance point. Screening is not a once-and-for-all gate at the moment of customer acceptance. It is a continuing process of re-evaluation tied to legal change, data change, and suspicion-based escalation. In sanctions practice against Russia, this matters because ownership structures change, designations expand, and circumvention patterns evolve. A screening system that is not event-driven will become stale even if it once functioned adequately[2].

The same logic applies at transaction level, where screening must move beyond the customer record and into the payment or transfer itself. The EBA requires PSPs to screen transfers of funds before making funds available to the payee and CASPs to screen crypto-asset transfers before making the assets available to the beneficiary. It further requires that all parties to transfers be screened against applicable restrictive measures and that relevant data include not only the originator and beneficiary, but also the purpose of the transfer, free-text fields, details of intermediate institutions, BIC and SWIFT identifiers, and wallet addresses where those are present in official restrictive-measures lists. This reveals a more advanced screening logic than simple counterparty comparison. The transaction itself becomes a data-rich object of sanctions analysis. This is especially relevant in cases where the sanctioned risk does not lie in the direct payer or payee alone but in the intermediate route, the payment narrative, or the concealed beneficial involvement of a listed party. Transaction filtering, in this sense, is the moving edge of sanctions detection[3].

Listing checks therefore need to be understood as a workflow rather than a binary query. Once an alert is generated, a firm must decide whether the hit is a false positive, a plausible match requiring enhanced review, or a confirmed true positive requiring freeze, rejection, suspension, reporting, or referral. The EBA states that firms should have policies and procedures to investigate alerts without delay, document any decision taken in respect of alerts, and apply different levels of review depending on the restrictive-measures exposure assessment, including at least a two-person review in higher-exposure situations. It also requires that alerts be analysed by staff with the needed expertise and sufficient training. This is critical because alert resolution is the point at which screening becomes legal action. A poorly governed alert workflow can undermine even a technically strong screening engine. It may dismiss serious alerts too quickly, allow commercial pressure to override control, or keep matters in limbo without lawful basis. Properly designed alert management therefore functions as the bridge between automated detection and defensible decision-making[4].

The EBA also makes clear that alert analysis must be supported by further due diligence where ambiguity remains. When in doubt about the trueness of a match, institutions are expected to use additional information that they may hold or obtain, including identification data not used at the initial screening stage, residence or registered address, nationalities, and representative, management, and organisational structure. This is analytically important because it demonstrates that screening is not self-sufficient. It is a trigger for structured inquiry. A firm that treats the initial alert as the whole exercise will either over-block or under-detect. A firm that uses the alert as the beginning of a targeted verification process is much more likely to identify real sanctions exposure accurately. In practice, this means that

[1] Ibid.
[2] Ibid.
[3] Ibid.
[4] Ibid.

sanctions-list screening and due diligence are not separate instruments. They are linked phases of a common control sequence. Screening narrows the field; due diligence resolves the ambiguity; escalation governs the decision[1].

At the same time, screening systems must manage the opposite problem of repetitive false positives. The EBA permits institutions to place repeatedly misidentified non-sanctioned persons or entities on a specific internal whitelist in order to avoid repeated false alerts, but it requires the reasons for this decision to be documented and the list to be reviewed immediately after new or amended restrictive measures enter into force or customer information changes. This is an important example of control refinement. It acknowledges that high false-positive volumes can degrade system usability, but it does not allow institutions to solve that problem informally or permanently. Whitelisting must itself be governed, reasoned, and updated. Otherwise, it risks becoming a covert blind spot through which newly relevant exposure is no longer detected. This example again shows that effective sanctions screening is not a purely technological question. It is an exercise in calibrated governance under changing legal conditions[2].

The role of outsourcing and third-party vendors further underlines this point. The EBA states that the ultimate responsibility for compliance with restrictive measures remains with the institution even when specific functions are outsourced, and that institutions must monitor and oversee the quality of the service provided. This is a significant principle because many firms rely on external vendors for list ingestion, screening software, name-matching tools, and alert-generation architecture. That reliance can be operationally useful, but it can also create a false sense of control. If the firm does not understand how the tool works, how it is calibrated, what data it excludes, how quickly it updates, or how false positives are managed, the presence of a vendor can become a source of complacency rather than resilience. Vendor dependence is especially dangerous in a sanctions' environment characterised by rapid legal amendment and increasingly complex circumvention patterns. A screening tool may be outsourced, but the accountability for screening cannot be outsourced[3].

Beneficial-ownership verification enters at precisely the point where list-based screening reaches its practical limit. Sanctions rarely operate only through directly listed names. The relevant exposure may lie in a non-listed entity that is owned, controlled, or used for the benefit of a listed person. The Commission's asset-freeze FAQ states that if a listed person is deemed to own or control a non-listed entity, it can be presumed that control extends to the assets of that entity and that any funds or economic resources made available to that entity would reach or benefit the listed person. The FAQ also stresses that operators must exercise the highest caution when dealing with associated persons or entities and that if non-listed entities are deemed to be owned or controlled by listed persons, their assets must be frozen and no funds or economic resources can be made available to them. This is a decisive compliance principle. It means that sanctions-list screening alone is structurally incomplete. A party can escape the list and still remain sanction-relevant through ownership or control. Beneficial-ownership verification is therefore not a supplementary AML-like exercise bolted onto sanctions after the fact. It is one of the principal ways in which sanctions penetrate beyond formal legal personhood[4].

The same Commission FAQ is equally clear that the EU does not maintain an official ready-made list of ownership percentages for all firms linked to sanctioned persons. It states explicitly that this is a task for EU credit institutions' compliance and due-diligence departments and points to EU Best Practices for guidance on ownership and control. This is analytically significant because it allocates responsibility for the ownership screen to the operator rather than to the listing authority. In other words, the public side defines the legal principle, but the private side must investigate and apply it in real cases. That allocation

[1] Ibid.
[2] Ibid.
[3] Ibid.
[4] European Commission. (2024, September 5). *Asset freeze and prohibition to provide funds or economic resources: Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it.*

is central to the broader sanctions' compliance architecture. It confirms that beneficial-ownership verification is an operational obligation resting heavily on firms, especially financial institutions and other high-exposure intermediaries. It also means that sanctions compliance cannot be reduced to mechanical database consultation. It requires structured inquiry into who really owns, controls, or benefits from the counterparty with whom the firm is dealing[1,2].

Aggregate ownership rules make this verification task more complex and more important. The Commission's 2024 asset-freeze FAQ states that if two or more listed persons each hold minority stakes in a non-listed entity but their aggregate ownership amounts to 50% or more, that entity should be considered as owned by listed persons. OFAC's 50 Per Cent Rule follows a related aggregate-ownership logic, stating that entities owned 50% or more in the aggregate by one or more blocked persons are themselves considered blocked, including through direct and indirect ownership chains. These comparative materials matter because they show that sanctions systems increasingly seek to prevent fragmentation tactics whereby exposure is broken into multiple smaller stakes to avoid obvious control thresholds. Ownership analysis must therefore be cumulative, not atomistic. It must consider how apparently separate holdings combine within the same entity or group structure. A compliance process that screens only for single-majority ownership can easily miss the relevant sanctions nexus[3,4].

At the same time, the comparison between EU, UK, and U.S. approaches is instructive because it shows that ownership and control are not conceptually identical across regimes. UK guidance provides that an entity may be caught where a designated person holds more than 50 per cent of the shares or voting rights, has the right to appoint or remove a majority of the board, or where it is reasonable to expect that the person can ensure the entity's affairs are conducted in accordance with that person's wishes. OFAC's 50 Per Cent Rule, by contrast, explicitly speaks to ownership and not to control as such, while still warning that transactions involving non-blocked entities controlled by blocked persons can raise serious sanctions risk and may involve blocked persons acting on behalf of those entities. The EU approach, as reflected in the Commission FAQ, links ownership and control through the presumption that making funds available to an owned or controlled entity reaches or benefits the listed person. For compliance teams, the lesson is simple but demanding: ownership tests cannot be lifted mechanically from one jurisdiction to another. Screening and BO verification must reflect the logic of the regime actually being implemented[5,6,7].

The data problem behind beneficial-ownership verification is therefore substantial. FATF's 2023 and 2024 guidance emphasises that countries should ensure competent authorities have access to adequate, accurate, and up-to-date beneficial-ownership information and highlights the importance of mechanisms that verify that information. FATF explicitly links stronger beneficial-ownership transparency to the ability to identify corrupt actors, money launderers, tax evaders, and sanctions evaders who hide behind shell companies, complex corporate structures, and legal arrangements such as trusts. This matters directly for sanctions compliance. If beneficial-ownership information is stale, inaccurate, or inaccessible, then the ownership-and-control test becomes highly difficult to apply in real time. Firms may not know whether the immediate counterparty is the economically relevant actor or merely the outer shell of a listed person's network. The quality of BO verification therefore depends not only on firm-level diligence but on the wider information environment in which that diligence is

[1] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[2] European Commission. (2024, September 5). *Asset freeze and prohibition to provide funds or economic resources: Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[3] Ibid.
[4] U.S. Department of the Treasury, Office of Foreign Assets Control. (n.d.). *Entities Owned by Blocked Persons (50% Rule)*.
[5] Ibid.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[7] European Commission. (2024, September 5). *Asset freeze and prohibition to provide funds or economic resources: Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

performed. Public registries, cross-border co-operation, and verification standards all affect the strength of private sanctions screening[1,2].

The EBA guidelines incorporate this same reality at supervisory level by requiring institutions to assess whether the data they hold are sufficiently accurate, up to date, and detailed to determine if a party to a transfer, its beneficial owner, or any authorised representative is subject to restrictive measures. The guidelines also state that when screening legal persons, institutions should, to the extent that this information is available, screen beneficial owners through ownership interest, beneficial owners through control, and any person authorised to act on behalf of the customer. This is an important evolution in EU compliance expectations. It shifts sanctions screening away from a narrow list-versus-name model and toward a more relational model of exposure. The question becomes not only who the customer is, but who stands behind the customer, who controls the customer, and who is acting for the customer. In the Russia context, this shift is indispensable because evasion often depends precisely on inserting layers between the listed person and the visible transaction. Beneficial-ownership verification is therefore one of the main ways in which screening becomes anti-circumvention-capable[3,4].

The Commission's 2025 guidance on common high-priority items takes the same principle into the trade sphere. That document notes that Article 12gb also applies to persons who own or control legal persons established outside the Union that sell or export specified common high-priority items to third countries. This is important because it extends the screening logic beyond direct export relationships and into the ownership chains of third-country operators used in re-export structures. In practical terms, it means that beneficial-ownership verification is not only a financial-sanctions issue. It is also a trade-control issue. Screening the counterparty without examining who owns or controls it may be insufficient where the risk lies in the indirect use of intermediary distributors or procurement vehicles. This is precisely the type of pattern that has characterised Russia-related sanctions circumvention. BO verification therefore functions as a bridge between targeted financial restrictions and anti-circumvention trade controls[5,6].

Transaction filtering, listing checks, and beneficial-ownership verification also converge at the point of action. The EBA guidelines require PSPs to suspend without delay operations triggering an alert of a possible match with a designated person or entity, or one owned, held, or controlled by a designated person or entity, or whose beneficial owner is a designated person. If internal analysis confirms the match, the institution should immediately freeze the corresponding funds and stop the execution of the transfer. This is the clearest possible example of how the instrument layer operates as a chain. Screening produces the alert. Listing checks and due diligence determine whether the alert is a true positive. Ownership and beneficial-ownership analysis determine whether the legal nexus extends beyond the directly listed party. The escalation workflow then transforms that determination into freeze, stop, report, or further instruction from the competent authority. These instruments therefore should never be analysed in isolation. Their force lies in their ordered combination (European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*).

[1] Financial Action Task Force. (2023, March 10). *Guidance on Beneficial Ownership of Legal Persons*.
[2] Financial Action Task Force. (2024, March 11). *Guidance on Beneficial Ownership and Transparency of Legal Arrangements*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] Ibid.
[6] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.

Table 7.2.1-1. Core Identification Instruments in Sanctions Compliance

Instrument	Primary object screened or verified	Main operational function	Typical failure risk	Required governance response
Sanctions list check	Listed persons, entities, ships, wallet addresses, other listed identifiers	Establish whether a direct designation exists	Outdated lists, missed amendments, poor data ingestion	Immediate list updates, official-source alignment, version control
Name and identifier screening	Names, aliases, transliterations, dates of birth, IDs, addresses, BIC/SWIFT data	Distinguish name matches from target matches	False positives, false negatives, weak transliteration handling	Multi-field matching, calibration, fuzzy matching, trained review
Customer screening	Existing and prospective counterparties	Detect exposure at onboarding and during the relationship lifecycle	One-off screening only, no trigger events, stale customer data	Regular rescreening, event-driven updates, trigger-based review
Transaction screening/filtering	Payer, payee, intermediaries, free-text fields, transfer purpose, wallet data	Detect prohibited involvement before execution	Narrow focus on direct parties only, ignored free-text or intermediate identifiers	Pre-execution screening, full-party coverage, route and narrative review
Ownership/control analysis	Shareholdings, voting rights, board rights, de facto influence	Extend sanctions reach to non-listed entities owned or controlled by listed persons	Surface-only review, fragmented minority stakes ignored	Aggregated ownership analysis, control assessment, group-structure review
Beneficial-ownership verification	UBOs, trustees, controllers, authorised representatives	Identify hidden or indirect sanctions nexus	Inaccurate BO data, opaque structures, registry gaps	Enhanced due diligence, documentary verification, repeated review
Alert triage and escalation	Potential hits from screening systems	Convert technical alerts into lawful operational decisions	Commercial override, poor documentation, no escalation discipline	Defined alert workflow, trained staff, record-keeping, four-eyes review

Authorship: prepared by the author on the basis of official EU institutional materials and U.S. documents
Sources:

- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Commission. (2024, September 5). *Asset freeze and prohibition to provide funds or economic resources: Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- Financial Action Task Force. (2023, March 10). *Guidance on beneficial ownership of legal persons*.
- Financial Action Task Force. (2024, March 11). *Guidance on beneficial ownership and transparency of legal arrangements*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2015, January 30). *How do I determine if I have a valid OFAC match?*
- U.S. Department of the Treasury, Office of Foreign Assets Control. (n.d.). *Entities Owned by Blocked Persons (50% Rule)*.

The broader strategic implication is that identification instruments are also deterrence instruments. When firms know that they must screen not only direct names but also aliases, beneficial owners, intermediaries, wallet addresses, and transaction narratives, the compliance perimeter becomes harder to game. This raises the cost of circumvention because evasive structures must now conceal more relationships, not merely avoid a listed name. It also increases the chance that hidden nexus will surface through inconsistencies between customer data, transfer details, ownership information, and operational behaviour. In the Russia sanctions context, this matters greatly because many adaptive strategies rely on the assumption that control and benefit can be concealed behind formally clean counterparties. Screening and BO verification undermine that assumption when they are properly joined to due diligence and escalation. The value of these instruments therefore lies not only in what they directly catch, but also in what they make more difficult to attempt[1,2,3].

The main analytical conclusion is therefore clear. Screening, listing checks, and beneficial-ownership verification should be treated as core compliance instruments because they operationalise the threshold question on which all later controls depend: who is really involved in the transaction, relationship, or structure under review. They do this through list usability, multi-field matching, calibration, customer and transaction screening, ownership aggregation, beneficial-owner identification, and structured alert management. Each component addresses a different form of concealment or ambiguity. Together they turn sanctions from a set of abstract prohibitions into a practical identification regime. In the EU case, recent guidance and supervisory developments show a clear move toward more systematic, data-rich, and governance-intensive screening models. That trend is not accidental. It reflects the reality that sanctions against Russia now operate in an environment where direct designation alone is insufficient and hidden nexus has become a central enforcement problem. A durable sanctions architecture therefore requires durable identification instruments at its front end[4,5,6].

7.2.2. Trade-Control Compliance: Export, Re-Export, and End-Use Due Diligence

Trade-control compliance is the part of the sanctions architecture where legal prohibition must be translated into granular decisions about goods, routes, counterparties, documents, and intended uses. Unlike simple asset-freeze implementation, export and re-export compliance must intervene before physical movement occurs and often before the full downstream chain is visible. This makes trade compliance structurally predictive rather than merely reactive. Exporters, distributors, freight forwarders, customs brokers, logistics providers, and in many cases financial intermediaries must determine whether the transaction is lawful not only in its declared form but in its probable operational trajectory. The European Commission's 2023 guidance expressly states that it currently focuses on export-related sanctions and that EU operators are expected to have due-diligence measures for all relevant activities within the scope of EU sanctions. The same guidance explains that the Commission's lists of common high priority items and economically critical goods are meant to support due diligence and effective compliance by exporters, as well as anti-circumvention action by customs and enforcement agencies of partner countries. This means that trade-control compliance is not confined to classification of goods under annexes. It is a broader governance process aimed at preventing restricted items from reaching Russia directly or indirectly through intermediary channels. In the Russia context,

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] Financial Action Task Force. (2023, March 10). *Guidance on Beneficial Ownership of Legal Persons*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] Ibid.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] European Commission. (2024, September 5). *Asset freeze and prohibition to provide funds or economic resources: Frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

the decisive question is therefore not only whether export is formally prohibited, but whether the operator can demonstrate that it has taken proportionate steps to prevent diversion, re-export, or disguised military end use[1,2].

The operational logic begins with the recognition that export control and sanctions compliance are now functionally intertwined. The Commission's Trade and Economic Security page explains that Regulation (EU) 2021/821 governs the EU export control regime and includes common provisions for end-use controls on non-listed items, controls on brokering and technical assistance, record-keeping obligations, and a network of competent authorities supporting consistent implementation and enforcement throughout the EU. The same page further states that, in certain cases, additional EU restrictive measures apply to dual-use exports and directly points operators to Russia-related sanctions guidance and the list of high-priority battlefield items. This official presentation is important because it shows that the Union itself does not treat sanctions-related export restrictions as wholly separate from the wider export-control toolbox. Instead, the sanctions layer is superimposed on, and interacts with, the pre-existing dual-use control architecture. For operators, this means that compliance cannot be reduced to checking whether a good appears in Annex VII or Annex XL alone. It also requires understanding end-use controls, brokering restrictions, technical-assistance restrictions, record-retention obligations, and the availability or non-availability of authorisations. Trade-control compliance is therefore built as a hybrid discipline combining sanctions law, export-control method, and anti-circumvention vigilance. That institutional hybridisation is one of the reasons why the trade-control layer has become so central in the sanctions' regime against Russia[3,4].

A core function of trade-control compliance is therefore classification plus contextualisation. Classification asks what the item is in legal and tariff terms and whether it is covered by export prohibitions, dual-use controls, common high priority lists, or other sensitive categories. Contextualisation asks who is buying it, who will use it, how it will move, why it is being ordered, and whether the pattern of trade makes commercial and logistical sense. The Commission's 2023 guidance is explicit that operators should map out the types of products, transactions, and economic activities within their range of services that are at risk of being involved in Russia sanctions circumvention techniques. It then recommends a strategic risk assessment moving from identification of threats and vulnerabilities, to risk analysis, to the design of mitigating measures, and finally to implementation of those measures. This is a notable shift away from a purely item-centric mindset. Goods still matter, but the broader risk environment in which those goods are traded matters just as much. A compliant exporter is not one that simply reads a control list. It is one that knows how the product sits within the relevant circumvention ecosystem and adapts controls accordingly. In trade-control compliance, the legal identity of the item and the operational profile of the transaction must therefore be assessed together[5].

This is why end-user and end-use due diligence now occupy such a central place in the compliance chain. The Commission's 2025 enhanced due-diligence FAQ for operators manufacturing or trading with common high priority items states that there is no single model for conducting due diligence and that operators should adapt their efforts to the risks identified using an effective yet proportionate approach. It then lists specific stakeholder-level questions, including whether all stakeholders involved in the transaction are known, whether they are targeted by EU sanctions directly or indirectly through ownership or control, who the end user is, whether the end use can be confirmed, and whether an end-user certificate can be provided. This is a very clear operational benchmark. It means that compliance

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[3] European Commission, Directorate-General for Trade and Economic Security. (n.d.). *Exporting dual-use items*.
[4] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[5] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.

is not satisfied by identifying the immediate purchaser alone. The operator must examine the actual user, the intended application, and the risk that the declared end use disguises diversion or military-industrial deployment. In the Russia setting, where intermediary jurisdictions and front companies are frequently used, this approach is indispensable. End-use and end-user due diligence are therefore best understood as the mechanism through which trade-control compliance reaches beyond the first contractual counterparty and into the probable downstream reality of the goods[1].

The practical content of end-use diligence also shows why trade-control compliance is deeply evidential in character. Operators are expected to ask not only who the end user is, but whether the stated use is plausible and documentable. The Commission's 2025 FAQ asks whether the end use can be confirmed and whether an end-user certificate can be provided. The G7's 2024 updated industry guidance takes the same logic further by recommending that, when red flags are encountered, traders inquire further regarding the end use, end user, and ultimate country of destination, request more information on customer history and business practices, and obtain written certification that items will not be transferred to parties in Russia or Belarus or to sanctioned parties in third countries. These are not symbolic additions. They are documentary instruments that make the customer commit to a specific downstream narrative and thereby create both evidential traceability and contractual leverage. In trade-control governance, documentation is not merely archival. It is part of how the operator tests whether the counterparty's story can withstand scrutiny. A transaction whose documentation resists completion, consistency, or independent verification is not only poorly documented; it is compliance-relevant by that very fact[2,3].

The EU's "no re-export to Russia" clause under Article 12g is one of the clearest examples of trade-control compliance being pushed from advisory practice into legal obligation. The Commission's FAQ on the clause states that Article 12g aims to combat the circumvention of EU export bans, especially where goods exported to third countries are re-exported to Russia. It explains that what had already existed as a good-practice contractual device is turned by Article 12g into a legal requirement for certain sensitive goods, thereby improving legal certainty and creating a deterrent effect on non-EU operators that might otherwise redirect controlled EU goods to Russia. The FAQ also states that exporters should not sell to non-EU operators unwilling to incorporate the clause and that paragraph 4 of Article 12g requires exporters to inform their national competent authorities as soon as they become aware of a breach or circumvention of the clause. This is a major development in the architecture of export compliance. It moves anti-diversion control from internal risk-management discretion into express contractual and reporting obligation. The EU is not only telling firms to be careful. It is requiring them to embed downstream non-re-export commitments into the legal structure of the transaction itself. This significantly strengthens the *ex ante* compliance perimeter[4].

Article 12gb extends that logic even further by imposing an enhanced due-diligence obligation for operators trading in common high priority items and goods listed in Annex XLVIII. The Commission's 2025 FAQ explains that the purpose of this measure is to strengthen the due diligence of EU operators in response to the re-exportation of CHP items and certain Annex XLVIII goods to Russia, and that it also gives national competent authorities a tool to curb circumvention through third countries. It further states that the obligation applies not only to EU persons that sell, supply, transfer, or export such items, but also to EU persons that own or control legal persons established outside the Union that engage in such sales or exports, unless excluded by the provision. This matters because it broadens the compliance horizon. It recognises that diversion risk can arise not only through a direct export from the EU but also through controlled affiliates and distribution structures outside the Union. In practical terms, this makes re-export compliance a network-governance problem rather than a single-transaction

[1] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*
[2] Ibid.
[3] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[4] European Commission. (2024, February 22; updated December 18, 2024). *Frequently asked questions concerning the "No re-export to Russia" clause and sanctions adopted following Russia's military aggression against Ukraine*.

problem. Operators are expected to consider not just the immediate shipment, but also the behaviour of foreign legal persons within their sphere of ownership or control[1,2].

High-risk routing analysis is another indispensable part of trade-control compliance because diversion often occurs through geography rather than through overt falsification alone. Both the 2023 Commission guidance and the 2025 Article 12gb FAQ ask operators to examine the country of transit and destination, whether that country neighbours Russia or Belarus, whether it offers easy transport access, whether it is otherwise known to re-export goods to those jurisdictions, and whether exports to those locations should be subject to enhanced vigilance or end-use controls. The 2025 FAQ adds that operators should consider transit through countries or territories known as circumvention hubs and, depending on their role, check the type of means of transport used, the routing, and the use of subcontractors. These questions are operationally significant because they reframe route analysis as a compliance obligation rather than a logistics detail. In this model, route choice carries evidential value. An unusual routing pattern, a newly favoured corridor, or a transit chain that makes little commercial sense can itself be a sanctions red flag. Trade-control compliance therefore demands that operators know not only what they are shipping but how and through whom it is moving[3,4].

Documentation scrutiny follows directly from this route-based logic. The Commission's 2025 FAQ asks whether there are unusual or abnormal elements in the documentation that do not match, e.g., between financial documents and the contract. The 2024 G7 guidance is even more specific, identifying false, inaccurate, or missing documentation as a key red-flag category, including false declarations of export authorisation, misclassification of goods, undervaluation of goods, use of one HS code at export and a different HS code on arrival in a third country, and civil end-use claims for items destined for companies known or associated with military entities. This is a powerful convergence between EU and G7 practice. It shows that document analysis is not a paperwork burden attached to the transaction after the main compliance work is done. It is itself a central detection instrument. When trade-control evasion becomes more sophisticated, document inconsistency often becomes the first visible symptom. Compliance teams therefore need the capacity to read documents relationally, comparing invoice value, shipping data, contract terms, customs codes, end-use declarations, and payment information for coherence rather than merely completeness[5,6].

Red-flag typologies are therefore not optional enhancements to compliance programmes. They are the method by which operators connect abstract legal restrictions to recurring patterns of evasion. The Commission's 2023 guidance states that various indicators should alert EU operators when they enter a commercial relationship with a new trading partner, and that, if operators find evidence of such indicators, they should launch deeper screening. The G7 guidance similarly lists indicators such as new importers or exporters of common high priority items, sudden changes in business activity after 24 February 2022, misclassification of goods, unusual routing through multiple third countries, freight forwarders listed as end users, circuitous routing of goods or financial flows, unexplained last-minute changes in parties, and customers unwilling to provide end-use assurances. The crucial analytical point is that these indicators are probabilistic, not determinative. No single red flag automatically proves illicit conduct, but the presence of unresolved red flags changes the compliance posture of the transaction. This is why both the Commission and the G7 stress risk-based deeper screening rather than automatic

[1] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[2] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[3] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[4] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[5] Ibid.
[6] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.

mechanistic blocking in every case. Typology-based compliance is thus a structured way of handling suspicion before it matures into an enforcement case[1,2].

The commercial-rationale test is one of the most useful tools inside this typology-based method. The Commission's 2023 guidance asks directly what the business rationale is for the transaction and whether the shipment seems in line with expectations regarding the prospective customer, or instead appears unjustified from a business perspective. This deceptively simple question is analytically powerful because many diversion schemes rely on preserving formal legality while eroding economic plausibility. A small or newly incorporated distributor may suddenly order sensitive technology in volumes inconsistent with its business model. A destination country with no apparent domestic market for a controlled item may become a fast-growing purchaser. A route may become longer, more expensive, and less efficient without any credible commercial explanation. These are not incidental features. They are precisely the type of deviations that distinguish normal trade from trade shaped by evasion pressure. The business-rationale test therefore serves as a bridge between sector knowledge and compliance law. It asks firms to use their understanding of markets and clients as a detection resource rather than pretending that sanctions risk can be evaluated purely through formal documentation[3,4].

Common high priority items have become the clearest substantive focus of this trade-control layer. The Commission's February 2024 CHPI page explains that the list is intended to support industry vigilance, while the BIS CHPL page states that the list is divided into four tiers, with Tier 1 items of highest concern because of their critical role in advanced Russian precision-guided weapon systems, Russia's lack of domestic production, and limited global manufacturers. The G7 guidance adds that the CHPL is intended to aid industry in conducting necessary due diligence and that, as of publication, it included 50 tariff lines identified by six-digit HS codes. This matters because it gives firms a shared multinational priority map. Rather than treating every controlled item as carrying identical diversion value, the CHPL/CHPI architecture focuses compliance attention on the goods most relevant to Russian warfighting capability. It thereby improves prioritisation, resource allocation, and cross-border coherence among coalition actors. In trade-control compliance, prioritisation is not a reduction in seriousness. It is a way of intensifying control where sanctions leverage is likely to be greatest[5,6,7].

That prioritisation logic also explains why the EU and partner jurisdictions increasingly use layered obligations rather than a single blanket control. The Commission's 2025 Article 12gb FAQ states that, for CHPI and Annex XLVIII goods, several obligations may apply simultaneously: direct or indirect export bans to Russia, contractual non-re-export obligations, intellectual-property-related prohibitions, and enhanced due diligence. The same FAQ makes clear that Article 12gb does not replace Article 12g. The two provisions work together. One imposes a contractual anti-diversion device for sensitive goods more broadly; the other imposes heightened due diligence for the most sensitive subsets. This layered approach is strategically rational. Different instruments address different stages of the diversion chain. Export bans block direct supply, contractual clauses raise downstream legal friction, and enhanced due diligence raises the evidential standard before the transaction is cleared. Trade-control compliance

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[3] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[4] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[5] European Commission. (2024, February 22). *List of common high priority items*.
[6] Bureau of Industry and Security. (n.d.). *Common High Priority Items List (CHPL)*.
[7] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.

therefore operates most effectively when these instruments are combined rather than treated as substitutes[1,2].

The 2022 Commission notice to economic operators, importers, and exporters remains important because it set out the anti-circumvention baseline on which these later instruments were built. The notice advised EU operators to take adequate due-diligence measures to prevent circumvention both via exports to third countries from which goods could be diverted toward Russia and Belarus, and through imports from third countries from which the goods concerned could be diverted easily to the EU. It specifically drew attention to exports to countries of the Eurasian Economic Union because of free circulation within that area. It also advised operators to use contractual provisions making respect for sanctions an essential element of the contract and to ensure that third-country importers do not export the goods onward to Russia or Belarus or resell to parties unwilling to take the same commitment. Finally, it warned that EU customs authorities could carry out stricter controls and request conclusive evidence that goods were not being exported to or imported from Russia and Belarus via third countries. This notice is important because it shows that trade-control compliance in the Russia context has always been as much about routing and re-export risk as about the direct Russia nexus. What later became codified in Article 12g and strengthened in Article 12gb was already present in embryo in this early anti-circumvention logic[3].

The U.S. and G7 materials reinforce this same point through a more openly typological vocabulary. BIS's 2023 guidance to prevent evasion of prioritised HS codes to Russia explains that it provides details on evasion typologies, highlights nine high-priority HS codes to inform customer due diligence, and identifies additional transactional and behavioural red flags to assist exporters and re-exporters in identifying suspicious transactions relating to possible export-control evasion. The document emphasises evaluation of end user and end use, asks whether the customer's line of business is consistent with the ordered items, and notes that physical location and public-facing website may themselves raise red flags. It then adds that anomalous increases in order volume or value, especially involving known transshipment points, should trigger additional information requests on end use and end user. The operational lesson is broader than the U.S. regime alone. It shows that advanced export-control compliance increasingly depends on risk-signalling patterns rather than only on static licensing rules. Typologies help operators identify what a plausible diversion attempt looks like before the goods move[4].

BIS's 2023 customer-certification best practice adds another important dimension: compliance should sometimes require the customer to help carry the control downstream. The BIS document recommends collecting the full name and address of the non-GECC customer, line of business, website, transaction role, and, for new customers, a copy of the business licence. It further recommends asking what the customer intends to do with the item, whether it will be consumed, transformed, stocked, or resold, and, if the customer is not the end user, identifying the known end user. The suggested attestation also requires the customer to acknowledge that any re-export or transfer in-country to Russia or Belarus would require a licence, to screen subsequent parties against the U.S. Consolidated Screening List, and not to provide the item for end use by military, intelligence, national-police, missile, UAV, nuclear, chemical, or biological weapons users or uses. Even though this is U.S. best practice, the governance logic is directly relevant to EU operators as well. Trade-control compliance becomes stronger when downstream actors are made to commit explicitly to non-diversion obligations and when those commitments are documented, reviewable, and flow-down capable[5].

[1] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[2] European Commission. (2024, February 22; updated December 18, 2024). *Frequently asked questions concerning the "No re-export to Russia" clause and sanctions adopted following Russia's military aggression against Ukraine*.
[3] European Commission. (2022, April 1). *Notice to economic operators, importers and exporters*
[4] Bureau of Industry and Security. (2023, May 24). *Guidance to Prevent Evasion of Prioritized Harmonized System Codes to Russia*.
[5] Bureau of Industry and Security. (2023, September 14). *Best Practice: Certification to Prevent Diversion to Russia of Highest Priority Items*.

A related point is that trade-control compliance increasingly reaches beyond exporters narrowly defined. The G7 updated guidance states that all parties in the supply chain, including exporters, re-exporters, manufacturers, distributors, resellers, financial institutions, logistics companies, transport providers, freight forwarders, warehouse operators, and customs brokers, should be aware of the diversion risks posed by Russia's procurement efforts and adopt appropriate measures to mitigate them. This is highly significant. It means that end-use and routing diligence are not solely the exporter's burden. Different actors see different slices of the transaction, and the compliance architecture expects each to use the visibility it has. A freight forwarder may see routing anomalies first. A warehouse operator may observe unusual consolidations of small shipments into a larger onward shipment. A bank may notice a last-minute change in payment routing or a third-country payer with no commercial role. Trade-control compliance is therefore a distributed control system. Export law provides the legal frame, but operational prevention depends on the different supply-chain actors using their vantage point to interrogate the transaction[1,2].

This distribution of responsibility is one reason why catch-all logic remains so important conceptually even when the transaction does not involve a clearly listed good. The Commission's Trade and Economic Security page explains that Regulation (EU) 2021/821 contains common provisions for end-use controls on non-listed items, for example in connection with WMD programmes or human-rights violations. The significance of this for the Russia sanctions environment is indirect but real. It confirms that EU trade-control governance is not limited to fixed annexes. It also includes an end-use logic that allows risk to be assessed in relation to the use-case and recipient rather than only to the item's formal listing status. In policy terms, this helps explain why the EU's Russia-related export compliance discourse is so heavily focused on end use, end user, and circumvention typologies. Trade control is no longer simply a list-administration exercise. It is a risk-governance discipline built around the possibility that items, routes, or intermediaries may change the effective nature of the transaction. Catch-all reasoning is therefore part of the intellectual architecture that underpins enhanced due diligence in sanctions settings[3].

None of this, however, means that operators are expected to eliminate all uncertainty. Both the Commission's 2025 FAQ and the G7 guidance stress that there is no one-size-fits-all approach and that due diligence should be risk-based, proportionate, and adapted to the operator's exposure. The EU FAQ notes that the depth and complexity of expected action depend on the operator's nature and size. The G7 guidance states that no single red flag is necessarily indicative of illicit conduct and that all surrounding facts and circumstances should be considered before determining whether a transaction is suspicious. This is an important balance. Trade-control compliance must be serious enough to detect adaptive evasion but not so blunt that every ambiguity becomes an automatic prohibition. The correct standard is disciplined proportionality. Operators must be able to show that they identified the relevant risks, asked the right questions, examined the right documents, and reacted properly where red flags remained unresolved. In trade-control compliance, effectiveness depends less on omniscience than on the quality of the procedure used to manage uncertainty[4,5].

[1] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[2] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[3] European Commission, Directorate-General for Trade and Economic Security. (n.d.). *Exporting dual-use items*.
[4] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[5] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.

Table 7.2.2-1. Core Trade-Control Compliance Instruments in Russia-Related Export and Re-Export Governance

Instrument	Primary compliance question	Typical operational checks	Main anti-circumvention function
Item classification and control-list review	Is the item controlled, restricted, or high-priority?	Annex checks, HS/CN/ECCN review, CHPI/CHPL relevance, dual-use status	Prevents misclassification and under-screening of sensitive goods
End-user due diligence	Who will actually receive and use the goods?	Corporate profile, business record, ownership/control, end-user certificate, sanctions screening	Detects disguised recipients and proxy structures
End-use verification	Is the declared use plausible and lawful?	Civil/military plausibility test, technical fit, customer business model, end-use assurances	Prevents false civil-use declarations and concealed military-industrial application
Route and logistics analysis	How will the goods move?	Transit countries, circumvention hubs, transport mode, subcontractors, route viability	Identifies diversion via third countries and suspicious logistics layering
Documentation scrutiny	Do the documents cohere across the transaction?	Contract-review, invoice value, HS-code consistency, licence references, shipping documents	Detects falsification, undervaluation, and document-level evasion signals
Contractual anti-re-export controls	Has downstream non-re-export risk been legally constrained?	Article 12g clause, liability wording, essential-element clauses, flow-down commitments	Adds legal friction and evidential leverage against third-country diversion
Enhanced due diligence for CHP / Annex XLVIII goods	Has higher-risk trade been subject to intensified checks?	Article 12gb process, strategic risk assessment, stakeholder and transaction-level questions	Focuses compliance resources on battlefield-relevant and diversion-prone items
Escalation and reporting	What happens when red flags remain unresolved?	Internal escalation, refusal/refrainment, NCA reporting, customs engagement	Converts suspicion into operational interruption and public follow-up

Authorship: prepared by the author on the basis of official EU institutional materials and other documents

Sources:

- European Commission. (2022, April 1). *Notice to economic operators, importers and exporters*.
- European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
- European Commission. (2024, February 22; updated December 18, 2024). *Frequently asked questions concerning the "No re-export to Russia" clause and sanctions adopted following Russia's military aggression against Ukraine*.
- European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
- European Commission, Directorate-General for Trade and Economic Security. (n.d.). *Exporting dual-use items*.
- Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
- Bureau of Industry and Security. (2023, May 24). *Guidance to Prevent Evasion of Prioritized Harmonized System Codes to Russia*.
- Bureau of Industry and Security. (2023, September 14). *Best Practice: Certification to Prevent Diversion to Russia of Highest Priority Items*.

For the Russia sanctions regime specifically, the strategic value of trade-control compliance lies in its ability to close the gap between formal prohibition and adaptive procurement behaviour. Russia and Russia-linked networks have repeatedly sought to reconstruct access to sensitive technologies through third-country distributors, altered routing, relabelling, transshipment points, proxy entities, and re-export structures. The trade-control layer is where the coalition tries to disrupt those patterns before they culminate in battlefield-relevant supply. The Commission's guidance, the 2022 notice, the Article 12g and 12gb FAQs, the G7 updated guidance, and BIS best-practice materials all converge on the same

conclusion: effective compliance depends on combining item knowledge, counterparty knowledge, route knowledge, documentary discipline, and escalation readiness. In that sense, trade-control compliance is not a clerical extension of sanctions. It is one of the principal operating systems through which sanctions try to stay effective under conditions of persistent evasion. Its strength determines whether export bans remain materially constraining or become increasingly porous over time[1,2,3].

The main analytical conclusion is therefore straightforward. Trade-control compliance should be understood as a risk-based operational discipline that integrates export classification, end-user checks, end-use verification, route analysis, documentation scrutiny, contractual safeguards, and escalation procedures. It is effective when these elements are used cumulatively rather than sequentially or selectively. A transaction involving a high-priority item, a weakly documented end user, a circuitous route, inconsistent paperwork, and reluctance to provide assurances should not be assessed as five separate minor irregularities. It should be seen as a composite diversion-risk profile. The recent EU and G7 guidance architecture is moving clearly in that direction. It asks operators not merely to observe prohibitions, but to construct decision processes capable of detecting when apparently lawful trade may in fact serve re-export, sanctions evasion, or prohibited end use. For Part Seven of this report, that is the central point: export, re-export, and end-use due diligence are not peripheral features of sanctions compliance. They are among its most decisive operational instruments[4,5,6,7].

7.2.3. Financial, Insurance, and Payment-System Compliance

Financial, insurance, and payment-system compliance occupies a uniquely strategic place in the sanctions architecture because it sits at the point where commercial relationships are converted into executable value flows. A sale may be agreed, a cargo may be loaded, and a service contract may be signed, but if payment, insurance, or financial intermediation cannot lawfully proceed, the transaction often becomes commercially non-viable. This gives financial compliance a multiplier effect that exceeds the boundaries of banking narrowly defined. It does not merely enforce sanctions after the fact. It often determines ex ante whether a deal can settle, whether risk can be transferred, and whether counterparties are willing to remain engaged at all. In operational terms, financial sanctions are therefore not simply a category of restrictions among others. They are one of the principal means by which the wider sanctions regime is translated into friction, delay, denial, and service withdrawal. The European Commission's consolidated Russia FAQs are organised explicitly under the heading "Banking and Finance", while the EBA's 2024 guidelines frame restrictive-measures compliance as a governance and control problem for financial institutions and, separately, for payment service providers and crypto-asset service providers. Together, these materials show that the financial layer is treated by public authorities as a core operating system of sanctions implementation rather than as a secondary reporting obligation. That is analytically decisive for understanding the pressure architecture applied to Russia[8,9].

The first governance function of financial compliance is to convert sanctions law into transaction-level control. The EBA's 2024 guidelines state that institutions should put in place, implement, and maintain up-to-date policies, procedures, and controls for compliance with restrictive measures, and should

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[3] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[4] European Commission. (2022, April 1). *Notice to economic operators, importers and exporters*.
[5] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[6] European Commission, Directorate-General for Trade and Economic Security. (n.d.). *Exporting dual-use items*.
[7] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[8] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[9] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

allocate responsibility clearly within a sound governance structure. The guidelines also require a restrictive-measures exposure assessment so that institutions can determine what resources and controls are necessary for effective compliance. This is important because financial institutions are not merely passive conduits for payments. They are institutions that must decide, under legal pressure and often under severe time pressure, whether a payment, transfer, trade-finance instrument, or insurance-related service can proceed. The governance logic is therefore risk-based but not optional. Exposure assessment does not remove the rule-based obligation to freeze and not make funds available directly or indirectly to designated persons. It determines how the institution will recognise and manage that obligation across real-world operations. Financial compliance is thus a structured control environment built around the movement of value, not only a legal awareness exercise[1,2].

Payment-system compliance makes this operational role especially visible. The EBA's second set of guidelines, EBA/GL/2024/15, is specifically directed to payment service providers and crypto-asset service providers and sets out what they should do to comply with restrictive measures when performing transfers of funds or crypto-assets. The guidance makes clear that payment compliance is not exhausted by customer onboarding. It requires a screening system adequate and reliable enough to screen transfer data, parties, beneficial owners where relevant, and the information accompanying the transfer itself. The same document also states that PSPs should suspend without delay operations triggering an alert of a possible match with a designated person or entity, or one owned, held, or controlled by a designated person, and that once a possible match is confirmed they should immediately suspend execution, block incoming transfers, freeze the funds, and report the action to the relevant authority. This is a particularly clear example of sanctions compliance functioning as an interruption mechanism. The payment chain is not merely observed; it is paused, analysed, and if necessary immobilised. In a sanctions' regime against Russia, where alternative routes and intermediaries are actively sought, that interruption capacity is one of the main points at which the regime acquires practical force[3].

The Commission's 2026 FAQ on the provision of payment services adds an important nuance to this picture by showing that payment-system compliance must also be legally precise. The FAQ states that Article 5b(2)(b) does not prohibit all payment services as defined in PSD2, but targets specific services such as issuing instruments, acquiring, and initiating, while direct bank transfers and cash withdrawals may continue subject to other compliance responsibilities under EU sanctions rules. The same FAQ clarifies that access to online or mobile banking may continue because Regulation 833/2014 contains an exemption for personalised security credentials necessary to access an existing account. This is highly relevant for compliance design. It shows that payment-system sanctions are not supposed to collapse into indiscriminate financial exclusion. Instead, they must be implemented in a granular way that distinguishes between prohibited enabling services and permitted basic account access or non-prohibited payment functions. In compliance terms, this requires system-level differentiation rather than blanket service denial. The operational challenge is therefore twofold: to stop prohibited payment functionality while preserving those channels that remain lawfully available. This is one of the clearest examples of how legal precision and technical control must work together in the financial layer[4,5].

Instant payment systems intensify these challenges because they compress the time available for sanctions review. OFAC's guidance on instant payment systems states that these systems allow payment transmission and the availability of funds to payees to occur almost in real time and that the high velocity of such payments has led to questions across the financial sector regarding how best to

[1] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] Ibid.
[4] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

implement sanctions compliance in this context. OFAC responds by insisting on a risk-based approach and by encouraging developers of instant payment systems to incorporate sanctions-compliance considerations into system design. It also recommends communication features that allow institutions to gather information relevant to sanctions alerts and exception-processing features that permit a transaction to be removed from the automated process so that an institution has sufficient time to investigate potential sanctions concerns. This guidance is operationally important because it recognises that the speed of a payment rail cannot be allowed to defeat the logic of sanctions control. Real-time settlement is commercially valuable, but near-instant execution without usable exception channels would either generate violations or force indiscriminate blocking. Payment-system compliance therefore becomes partly a matter of infrastructure design. The architecture of the rail itself must make legally informed delay possible[1,2].

This point is even more important when payment services are assessed from a cross-border perspective. OFAC's instant-payment guidance states that domestic instant payment systems generally pose lower sanctions exposure than systems permitting cross-border transactions, and that institutions should base decisions on whether and how to screen such transactions on their risk assessment. The implication is that payment-system compliance is not uniform across rails, products, and geographies. The more cross-border, higher-volume, and data-fragmented a system becomes, the more sensitive it is to sanctions risk. That does not mean all cross-border payments are inherently suspect. It means that system design, onboarding standards, and transaction screening norms must be calibrated to the actual probability that a sanctions nexus will appear. This is particularly important in the Russia context, where routed payments, substituted intermediaries, and modified messaging patterns may be used to preserve access after direct channels have narrowed. Payment-system compliance is therefore not only about detecting listed names. It is about preserving enough informational and procedural control within fast-moving payment systems to prevent speed itself from becoming a circumvention vector[3,4].

The role of correspondent banking and financial messaging is similarly central because sanctions frequently operate by constraining the channels through which cross-border payments are communicated and settled. The Commission's consolidated FAQ explains that Article 5h of Regulation 833/2014 prohibits the provision of specialised financial messaging services to certain Russian banks and to Russian entities more than 50 per cent owned by banks listed in Annex XIV. It then clarifies that while transactions for non-sanctioned trade may still be allowed with de-SWIFTed banks using other means of communication, financial-messaging service providers subject to EU sanctions must not circumvent the prohibition by setting up systems that, under a formal appearance of legality, enable the relevant bank to avoid the substance of the restriction. This is highly instructive for compliance analysis. It shows that messaging infrastructure is not neutral plumbing. It is an object of sanctions control in its right. It also shows that financial compliance must distinguish between the prohibited provision of specialised infrastructure and the continued permissibility of non-prohibited trade using other lawful channels. Correspondent and messaging controls therefore operate at the boundary between outright decoupling and managed residual connectivity[5].

From a compliance-engineering perspective, one of the clearest lessons of partner-jurisdiction practice is that the financial system itself can become the site of violation even when the underlying trade occurs elsewhere. OFAC's 2019 framework identifies as a recurring root cause the use of the U.S. financial system, or the processing of payments to or through U.S. financial institutions, for commercial transactions involving sanctioned persons or countries. It notes that many non-U.S. persons have

[1] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2022, September). *Sanctions Compliance Guidance for Instant Payment Systems*.
[3] Ibid.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

violated OFAC regulations by processing financial transactions, often denominated in U.S. dollars, through U.S. financial institutions in connection with sanctioned activity, and that such cases often involved attempts to conceal activity by stripping or manipulating payment messages or making false representations to banks. This matters beyond the U.S. context because it illustrates a general compliance problem: the payment route itself can activate sanctions exposure even where the goods, services, and immediate parties sit outside the primary jurisdiction. For institutions dealing with Russia-related flows, correspondent banking controls therefore serve both as a legal filter and as a channel-risk indicator. The bank is not simply an intermediary. It is a sanctions gatekeeper whose participation can itself make the transaction unlawful or detectable[1].

This is one reason why suspicious-activity logic in sanctions compliance cannot be collapsed entirely into ordinary AML reporting. OFSI's 2026 general guidance states that an obligation to report to OFSI is additional to any other sanctions reporting obligations, including reports required by regulators or Suspicious Activity Reports submitted to the National Crime Agency under the Proceeds of Crime Act 2002. The guidance expressly adds that reporting to a regulator or submitting an SAR does not fulfil reporting obligations under financial sanctions. This distinction is operationally significant. AML suspicion may focus on criminal proceeds or unusual movement of value, while sanctions suspicion focuses on prohibited nexus, asset freezes, ownership and control, or circumvention of restrictive measures. The two can overlap, but they are not identical. For financial institutions, this means that suspicious-activity logic in the sanctions field must be designed with its escalation pathways, reporting thresholds, and documentation disciplines. The result is a dual-reporting environment in which sanctions-specific alerts must be handled under sanctions rules even when the same facts also raise AML concerns[2,3].

This reporting distinction also affects how institutions think about asset-freeze implementation. The Commission's consolidated FAQ states that the obligation to freeze assets is activated as soon as the holder has reasonable grounds to believe the assets are owned or controlled by a listed person, while the EBA requires PSPs to suspend operations without delay upon a possible match and to freeze without delay once the match is confirmed. OFSI's general guidance then overlays statutory reporting duties, annual frozen-asset reviews, and additional reporting requirements for designated persons under the Russia and Belarus regimes. In practical terms, this means that financial compliance is not limited to screening at the front end. It also includes continuing obligations once funds or economic resources have been immobilised. Institutions must preserve the freeze, document the basis, report through the proper channel, and keep those controls current over time. The freeze is not a one-off event; it becomes a governed state of the asset. This gives financial compliance an enduring custodial dimension that differs from transaction rejection or initial service denial[4,5,6].

The insurance layer adds another essential dimension because it determines whether high-risk transactions can be commercially absorbed and legally serviced. OFSI's maritime-shipping guidance states that UK financial sanctions present unique challenges for those engaged in insurance within the sector and explains that direct insurance, reinsurance, retrocession, insurance intermediation, and services auxiliary to insurance are all considered financial services under UK sanctions regulations. It further notes that making economic resources indirectly available is also a breach, including where insurance coverage is made available to a body corporate owned or controlled by a designated person, and that proxy arrangements may be used to procure insurance on behalf of a designated person. This

[1] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[5] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

is a highly significant compliance principle. It shows that insurance compliance is not only about checking whether the named insured is itself designated. It also requires understanding who benefits from the coverage, who procures it, and whether the cover is being used to shield a transaction or vessel that would otherwise lose access to legitimate risk transfer. Insurance thus functions as both a service and a risk-carrier. Denying that service can have strong coercive effects[1].

The maritime context demonstrates particularly well why insurance compliance is inseparable from beneficial-ownership analysis and anti-evasion due diligence. OFSI's maritime-shipping guidance identifies maritime insurance companies, charterers, ship brokers, ship owners, bunker suppliers, and financial institutions involved in maritime trade finance as actors especially exposed to sanctions risk. It recommends regular risk-based due diligence, including collection and verification of information on beneficial owners, vessel flag details, home ports, and recent ports visited. It also advises that where a company wants to register a vessel or obtain insurance or financing, all parties could ask for thorough documentation about the ultimate beneficial owner or owners of the vessel and verify that information based on the risk level involved. This is a clear illustration of the broader compliance pattern seen elsewhere in Part Seven: identification, verification, and service provision cannot be separated. In the maritime sector, a failure to understand who really owns the vessel, who operates it, and what trade it supports can turn insurance into an unwitting channel of sanctions evasion[2].

EU practice reinforces the same point through asset-freeze logic. The Commission's consolidated FAQ states that ships fall under the asset freeze where they are assets owned or controlled by a listed person and that no services, including maritime services, can be provided to ships owned by listed persons. It goes further in relation to Sovcomflot, stating that it is prohibited for EU operators to provide any funds or economic resources to Sovcomflot and that it is likewise prohibited to provide any funds or economic resources to vessels owned by Sovcomflot because those would be presumed to reach or benefit the company. The significance of this for insurance compliance is obvious. Insurance, reinsurance, P&I cover, financing support, and related maritime services cannot be assessed only at company level if the vessel itself is an asset whose servicing would amount to making economic resources available to a listed party. Service-denial mechanisms thus operate not only against named corporate entities but against the specific operational assets through which trade is conducted[3].

The Price Cap Coalition's 2024 updated advisory for the maritime oil industry shows how the insurance layer is also used as a quality-control and risk-screening device. The advisory warns that ships involved in the shadow trade may rely on unproven P&I insurers operating in opaque jurisdictions with insufficient capital, reinsurance arrangements, or technical expertise to handle a major claim. It then recommends that stakeholders require continuous and appropriate maritime insurance coverage for the entirety of voyages and require vessels to be insured by legitimate providers with sufficient coverage for relevant liabilities. Where that is not the case, the advisory recommends due diligence into the insurer's financial soundness, track record, regulatory record, and ownership structure. This is a crucial evolution in compliance logic. Insurance is no longer treated only as a service that may need to be withdrawn if prohibited. It is also used positively as a proxy indicator for whether a vessel and its wider network remain inside the reputable maritime-services ecosystem. Weak, opaque, or fraudulent insurance becomes a red flag for shadow-fleet activity and price-cap evasion[4].

The same advisory links insurance compliance directly to broader service-denial dynamics. It notes that deceptive practices in the shadow trade may trigger de-risking behaviour from counterparties and lead to loss of access to reputable service providers, financing, customers, and ports. This is an analytically important observation because it captures how sanctions pressure often operates indirectly through

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *Financial sanctions guidance for maritime shipping*.
[2] Ibid.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.

private risk withdrawal rather than solely through formal designation. Where a vessel or shipping structure becomes associated with poor insurance, AIS manipulation, ownership opacity, or opaque ancillary-cost structures, reputable market actors may disengage even before a formal enforcement action is completed. This is not merely over-compliance. In many cases it is a rational response to the difficulty of separating lawful trade from sanctionable conduct in a contaminated risk environment. Insurance, therefore, can function as both a direct compliance instrument and a reputational signal that influences the wider ecosystem of finance, logistics, and port access[1,2].

OFSI's oil-price-cap and maritime-services guidance demonstrates how service-denial mechanisms can also be structured through attestation, general licensing, and breach reporting rather than only through blunt prohibition. The UK guidance page explains that the maritime-services ban and oil-price-cap exception are implemented through industry guidance, reporting forms, and general licences. It also indicates that there is a specific general licence on correspondent banking and payment processing to address the financial-services scope of the maritime-services ban. The same page records updates clarifying that, in some circumstances, actors must cease doing business with counterparties who refuse or fail to provide required information and that online reporting channels exist for suspected breaches and compliance issues related to the maritime transportation of Russian oil and associated services. This is operationally significant because it shows that service denial is not arbitrary. It is tied to documentary cooperation, attestation integrity, and compliance responsiveness. A party that cannot or will not provide the information necessary to establish lawful conduct may lose access to the relevant services[3,4].

Financial institutions are also increasingly expected to function as trade-finance gatekeepers in the export-control environment linked to Russia sanctions. BIS's October 2024 guidance to financial institutions states that their responsibilities under the EAR have increased significantly following Russia's further invasion of Ukraine and the broader national-security imperative surrounding export controls. This is important because it expands the role of banks beyond classic payments screening. Trade-finance providers, correspondent banks, and institutions handling documentary credits or supply-chain finance are also expected to detect export-control and sanctions risk embedded in the underlying trade. That means banks may need to examine end-user information, transaction parties, documentation quality, and jurisdictional routing when deciding whether to process or support trade. Financial compliance in the Russia context therefore intersects increasingly with trade-control compliance. The payment institution is no longer only a settlement agent. It is also a point of scrutiny for whether the commercial activity being financed is itself lawful[5].

These overlapping functions help explain why the OFSI annual review emphasises clear communications, targeted guidance, and responsive licensing across the financial services, cryptoasset, and maritime sectors. OFSI states that its core objective is to ensure sanctions are targeted and impactful while enabling businesses to operate with confidence, and reports tailored support across financial services, legal services, cryptoasset, charity, and maritime sectors. This is a useful reminder that the financial layer is not governed solely through punishment. It is sustained through ongoing interface management between regulators and market actors. In high-friction environments like sanctions against Russia, clarity about reporting, licensing, screening expectations, maritime sector obligations, and oil-price-cap procedures becomes part of compliance effectiveness itself. Financial

[1] Ibid.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.
[3] Office of Financial Sanctions Implementation & HM Treasury. (2026, January 15 update). *Maritime Services Ban and Oil Price Cap: licences and reporting forms*.
[4] Office of Financial Sanctions Implementation. (2026, January 15 update). *Maritime Services Ban and Oil Price Cap: industry guidance*.
[5] Bureau of Industry and Security. (2024, October 9). *Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations*.

and insurance institutions need not only prohibitions, but workable assumptions under which they can refuse, freeze, report, or continue lawfully[1,2].

The cumulative logic of this instrument cluster can therefore be described as one of value-channel governance. Payment systems control transfer execution. Banks control settlement access, account relationships, and trade-finance facilitation. Insurers control whether risk can be externalised and voyages can proceed within the legitimate maritime-services ecosystem. Messaging systems control whether financial communication itself can lawfully occur. Reporting systems convert alerts, freezes, and suspicions into public action. Each component addresses a different point in the chain, but together they determine whether value, risk, and service can continue to circulate. That is why financial, insurance, and payment-system compliance should be analysed not as a subchapter of banking technique but as one of the main pressure systems of sanctions policy. In the Russia case, where alternative logistics, shadow fleets, and rerouted payments have become central to circumvention, control over these channels is often more consequential than control over the formal contract alone[3,4,5].

Table 7.2.3-1. Core Financial, Insurance, and Payment-System Compliance Instruments

Instrument cluster	Primary control object	Key operational tools	Main compliance effect
Banking and asset-freeze compliance	Accounts, funds, economic resources, payment relationships	Sanctions screening, freeze orders, reporting to competent authorities, ownership/control checks	Prevents funds from being made available directly or indirectly to sanctioned persons or entities
Payment-system compliance	Transfers of funds and crypto-assets, payment instruments, acquiring and initiation services	Transaction screening, alert adjudication, suspension without delay, exception processing, data review	Interrupts prohibited or suspicious value transfers before execution or settlement
Correspondent banking and messaging controls	Cross-border communication and settlement channels	Messaging restrictions, route scrutiny, payment-message integrity review, correspondent controls	Denies or constrains access to international payment infrastructure and reduces channel-based circumvention
Suspicious-activity and sanctions reporting	Alerts, freezes, possible circumvention, frozen-asset holdings	Sanctions-specific reporting, frozen-asset reviews, escalation to OFSI/NCAs, separate SAR logic where relevant	Converts private detection into public supervisory or enforcement follow-up
Insurance and reinsurance compliance	Cover for vessels, cargo, aviation/space goods, ancillary financial services	Insured-party screening, ownership/control analysis, proxy-risk checks, denial of cover or renewal	Removes lawful risk-transfer services from sanctioned or high-risk actors
Maritime and oil-price-cap service controls	Russian oil transport chains, shadow-fleet vessels, associated service providers	P&I due diligence, AIS-related red flags, attestation models, itemised cost review, breach reporting	Blocks access to reputable maritime services and disrupts evasion of the oil price cap
Trade-finance and export-linked financial controls	Documentary credits, supply-chain finance, export-related payment flows	Counterparty screening, documentation review, end-user/end-use sensitivity, route analysis	Extends sanctions and export-control discipline into financing and settlement of trade

Authorship: prepared by the author on the basis of official EU institutional materials and other documents
Sources:

[1] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.
[5] U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.

- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). F*inancial sanctions guidance for maritime shipping*.
- Office of Financial Sanctions Implementation & HM Treasury. (2026, January 15 update). *Maritime Services Ban and Oil Price Cap: licences and reporting forms*.
- Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
- Office of Foreign Assets Control. (2022, September). *Sanctions Compliance Guidance for Instant Payment Systems*.
- Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.
- Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.
- Bureau of Industry and Security. (2024, October 9). *Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations*.

The main conclusion is therefore clear. Financial, insurance, and payment-system compliance is one of the most coercively efficient parts of the sanctions architecture because it governs the circulation of value, the availability of risk-transfer services, and the usability of settlement infrastructure. It does so through screening, freezing, transaction suspension, sanctions-specific reporting, insurance denial, maritime due diligence, and infrastructure-level controls over messaging and payment execution. In the Russia sanctions context, this cluster matters especially because circumvention frequently depends on alternative financial channels, opaque vessel ownership, manipulated trade documentation, and shadow-fleet service arrangements. The stronger the financial and insurance compliance layer, the harder it becomes for those adaptive structures to preserve commercially viable access to legitimate markets and services. For that reason, this cluster should be treated not as a technical annex to sanctions policy but as one of its principal operational pressure mechanisms[1,2,3].

7.2.4. Licensing, Derogations, Internal Controls, and Audit Trails

Licensing, derogations, internal controls, and audit trails form the governance layer that allows sanctions compliance to operate lawfully under conditions of complexity rather than collapse into either mechanical prohibition or uncontrolled discretion. Sanctions regimes are not built only from bans and designations. They also contain exceptions, derogations, authorisation procedures, reporting duties, and institutional requirements for how firms are to organise decision-making. This makes the compliance task qualitatively different from simple rule recognition. The operator must not only identify a prohibition, but also determine whether the activity may proceed under an exemption, requires prior authorisation, must be routed through a frozen account, or must be rejected outright. At the same time, it must be able to show, retrospectively, why that decision was taken and on what evidence. This is where internal governance and record discipline become decisive. Without them, licensing and derogation regimes generate uncertainty, inconsistency, and enforcement risk. With them, sanctions law becomes

[1] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.

not only restrictive but administrable. In practical terms, this section concerns the infrastructure of lawful exception-handling and defensible compliance rather than the front-end detection tools analysed in Sections 7.2.1–7.2.3[1,2,3].

The first analytical point is that licensing and derogations are not loopholes in the sanctions' regime. They are structured legal devices through which restrictive measures remain targeted, proportionate, and administrable. The Commission's consolidated FAQs explain that Member States and their national competent authorities are responsible for implementation and enforcement of EU sanctions, including authorisation procedures such as processing times, information and documents required, and the duration of an authorisation. The same FAQ states that, while a national competent authority may grant "bundled authorisations" for similar services offered under the same derogation to the same Russian client during a defined period, Council Regulation 833/2014 does not foresee general authorisations covering entire sectors or activities because such a general authorisation would amount to a de facto exemption requiring explicit Council action. It further notes that, according to the Court of Justice, competent authorities must assess authorisation requests on a case-by-case basis and may not give general approval relieving entities of the need to request authorisation individually. This framework is highly significant. It means that licensing is an instrument of controlled flexibility rather than general relaxation. It allows sanctions to accommodate legally recognised necessities without dissolving into broad administrative permissiveness[4].

This case-by-case logic matters because it defines the legal discipline under which derogations operate. A derogation is not a private interpretation that a firm may apply on its whenever the transaction seems commercially or ethically compelling. It is a legally structured path that normally requires prior authorisation where the regulation so provides. The Commission's FAQ makes clear that authorisations issued by a national competent authority are valid only within that Member State and are not automatically valid in another Member State, including where a parent company and subsidiary operate in different jurisdictions. Operators planning to provide services from multiple Member States must therefore request authorisations in each relevant Member State, while informing their authorities when similar authorisations are being sought elsewhere so that competent authorities can exchange information. This is an important institutional safeguard. It prevents a derogation regime from becoming a fragmented patchwork of uncoordinated permissions that could be exploited through forum-shopping or legal arbitrage. Licensing, in other words, is not just about permission. It is about maintaining the unity of the sanctions regime while allowing limited lawful passage through restricted space[5,6].

The Council's 2024 Best Practices document reinforces this structure by treating authorisation handling as a co-ordination problem as much as a legal one. It states that where a regulation provides for an authorisation regime and so requires, competent authorities should inform the other competent authorities and the Commission of rejected authorisation requests. Even where a regulation does not explicitly impose such a duty, the Best Practices still recommend that competent authorities aim to notify rejected requests in order to minimise the risk of distorting competition in the internal market. This is a very important governance principle. It recognises that sanctions implementation can become uneven not only when authorisations are granted too freely, but also when refusals are not communicated and different Member States unknowingly approach similar applications differently. A licensing regime without communication creates room for duplicated applications, inconsistent outcomes, and unequal burdens across the Union. The legal structure of derogations therefore depends

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[3] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[4] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*
[5] Ibid.
[6] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.

on an informational structure that supports coherence. Compliance, in this part of the regime, is inseparable from inter-authority visibility[1].

The same Council document also clarifies that derogation handling must remain sensitive to purpose and urgency. It states that competent authorities should treat requests for authorisations for humanitarian purposes with priority where appropriate, ensure that applicants are aware of the process, contact points, and indicative timeline, and require applicants to explain the urgency and underlying humanitarian purpose in their applications. This is not a minor administrative courtesy. It is part of how the sanctions regime preserves political and legal legitimacy under high-pressure conditions. Humanitarian derogations are credible only if they are real, accessible, and processed in a manner that does not defeat the urgent needs they are meant to address. At the same time, they must remain sufficiently disciplined to prevent misuse or disguised circumvention. The Council's formulation captures that balance. It does not treat humanitarian handling as automatic. It treats it as priority-based, process-based, and evidentially grounded. Licensing and derogations are therefore not only about deciding yes or no. They are about designing a procedural environment in which lawful urgency can be distinguished from opportunistic invocation[2].

Another important element in this legal-operational architecture is the use of conditions attached to authorisations. The Council Best Practices state that, when competent authorities authorise uses of frozen funds or economic resources, they should consider conditions or safeguards to avoid released funds or resources being used for purposes incompatible with the derogation, and specifically note that direct bank transfers are preferable to cash payments. The same document states that authorisations in such circumstances should normally require payments to be made to a frozen account and that any payment in cash should be explicitly authorised. This is a highly practical compliance principle. It shows that an authorisation is not merely a binary permit. It can be structured to contain the risk associated with the permitted transaction. Conditions such as payment through a frozen account, documentation requirements, or reporting at the end of the authorised period transform the derogation from a simple exception into a monitored corridor of lawful activity. Compliance teams therefore need to treat licences as structured operational instruments, not as blanket waivers. The exact terms matter, and breaching those terms can itself amount to a sanctions' violation[3,4].

The UK framework is particularly useful in showing how a mature licensing system differentiates between specific and general licences. OFSI's 2026 general guidance states that a general licence, issued by OFSI on behalf of HM Treasury, allows multiple parties to undertake specified activities that would otherwise be prohibited, without the need for a specific licence. It also states that, where a relevant general licence exists, OFSI expects applicants to use it, and that a specific licence will generally not be issued for the same activity unless the applicant can show that the general licence cannot be used or is deficient in some way. At the same time, OFSI notes that it does not accept applications for general licences and that such licences are issued by government under conditions deemed appropriate to support policy priorities, often in response to unforeseen circumstances. This provides a useful contrast to the EU model. The UK system has a more developed general-licence practice, while the EU system, at least in the Russia context, remains anchored in Member-State-specific authorisations and case-by-case derogations. For compliance design, this means that firms must understand not only the substantive sanctions rule but also the legal style of exception-management used by the jurisdiction concerned[5].

OFSI's guidance also shows how licensing becomes part of the broader compliance burden rather than a substitute for it. The same general guidance states that each general licence will include any requirements for prior notification of use, record-keeping, and reporting, and that it is the responsibility

[1] Ibid.
[2] Ibid.
[3] Ibid.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[5] Ibid.

of the party using the general licence to ensure that its activities fall within the terms of the licence and that all conditions are met. OFSI further warns that breaching the terms of a general licence is a serious offence, and that parties should not assume a licence will be granted or engage in prohibited activity until they have received an appropriate licence or have been informed that no licence is required. This is a crucial operational principle. A licence is not a device for transferring interpretative risk from the firm to the authority. It is a mechanism that often imposes further compliance obligations on the firm itself. Licensing therefore enlarges the governance task: the institution must track scope, conditions, expiration, amendments, reporting duties, and the exact relationship between the authorised act and the broader sanctions perimeter[1].

Specific licences bring yet another governance challenge because they are often tailored, non-public, and transaction-sensitive. OFSI's 2026 general guidance states that specific licences issued by OFSI are not published, but that licence holders are expected to share them with other parties to the transaction where relevant. It also states that, where applicants are unsure whether a proposed action falls within the licence or whether the licence remains valid, they may seek clarification from OFSI, and that licence applicants are expected to communicate licence issuances, amendments, revocations, or changes to relevant third parties where necessary. This creates a distinctive compliance problem. The operator cannot rely on public market knowledge of the licence. It must govern the licence internally and operationally across all relevant parties. Internal dissemination, version control, and transaction-specific instruction therefore become central. A licence that sits only in the legal department but is not embedded into front-office, operations, finance, or logistics workflows may fail at the point of use. Licensing compliance thus requires controlled internal circulation of authorisation knowledge, not merely possession of the authorisation document[2].

This is the point at which internal controls become indispensable. The EBA's 2024 guidelines state that the management body in its supervisory function should oversee and monitor the internal controls and governance framework put in place to comply with restrictive measures, while the management body in its management function should approve policies, procedures, and controls proportionate to the institution's exposure and ensure the effective implementation of those processes. The same guidelines require that the human and technical resources allocated to compliance with restrictive measures be appropriate and commensurate with exposure. This is highly relevant to licensing and derogation handling because authorisation is not a standalone legal event. It must be fitted into an internal control framework that determines who can submit applications, who can approve reliance on a licence, who monitors conditions, and who escalates uncertainty. Without internal governance, derogations become ad hoc exceptions scattered through the institution. With internal governance, they become rule-bound operational pathways controlled by identifiable actors and procedures[3].

The EBA goes further by requiring a senior staff member in charge of restrictive-measures compliance and by insisting that this person be able to report and have direct access to the management body in both its management and supervisory functions. This is a major governance point for sanctions compliance. It means that responsibility for restrictive-measures handling must be institutionally located at a sufficiently senior level to influence business practice, resource allocation, and escalation decisions. Licensing and derogation questions are often too sensitive to be left to fragmented operational judgement. They may require balancing legal interpretation, business urgency, reputational risk, supervisory expectations, and cross-border coordination. The EBA structure is designed precisely to prevent these issues from being buried within low-level process functions. It gives sanctions compliance a governance anchor. In practical terms, that anchor supports coherent approval matrices, clearer escalation channels, and more reliable interaction with competent authorities[4].

[1] Ibid.
[2] Ibid.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] Ibid.

Approval matrices are therefore not simply a matter of managerial tidiness. They are essential to lawful derogation management. While the EBA guidelines do not use the exact phrase “approval matrix” as a headline concept, they require clear allocation of roles between the management body, senior staff member, business lines, and internal units, and they require staff dealing with alerts and restrictive-measures compliance to have the relevant authority and expertise. In operational terms, this means firms must decide which matters can be resolved by front-line teams, which require compliance or legal review, which need sign-off by senior management, and which must be referred to a competent authority before any action is taken. The need for such matrices becomes acute where a transaction may fall under a derogation but only on certain conditions, or where a licence exists but its scope is uncertain. Without clearly defined approval levels, organisations either over-escalate and paralyse business, or under-escalate and expose themselves to violations. Good internal control does not eliminate discretion, but it structures where discretion resides and under what evidential standard it may be exercised[1,2].

The OFAC framework is particularly useful here because it formalises the governance components of a mature sanctions’ compliance programme as management commitment, risk assessment, internal controls, testing and auditing, and training. Although it is not an EU document, it has analytical value because it captures, in a concise institutional grammar, what is needed to make licensing and derogations usable rather than destabilising. Management commitment ensures that exception-handling does not become an invisible legal backwater. Risk assessment determines where derogation or licensing requests are likely to arise and where internal safeguards should be strongest. Internal controls structure how those requests are documented, escalated, and implemented. Testing and auditing determine whether the control system actually works. Training ensures that staff know how to recognise when an authorisation issue exists and what to do about it. Licensing and derogations therefore sit inside the broader internal-control architecture rather than outside it. They are one of the main areas in which that architecture is stress-tested[3,4].

Outsourcing is another area where the interaction between licensing, controls, and auditability becomes very clear. The EBA states that where operational functions relating to compliance with restrictive measures are outsourced, the institution remains accountable for monitoring and overseeing the quality of the service provider. The guidelines also require controls to ensure that the use of outsourced service providers does not expose PSPs and CASPs to the risk of breaches of restrictive measures, and they require those controls to be documented in the outsourcing agreement. This is highly relevant because many institutions outsource parts of sanctions screening, list updates, alert handling, and sometimes document workflows relevant to licensing or authorised transactions. Outsourcing may increase efficiency, but it does not reduce responsibility. Where a licence has transaction-specific conditions, where reporting is required, or where record retention must be precise, outsourced execution can create severe governance failures if oversight is weak. A defensible compliance system must therefore ensure that any third-party provider involved in restrictive-measures operations is subject to clear contractual obligations, monitoring, and periodic assessment of effectiveness[5].

Training is equally central because licensing and derogation handling cannot be limited to compliance specialists alone. The EBA requires financial institutions to provide regular training to staff so that they remain aware of applicable restrictive measures, the results of the restrictive-measures exposure assessment, and the policies, procedures, and controls used to comply with those measures. It also states that training should be tailored to staff members and their specific roles, and that institutions should document their training plans and be ready to demonstrate to competent authorities that training

[1] Ibid.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] Ibid.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] Ibid.

is adequate and effective. This matters because authorisation issues surface in multiple business locations: onboarding, payments, legal review, trade operations, relationship management, shipping, treasury, and sometimes customer support. If only the formal compliance team understands licensing triggers, firms will miss opportunities to pause or escalate transactions before a breach occurs. Training is therefore part of the audit trail even before an event takes place. It demonstrates that the institution tried to distribute operational literacy across the people most likely to encounter sanctions-sensitive decisions[1,2].

This brings the analysis directly to audit trails and record retention. The EBA's payment-focused restrictive-measures guidelines require rules, following the general record-keeping policy of PSPs and CASPs, for documenting any decision taken in respect of alerts. They also require regular review of screening-system performance and document that policies and procedures should allow case-by-case determinations where they are duly justified and documented. These requirements are not cosmetic. They create the documentary infrastructure through which institutions can explain why a possible match was dismissed, why a transaction was suspended, why a particular authorisation pathway was relied upon, or why a payment was released under specified conditions. In the sanctions field, an undocumented judgement is often little better than no judgement at all. Auditability requires not only retention of the final decision, but retention of the evidential path that led to it. This is why record discipline is so closely tied to defensibility. When challenged by regulators, counterparties, or courts, firms need more than a conclusion. They need a traceable rationale[3].

UK practice makes the reporting and record-retention dimension particularly concrete. OFSI's general guidance states that reporting obligations apply to relevant firms that know or reasonably suspect that a person is designated or that a prohibition has been breached, and it specifies that Russia-specific reporting requirements introduced in December 2023 require relevant firms to submit an initial report and then, by no later than 30 November in each calendar year, a report on the nature and amount or quantity of funds or economic resources held as of 30 September. The annual frozen asset review guidance similarly states that persons holding or controlling funds or economic resources belonging to a designated person must complete and submit the reporting form to OFSI for the reporting exercise. These arrangements are operationally important because they turn record-keeping into a recurring compliance duty, not merely a passive archival practice. Firms must be able to identify frozen assets, quantify them, distinguish changes over time, and report them in an organised way. Audit trails in sanctions compliance thus support not only retrospective enforcement but continuing supervisory visibility over the frozen-asset stock[4,5].

The same UK guidance also shows that sanctions reporting is not exhausted by general suspicious-activity reporting. OFSI states that reporting obligations to OFSI are additional to other reporting duties, including those to regulators or SARs submitted under the Proceeds of Crime Act 2002. This is significant for internal control design because it means that audit trails must be able to support sanctions-specific reporting pathways as distinct from broader AML/CFT processes. Institutions need to know not only that something suspicious occurred, but what sanctions-relevant facts triggered the obligation, what was reported to OFSI, on what date, under which regime, and whether follow-up reporting or annual review was subsequently required. A weakly integrated case-management system can easily cause reporting fragmentation or omission here. For a sanctions programme to be defensible, it must therefore align its documentation architecture with its reporting architecture[6].

[1] Ibid.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[5] HM Treasury, Office of Financial Sanctions Implementation. (2025). *Annual frozen asset review: guidance and reporting form*.
[6] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.

Licensing-specific record discipline is equally important. OFSI's licensing guidance states that each general licence may include requirements for prior notification, record-keeping, and reporting, and that prior notification does not constitute any verification by OFSI that the licence is being used correctly. It also states that if a specific licence has been issued, parties should not assume OFSI agrees with their interpretation of it until clarification is obtained where necessary. These points are crucial because they show that the existence of a licence does not eliminate interpretative risk. Instead, it relocates that risk into the institution's ability to show that it acted within the terms of the licence. This is one reason why specific licences must often be shared with other parties to the transaction and why amendments, revocations, and changes must be communicated to relevant third parties. A valid licence with poor internal dissemination is operationally unstable. A valid licence with strong internal documentation and communication becomes a controlled exception[1,2].

The OFSI supplementary licensing guidance adds another useful governance insight by explicitly covering licensing principles and delegation frameworks. Even without turning to the underlying sub-documents, the page itself makes clear that licensing is treated as a structured area of administrative practice, not merely as an ad hoc discretion exercised in opaque fashion. That matters because a predictable licensing environment supports better compliance behaviour. Firms are more likely to seek authorisation rather than make their aggressive legal assumptions if they understand the principles under which licensing decisions are made, the kinds of delegation that exist internally at OFSI, and the standards of "reasonableness" that may govern permissible payments or expenses. The broader analytical point is that licensing clarity reduces incentives for self-help interpretation. It encourages institutions to route difficult cases into formal channels rather than solving them privately through either over-blocking or under-compliance. In this sense, licensing guidance is part of the control environment on both sides of the public–private interface[3,4].

From the EU perspective, one of the most important discipline-enhancing principles is that authorisation handling must not undermine the restrictive logic of the sanctions' regime. The Council Best Practices state that competent authorities should consider safeguards to prevent released funds or economic resources from being used for purposes incompatible with the derogation and that direct bank transfers are generally preferable to cash. The Commission's FAQ similarly explains that bundled authorisations may be coupled with reporting obligations at the end of the specified period to ensure that the authorisation was used according to the stated conditions. These instruments reveal a common governance logic. Authorisations are not meant to create unmonitored zones of permissibility. They are meant to enable specific lawful acts within a monitored and conditioned framework. Internal controls on the firm side must therefore mirror this logic by treating post-authorisation monitoring as part of compliance, not as a completed matter once approval has been obtained. Audit trails continue after the licence is granted[5,6].

Another reason why auditability matters is enforcement. OFSI's 2026 monetary-penalties guidance states that it sets out the circumstances in which OFSI may consider it appropriate to impose a monetary penalty and how the relevant powers will be used. That means that institutions operating in sanctions-sensitive sectors must assume that, where a suspected breach occurs, the adequacy of internal controls, records, reporting, and decision-making processes may itself become relevant to enforcement assessment. OFAC's framework is even more explicit on this logic, since its core architecture links management commitment, internal controls, testing and auditing, and training to mitigation and enforcement outcomes. In both systems, governance quality affects not only the likelihood of breach

[1] Ibid.
[2] Office of Financial Sanctions Implementation. (2024, updated February 2, 2026). *Financial sanctions licensing: supplementary guidance*.
[3] Office of Financial Sanctions Implementation. (2024, updated February 2, 2026). *Financial sanctions licensing: supplementary guidance*.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.

but the way apparent breaches are judged. This is an important compliance insight. Internal controls and audit trails are not only preventive. They are also part of the institution's defensive architecture when regulators later ask what happened and why[1,2].

The same applies to group structures and cross-border organisations. The EBA requires parent undertakings to ensure that subsidiaries perform restrictive-measures exposure assessments in a co-ordinated way based on a common methodology, while also emphasising that ultimate responsibility for compliance lies with each entity in the group. This has direct implications for licensing and derogation handling. A group may wish to take a consistent approach across jurisdictions, but authorisations are often granted nationally and may not automatically extend to affiliates in other Member States or other legal persons within the group. Internal controls must therefore balance group coherence with entity-level legal specificity. Audit trails must show not only that the group had a common policy, but also that the relevant local entity acted on the basis of the permissions actually available to it. In sanctions governance, group-level consistency is valuable, but it cannot substitute for entity-level legality[3,4].

At a broader strategic level, this entire instrument cluster should be understood as the defensibility layer of sanctions compliance. Screening and due diligence may identify risk, but licensing, derogations, internal controls, and audit trails determine whether the organisation can act on that risk in a way that remains lawful, proportionate, reviewable, and sustainable over time. A sanctions regime without these instruments is likely to become either brittle or arbitrary. It becomes brittle when staff are afraid to move in any ambiguous case because there is no clear authorisation or escalation route. It becomes arbitrary when exceptions are handled informally, records are weak, and oversight is inconsistent. The EU and partner guidance examined here both move in the opposite direction. They build controlled pathways for lawful exceptions, assign responsibility inside institutions, require documentation and reporting, and link governance quality to both implementation and enforcement outcomes. That is why this layer should be treated as a core compliance instrument in its right, not as mere administrative overhead[5,6,7,8].

Table 7.2.4-1. Governance Instruments for Licensing, Derogations, Internal Controls, and Auditability

Instrument	Core Governance Question	Main Operational Content	Principal Compliance Value
Derogation and authorisation procedures	Can otherwise restricted activity proceed lawfully?	Case-by-case assessment, supporting documents, time-limited permissions, conditions and safeguards	Keeps sanctions targeted while preserving lawful narrow exceptions
Bundled or structured authorisations	Can repeated similar activity be managed without collapsing into general exemption?	Time-bound permissions for similar services to the same counterparty, often coupled with reporting obligations	Improves administrative usability without abandoning control
Conditions attached to permissions	Under what safeguards may the authorised act occur?	Frozen-account routing, no-cash assumptions, documentary conditions, post-use reporting	Reduces risk that permitted activity is repurposed for circumvention

[1] HM Treasury, Office of Financial Sanctions Implementation. (2026, February 9). *Financial sanctions enforcement and monetary penalties guidance*.
[2] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[5] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[7] Office of Financial Sanctions Implementation. (2024, updated February 2, 2026). *Financial sanctions licensing: supplementary guidance*.
[8] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

Instrument	Core Governance Question	Main Operational Content	Principal Compliance Value
Internal governance and approval structures	Who is responsible for restrictive-measures decisions inside the institution?	Management-body oversight, senior staff responsibility, escalation channels, role allocation	Prevents ad hoc exception handling and strengthens accountability
Licensing controls in firms	How does the institution ensure reliance on licences stays within scope?	Licence validation, internal dissemination, amendment tracking, expiry monitoring, third-party communication	Converts permissions into operationally controlled conduct
Record-keeping and audit trails	Can the institution explain what decision was taken, why, and on what basis?	Documentation of alerts, approvals, derogation use, reporting, frozen-asset records, training records	Enables supervisory review, enforcement defence, and internal consistency
Training and review	Do staff know when to escalate and how to apply authorised pathways?	Role-specific training, documented training plans, periodic effectiveness review	Keeps licensing and derogation handling usable across business functions
Outsourcing controls	Does third-party support weaken sanctions governance?	Oversight of outsourced functions, contractual controls, effectiveness monitoring	Preserves accountability where operational tasks are externalised

Authorship: prepared by the author on the basis of official EU institutional materials and U.S. official documents
Sources:

- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
- HM Treasury, Office of Financial Sanctions Implementation. (2025). *Annual frozen asset review: guidance and reporting form*.
- Office of Financial Sanctions Implementation. (2024, updated February 2, 2026). *Financial sanctions licensing: supplementary guidance*.
- HM Treasury, Office of Financial Sanctions Implementation. (2026, February 9). *Financial sanctions enforcement and monetary penalties guidance*.
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.

The main conclusion is therefore clear. Licensing, derogations, internal controls, and audit trails are the instruments through which sanctions compliance remains legally usable and institutionally defensible in situations where pure prohibition is either too blunt or insufficiently administrable. They enable lawful exceptions without converting those exceptions into ungoverned openings. They allocate responsibility within firms and between firms and authorities. They structure escalation, condition authorised conduct, and preserve a documentary record capable of supporting review, reporting, and enforcement. In the Russia sanctions context, where the regime is cumulative, operationally dense, and often dependent on careful management of humanitarian, financial, and service-related exceptions, this layer is especially important. A sanctions architecture that identifies risk but cannot process permissions, justify decisions, or preserve records will not remain stable over time. A sanctions architecture that can

do all of those things stands a much better chance of remaining both effective and legally credible through 2026–2030[1,2,3,4].

7.3. Circumvention Risks and Enforcement Challenges

7.3.1. Typologies of Circumvention: Intermediaries, Re-Routing, and Proxy Structures

Circumvention typologies are not marginal anomalies at the edge of the sanctions' regime. They are the adaptive techniques through which targeted actors seek to restore access to goods, services, finance, logistics, and commercial relationships after direct channels have been restricted. For sanctions analysis, this means that effectiveness cannot be assessed only by reference to the formal scope of prohibitions. It must also be assessed against the repertoire of evasive practices that emerges in response to those prohibitions. The European Commission's 2023 due-diligence guidance was issued precisely because operators needed a structured way to identify circumvention risks in their transactions and business relationships. The G7's 2024 updated industry guidance makes the same basic point by treating evasion indicators and typologies as central to compliance rather than as auxiliary intelligence material. FATF's 2025 report broadens the lens still further by arguing that illicit actors are using increasingly sophisticated schemes to evade sanctions and exploit jurisdictional differences, weak transparency regimes, and new technologies. These materials converge on one operational conclusion. Circumvention is now systemic enough that compliance and enforcement must be typology-based, not only rule-based. In the Russia context, that means focusing on the network forms through which restricted access is reconstituted after direct bilateral channels have narrowed[5,6,7].

The first broad typological shift is from direct prohibited dealing to indirect, distributed, and commercially layered engagement. The Commission's 2023 guidance explicitly identifies indirect transactions using intermediaries and shell companies that make no or little economic sense as a red flag requiring deeper screening. The same document also highlights new transactions involving companies in countries known as circumvention hubs, transit through those hubs, and complex corporate or trust structures whose complexity is not justified by the customer's business profile. FATF's 2025 report captures this more generally by listing "enlisting intermediaries to evade sanctions" as a core typology category and by placing front and shell companies, transit through third countries, and bank accounts and financing within that same typological cluster. This is analytically important because it shows that circumvention is often less about a single disguised shipment than about the reassembly of a restricted transaction across multiple nodes. Each node looks less suspicious in isolation than the original direct Russia-linked transaction would have looked. The compliance burden therefore shifts from identifying single obvious breaches to reconstructing the network logic of a transaction that has

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *UK financial sanctions general guidance*.
[4] U.S. Department of the Treasury, Office of Foreign Assets Control. (2019, May 2). *A Framework for OFAC Compliance Commitments*.
[5] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[6] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*
[7] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*

been deliberately fragmented. Circumvention typologies are, in that sense, typologies of disaggregation[1,2].

Third-country intermediaries are central to this disaggregation model. The Commission's 2023 guidance asks operators to examine the country of transit and destination, whether it neighbours Russia or Belarus, whether it has easy transport access to them, and whether it is otherwise known to re-export goods to those jurisdictions. It also states that operators should pay particular attention to exports to countries that do not apply restrictions equivalent to those of the EU. The UK's 2025 guidance for businesses on countering Russian sanctions evasion, updated on 12 March 2026, shows that this logic has only intensified over time: the update specifically revised the list of higher-risk goods and third-country exporters. OFSI's 2025 financial-services threat assessment adds a parallel financial dimension, stating that over 25 per cent of suspected breach reports received from UK financial-services firms had made reference to intermediary jurisdictions and that Russian designated persons have traditionally structured ownership and control of assets through favoured intermediary jurisdictions. These materials point to a common pattern. Intermediary jurisdictions function as substitution spaces where the sanctioned nexus is diluted, relabelled, or delayed rather than openly removed. They are not automatically proof of wrongdoing, but they have become one of the most persistent organisational environments for sanctions evasion in the Russia case[3,4,5].

The significance of intermediary jurisdictions lies not merely in geography but in function. OFSI's threat assessment explains that some intermediary jurisdictions offer greater secrecy through their legal and financial systems, but that jurisdictions lacking strong secrecy features may still be attractive because of the services and products they offer or their links to major markets. The same assessment identifies patterns such as ownership or transfers of assets, networks used to process the funds of sanctioned individuals, non-resident banking, enabler activity, offshore account payments, the use of complex trust or offshore company structures, and the setting up of new companies that appear to be copies of companies closed elsewhere. This is a valuable analytical clarification. Circumvention does not always seek the most clandestine jurisdiction in absolute terms. It often seeks the jurisdiction that best combines legal permissibility, market access, operational familiarity, and sufficient opacity. That makes intermediary jurisdictions functionally heterogeneous but structurally similar. Their role is to host, disguise, or reroute parts of the transaction chain until the original Russia-linked nexus becomes less visible or more deniable. In compliance terms, the jurisdiction becomes a risk signal because of the role it plays in the structure, not simply because of its name on a map[6].

Shell companies, front companies, and shelf entities are a second major typological family. FATF's 2025 report identifies the use of front and shell companies as a core sub-topic under sanctions-evasion typologies and notes that such entities may either conduct no genuine activity or engage in legitimate-appearing transactions in order to access financial systems, facilitate payments, and conclude contracts. The Commission's 2023 guidance provides a more compliance-oriented expression of the same risk by identifying business partners sharing addresses with multiple different companies as likely shelf-company indicators and by warning against complex corporate or trust structures involving offshore companies where the complexity is not justified by the customer's profile. The G7's 2024 guidance likewise identifies shell companies, front companies, intermediaries, brokers, and layered letters of credit as common elements in shipments circumvented through one or more third countries. The typological logic here is straightforward. Shells and fronts create a legal person that can appear

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[4] Department for Business and Trade & Office of Trade Sanctions Implementation. (2025, January 7; updated March 12, 2026). *Countering Russian sanctions evasion and circumvention*.
[5] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
[6] Ibid.

commercially independent while carrying little or no independent economic rationale. The company becomes a masking layer between the sanctioned objective and the visible transaction. Once that masking layer is normalised, further acts such as contracting, invoicing, financing, and shipping can be made to appear routine[1,2,3].

This shell-and-front logic is closely connected to beneficial-ownership manipulation. The Commission's 2023 guidance identifies changes of ownership designed to reduce stakes below the 50 per cent threshold, changes in ultimate beneficial owner shortly before or after sanctions were imposed, movements of assets associated with a sanctioned person by family members or others acting on their behalf, and numerous transfers of shares from sanctioned to non-sanctioned entities incorporated by the same individuals or sharing the same physical address. These are not separate red flags. They are components of a coherent evasive technique: restructuring the visible ownership chain so that the entity no longer looks sanctionable while the substantive control relationship persists. FATF's 2025 report supports the same logic more generally by flagging corporate vehicles, opaque ownership structures, shell companies, and one-day firms as indicators of sanctions-evasion-related activity. The typology therefore depends on the gap between formal control and practical control. Where enforcement relies too heavily on the visible ownership snapshot, rapid ownership engineering can create the appearance of compliance while leaving the underlying influence structure intact. Beneficial-ownership verification is thus central precisely because circumvention often aims to weaponise formal corporate separateness against sanctions enforcement[4,5].

Proxy structures and enabler networks are a third major typological cluster. OFSI's 2025 financial-services threat assessment states that it is almost certain that Russian designated persons have turned to new professional and non-professional enablers in attempts to breach UK financial sanctions and that OFSI has observed significantly increased enabler activity since 2023. It defines non-professional enablers as individuals with close personal ties to designated persons, including family members, ex-spouses, associates, and other proxies, and it explains that such actors may make payments to maintain designated persons' lifestyles and assets, including superyachts, school fees, security services, property management, and high-value goods. This is typologically important because it shows that circumvention does not always require sophisticated international trade structures. Sometimes it relies on social proximity and delegated appearance. The sanctioned person becomes harder to detect because the visible actor is not a front company but a relative, associate, or apparently independent service provider. Such structures can be especially difficult to detect because they often mimic normal personal or professional support relationships rather than unusual corporate behaviour[6].

The proxy typology becomes even more acute where enablers actively front for designated persons. OFSI's threat assessment states that it is likely a small number of enablers have attempted to front for Russian designated persons and claim ownership of frozen assets. It explains that such fronting may be observed especially where ownership or control is unclear because of insolvency, complex corporate structures, or significant liquidity, and that a person presenting as an apparently legitimate businessperson may come forward to claim to be the owner of frozen assets while in reality acting for the designated person. OFSI then identifies red flags such as limited public profiles, little relevant professional experience, inconsistencies in name spellings or transliterations, recently acquired non-Russian citizenships, and frequent or unexplained changes in name or declared location. This is a particularly revealing typology because it shows how circumvention can target the enforcement

[1] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[2] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[3] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[6] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.

perimeter itself. Instead of only moving assets around, the enabler tries to redefine who the asset legally belongs to in the eyes of the institution or authority. Proxy ownership claims therefore operate as an attack on attribution, not only on detection[1].

Another important circumvention family concerns substitution and party-switching within the transaction chain. The G7's 2024 guidance identifies last-minute changes to the parties involved in a transaction from an entity in Russia or Belarus to an entity in another country, payments from entities in third countries not otherwise involved in the transaction, and the listing of a freight forwarder or charter-aircraft operator as the end user. The Commission's 2023 guidance similarly asks operators whether all direct and indirect stakeholders are known, whether the end user can be identified, and whether intermediaries, banks, and end users may themselves be targeted by sanctions or affected by them through ownership or control. This typology works by altering the visible formal party to the transaction while preserving the economic logic of the original prohibited deal. A freight forwarder appears as end user, a third-country payment agent appears as payer, or a newly introduced intermediary appears as consignee. The transaction remains functionally directed toward the same ultimate objective, but its visible party structure has been rearranged to frustrate straightforward sanctions screening. Circumvention in this form relies on the assumption that institutions will privilege declared roles over plausible operational roles. That is precisely why stakeholder mapping has become so important in trade and financial compliance[2,3].

Re-routing and transshipment through third countries constitute a further typology that is both geographically and operationally layered. The Commission's 2023 guidance asks whether the country of transit or destination neighbours Russia or Belarus, whether it has easy transport access, whether it is known to re-export goods there, and whether complex or unusual transportation routes are being used. It also lists transit through countries or territories known as circumvention hubs as a specific indicator warranting deeper screening. The G7's 2024 guidance is even more explicit, identifying circumventing shipments through one or multiple third countries, multiple third-country freight forwarders or shippers, and unclear transportation routes as concrete indicators of evasion risk. FATF's 2025 report likewise lists freight-forwarding firms operating in high-risk transshipment areas, routing purchases through transshipment points commonly used to redirect restricted items to embargoed destinations, and atypical shipping routes for the product and destination as risk indicators. This convergence across sources is important. It shows that re-routing is not a peripheral logistical problem. It is one of the central organisational forms through which sanctions pressure is diluted and reassembled[4,5,6].

Within this routing typology, logistics layering is especially significant. The G7 guidance refers not only to third-country routing in the abstract, but specifically to shell companies, front companies, intermediaries, brokers, layered letters of credit, and multiple third-country freight forwarders and shippers used in connection with such shipments. The Commission's 2023 guidance complements this by recommending checks on the type of means of transport used, routings, and the use of subcontractors where transit through circumvention hubs is involved. The UK's 2025 freight-and-shipping guidance, aimed specifically at freight forwarders, carriers, customs intermediaries, and postal and express operators, begins from the same premise: freight actors may be the first to detect circumvention when transporting or facilitating the transport of goods. The value of logistics layering for evasive actors is obvious. Each additional operator narrows the informational field visible to the others and makes it harder for any single firm to reconstruct the whole transaction. Layering therefore serves

[1] Ibid.
[2] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[3] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention.*
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry.*
[6] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes.*

both concealment and plausible deniability. It is a typology of operational fragmentation designed to exploit the partial vision of each service provider in the chain[1,2,3].

Blind shipments and switch bills are a particularly concrete sub-type of this logistics-layering pattern. The UK's 2025 freight-and-shipping guidance advises operators to treat enquiries from third-party intermediaries arranging a transaction in which the identity of the consignee is hidden from the original supplier or exporter as potentially suspicious and to verify that the use of blind-shipping procedures is legitimate rather than designed to facilitate diversion to a sanctioned country, person, entity, or shell company. It also warns operators to examine requests to produce altered copies of the bill of lading, known as switch bills, and to watch for requests to change paperwork or labels during transit that were not part of the original arrangements. This is an operationally valuable typology because it reveals how evasion can occur not through a hidden item or hidden payer, but through hidden consignee identity and post-dispatch documentary alteration. The shipment moves physically in one chain while its legal-documentary presentation mutates in another. That split between physical movement and documentary identity is precisely what makes the technique dangerous for sanctions enforcement[4].

Postal and express channels can also be exploited as a circumvention sub-typology, especially for smaller high-value components. The UK freight-and-shipping guidance states that postal and express operators should be especially mindful of falsely declared contents because many sanctioned components sought by Russia can be packaged in smaller consignments and declared below customs thresholds. It further warns that those seeking to evade sanctions may take advantage of simplified customs processes, including bulk declarations, and recommends closer checking of shipments containing electronics, drones and drone parts, power tools, mechanical components, vague descriptions such as "spare parts" or "samples", apparent gifts that look commercial, or other signs that the nature or value of the goods may have been falsely declared. This is a useful reminder that circumvention is not always organised through large consignments or complex maritime flows. It can also proceed through repeated small shipments designed to stay below documentary, customs, or screening thresholds. In typological terms, this is fragmentation by quantity rather than by corporate layering[5].

Documentation manipulation is another recurring family of typologies because it allows the transaction to retain formal completeness while distorting the underlying risk picture. The G7's 2024 guidance identifies false, inaccurate, or missing documentation, including names, companies, addresses, final destination, and information in trade documents and financial flows that do not cohere. It also refers to customers unwilling to provide certification that items will not be sold to Russia or sanctioned parties in third countries, vague or incomplete information, and websites or corporate identities that appear thin or recently altered to remove links to Russia. The UK freight-and-shipping guidance likewise highlights vague or dubious descriptions of goods, unusual requests regarding packaging or labels, misclassification of higher-risk goods under adjacent HS codes, and suspected fraudulent documentation as sector-specific red flags. Documentation in these typologies is not merely incomplete. It is actively curated to create an administratively manageable fiction. Circumvention relies on the fact that much trade and finance is processed through documentary trust. Once that trust is strategically exploited, the document layer becomes one of the first places where enforcement must reinsert scepticism[6,7].

[1] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[2] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[3] Department for Business and Trade & Office of Trade Sanctions Implementation. (2025, November 3). *Countering Russian sanctions evasion: guidance for the freight and shipping sector*.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.

Financial re-routing is the parallel typology on the payments side. The G7's 2024 guidance identifies payments from entities located in third countries that are not otherwise involved in the transaction, particularly where the payment runs through a sanctioned country or otherwise breaks with the apparent commercial logic of the deal. The Commission's 2023 guidance likewise treats banks among the indirect stakeholders that must be known and screened, and FATF's 2025 report includes bank accounts and financing within the typology of using intermediaries to evade sanctions. The operational rationale of this technique is clear. Once the original buyer, shipper, or consignee becomes too visible, payment responsibility is displaced onto another company, another account, or another jurisdiction that appears commercially ancillary or neutral. The payment path is then used to absorb or redirect sanctions risk away from the visible trade chain. This means that financial compliance and trade compliance cannot be treated as separate investigative universes. Circumvention often works by breaking that separation and moving the hidden nexus into the payment architecture[1,2,3].

More specifically, OFSI's 2025 financial-services threat assessment shows that intermediary-jurisdiction typologies often involve non-resident banking, offshore account payments, and networks used to process the funds of sanctioned individuals. The same assessment also states that enablers have almost certainly used alternative payment methods, in particular cryptoassets, to breach UK financial sanctions prohibitions on Russia. This is an important extension of the typology map. Circumvention is not only about goods moving through third countries; it is also about value moving through alternative or more weakly monitored channels. Non-resident banking can loosen the connection between the customer and the jurisdiction of account provision. Offshore account payments can complicate attribution and beneficial-owner tracing. Cryptoassets can be used to move value outside traditional payment-system friction, especially where enablers or non-bank payment providers are involved. These methods differ technically, but typologically they perform the same function: they create parallel rails for funds once the primary rails become constrained[4].

Fragmented service provision is another highly consequential but sometimes underappreciated typology. The G7's 2024 guidance indicates that shipments may involve shell companies, intermediaries, brokers, layered letters of credit, multiple freight forwarders, and unexplained third-country payers. The UK freight guidance is specifically addressed not only to exporters, but to freight forwarders, carriers, hauliers, customs intermediaries, postal and express operators, and others facilitating movement of goods. These official materials imply a broader point: evasive networks increasingly distribute functions across specialised actors so that no one actor appears to control the whole transaction. One entity manages the customer relationship, another arranges freight, another provides customs clearance, another pays, another appears as consignee, another insures the cargo, and another receives the goods. This fragmented-service model creates compliance blind spots because each actor may see only a plausible partial narrative. Circumvention then exploits the seams between service providers rather than relying on one large hidden lie. The typology is therefore organisationally sophisticated but conceptually simple: break the prohibited transaction into compliant-looking pieces and rely on the fragmentation of market attention[5,6].

Maritime circumvention patterns are among the most visible and operationally developed forms of this fragmentation logic. The Price Cap Coalition's updated October 2024 advisory states that actors involved in the shadow trade often conceal ownership structures and the origin of cargo, that ownership

[1] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[2] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
[5] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[6] Department for Business and Trade & Office of Trade Sanctions Implementation. (2025, November 3). *Countering Russian sanctions evasion: guidance for the freight and shipping sector*.

of shadow-fleet tankers may be concealed through complex corporate arrangements with increasing use of single-vessel fleets, and that such tankers have been observed disabling or manipulating Automatic Identification Systems to conceal illicit activity or voyage information. OFAC's October 2024 maritime-shipping guidance adds that sanctions evaders are increasingly using vessel location manipulation, including AIS spoofing to show a vessel in a different location and thereby obscure the origin of certain oil cargoes. These sources show that maritime circumvention is not reducible to ship movement alone. It combines vessel identity management, ownership opacity, cargo-origin concealment, and data manipulation. The ship becomes both transport asset and evasive platform. For sanctions analysis, this matters because the maritime typology compresses many other typologies into one sector: shell ownership, proxy service providers, route manipulation, documentation issues, and fragmented risk transfer all converge on the same voyage[1,2].

The maritime typology also includes substandard or opaque insurance and service ecosystems. The Price Cap Coalition advisory warns that shadow-fleet vessels may rely on unproven P&I insurers operating in opaque jurisdictions, without the capital, regulatory oversight, or technical expertise expected in the legitimate maritime-insurance market. It also notes that such vessels may be older, poorly maintained, or associated with weaker safety and certification practices, making marine-casualty accountability more difficult. This is not only a safety issue. It is a circumvention issue because the move into opaque insurance and service chains helps sanctioned or price-cap-evading trade detach itself from the compliance expectations of reputable maritime providers. Once legitimate insurers, financiers, and service providers withdraw, an alternative ecosystem emerges in which the absence of transparency is part of the commercial model. Circumvention here works by reconstructing the service architecture around lower-scrutiny or lower-capability providers. The consequence is that enforcement cannot focus only on cargo ownership or voyage routing. It must also examine who is insuring, certifying, financing, and servicing the vessel[3,4].

These typologies also reveal why public authorities increasingly communicate risk outside formal sanctions lists. BIS's July 2024 guidance on parties presenting diversion risk explains that BIS uses supplier-list letters, Project Guardian requests, red-flag letters, and "is informed" letters to alert companies and universities about parties beyond those identified on screening lists that present diversion concerns in relation to Russia-related end uses or end users. The document also explains that, where a company receives a red-flag letter, it must conduct additional due diligence to resolve the red flag before proceeding and that unresolved red flags should lead the company either to refrain from the transaction or seek a licence. This is an important enforcement-development point. Circumvention increasingly relies on actors who are not yet formally listed but are nonetheless known to present diversion risk. Authorities therefore supplement static list-based enforcement with a more dynamic warning architecture. Typologies matter precisely because not all relevant actors will already sit inside the formal designation perimeter. A sanctions regime facing adaptive circumvention must therefore operate partly through risk-notification and behavioural expectation, not only through list publication[5].

This, in turn, helps explain why no single circumvention sign is usually decisive. The G7's 2024 guidance states explicitly that no single red flag is necessarily indicative of illicit conduct and that transactions should be assessed holistically, while the UK freight guidance makes the same point for logistics actors. Typologies should therefore be understood as composite patterns rather than as isolated facts. A shell company with no web presence may still be innocent in isolation. A route through a third country may still be legitimate in isolation. A third-country payer may sometimes be commercially justified in

[1] U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.
[2] Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.
[3] Ibid.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2026, January 28). *Financial sanctions guidance for maritime shipping*.
[5] Bureau of Industry and Security. (2024, July 10). *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*.

isolation. But when a recently created company with residential address orders high-priority goods inconsistent with its business profile, routes them through a known transshipment hub, uses a third-country payer with no clear role, and resists providing end-use assurances, the pattern becomes typologically legible as circumvention risk. Enforcement and compliance increasingly depend on this pattern-reading capacity. The operative unit is not the single anomaly but the structured cluster of anomalies that make little economic sense except as evasion[1,2].

Table 7.3.1-1. Principal Circumvention Typologies in the Russia-Related Sanctions Environment

Typology	Core Mechanism	Typical Operational Indicators	Main Compliance Implication
Third-country intermediary routing	Reconstructing restricted transactions through non-Russian jurisdictions	Transit through circumvention hubs, unusual destinations, new third-country exporters, non-resident banking links	Requires route, jurisdiction, and stakeholder-based due diligence
Shell / front / shelf companies	Using low-substance legal entities to mask sanctioned nexus	Shared addresses, thin web presence, recent incorporation, little commercial history, opaque ownership	Requires enhanced counterparty and beneficial-ownership verification
Proxy and enabler structures	Using relatives, associates, or service providers to act for designated persons	New payers replacing DPs, family links, lifestyle-maintenance payments, claims over frozen assets	Requires scrutiny of personal/professional connections and source-of-funds logic
Ownership restructuring	Altering legal form while preserving control or benefit	Stakes moved below thresholds, rapid UBO changes, same controllers behind new entities	Requires dynamic ownership/control analysis, not static snapshots
Party substitution	Swapping visible transaction parties while keeping the same end objective	Last-minute changes of consignee, freight forwarder listed as end user, unrelated third-country payer	Requires full stakeholder mapping and explanation of each party's role
Re-routing and logistics layering	Fragmenting transport chains across multiple actors and jurisdictions	Multiple freight forwarders, atypical routes, subcontractors, transshipment points	Requires route coherence checks and chain-of-custody scrutiny
Documentary manipulation	Rewriting the paper trail to mask the real transaction	Misclassification, vague descriptions, false destination/end-use data, switch bills, altered labels	Requires cross-document consistency checks and heightened scepticism
Fragmented service provision	Distributing functions across separate service actors to dilute visibility	Separate parties for payment, freight, customs, insurance, and consignment identity	Requires cross-functional information sharing and holistic transaction review
Shadow-fleet / maritime evasion	Using opaque vessel ownership and service ecosystems to preserve Russian-linked trade	AIS spoofing, single-vessel fleets, opaque P&I, concealed cargo origin, STS-related anomalies	Requires maritime due diligence extending beyond vessel name alone

Authorship: prepared by the author on the basis of official EU institutional materials and U.S. official documents
Sources:

- European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
- Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.

[1] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[2] Department for Business and Trade & Office of Trade Sanctions Implementation. (2025, November 3). *Countering Russian sanctions evasion: guidance for the freight and shipping sector.*

- Bureau of Industry and Security. (2024, July 10). *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*.
- Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
- Department for Business and Trade & Office of Trade Sanctions Implementation. (2025, November 3). *Countering Russian sanctions evasion: guidance for the freight and shipping sector*.
- Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.
- U.S. Department of the Treasury, Office of Foreign Assets Control. (2024, October 31). *Sanctions Guidance for the Maritime Shipping Industry*.

The enforcement challenge created by these typologies is that each one is designed to convert a direct sanctions problem into a disputed factual problem. Instead of an obvious Russian counterparty, there is a third-country company. Instead of a listed owner, there is a recently changed UBO. Instead of a sanctioned payer, there is a non-resident bank account or an apparently unrelated intermediary. Instead of a direct voyage, there is a layered maritime route with manipulated location data and opaque insurance. This is why modern sanctions enforcement increasingly depends on reconstruction rather than mere detection. Authorities and firms must piece together party roles, ownership, routes, payment flows, and documentary inconsistencies across fragmented datasets. Typologies matter because they anticipate where this reconstruction burden will arise. They show that circumvention is not random. It follows recurrent organisational strategies that compliance systems can be designed to recognise. The better the typology map, the more quickly institutions can detect when a transaction is trying to look ordinary by being structurally unusual[1,2,3].

The main conclusion is therefore straightforward. The dominant circumvention typologies in the Russia-related sanctions environment are not isolated technical tricks but recurring organisational forms: third-country intermediation, shell and front companies, ownership restructuring, proxy and enabler activity, re-routing, logistics layering, documentary manipulation, fragmented service provision, and shadow-fleet service ecosystems. Each typology attempts to break the visible link between the prohibited objective and the visible transaction. Each also exploits a different weakness in the compliance chain, whether ownership opacity, route complexity, documentary trust, or fragmented service provision. Effective sanctions implementation therefore requires typology-based vigilance across sectors rather than narrow legal literalism. For Part Seven, the core point is that circumvention is now best understood as a network phenomenon. Enforcement challenges arise not only because actors hide, but because they hide through reproducible structures that reappear across trade, finance, logistics, and maritime services. That is why sanctions compliance and enforcement must increasingly be organised around pattern recognition, not merely static prohibition lists[4,5,6,7].

[1] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[2] Bureau of Industry and Security. (2024, July 10). *Guidance to Industry on BIS Actions Identifying Transaction Parties of Diversion Risk*.
[3] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
[4] European Commission. (2023, September 7). *Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention*.
[5] Group of Seven Sub-Working Group on Export Control Enforcement. (2024, September 24). *Preventing Russian Export Control and Sanctions Evasion: Updated Guidance for Industry*.
[6] Price Cap Coalition. (2024, October 21). *Updated Price Cap Coalition Advisory for the Maritime Oil Industry and Related Sectors*.
[7] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.

7.3.2. Weak Points in the Compliance Chain

The compliance chain is only as strong as its weakest operational link, and in the Russia-related sanctions environment those weak links are rarely isolated. They tend instead to accumulate across data, institutions, workflows, and sectors, creating compound implementation risk. A sanctions regime may have broad legal coverage, detailed lists, and strong political backing, yet still underperform when information is incomplete, ownership opacity persists, reporting is fragmented, or institutions lack the capacity to act on the signals they receive. The European Parliament's 2023 study is particularly useful here because it frames implementation and enforcement as the underdeveloped side of EU sanctions policy and shows that the Union's decentralised model has produced a mosaic of practices rather than a uniformly robust system. FATF's 2025 report adds a wider cross-border dimension by warning that sanctions-evasion schemes exploit jurisdictional differences, weak beneficial-ownership regimes, uneven oversight, and limited information sharing. The EBA's 2024 guidelines then bring the problem down to operational level by documenting weaknesses in screening systems, data quality, calibration, and institutional understanding. These sources together show that the compliance chain does not fail only at the endpoint of enforcement. It can fail at almost every stage: identification, verification, escalation, reporting, supervisory follow-up, and cross-border coordination. Weakness in one stage can easily distort or neutralise the others. For that reason, the present subsection treats compliance failure not as a single gap but as a chain of interlocking vulnerabilities[1,2,3].

A first weak point is basic data quality. Screening, ownership analysis, route checks, and transaction monitoring all depend on the availability of accurate, up-to-date, and sufficiently detailed data. The EBA's 2024 report states that competent authorities found deficiencies in screening systems to be common, including outdated or incorrect lists, overreliance on vendor systems, inadequate screening frequency, limited fuzzy matching, and weaknesses in the scope of screening. The same report also notes that even technically sound systems will produce inefficient and inaccurate outcomes where customer or beneficial-owner data are incomplete or mistaken. This is a critical starting point because compliance is often described as a matter of governance, yet governance itself cannot perform reliably on a poor informational base. If the customer database contains misspelled names, outdated ownership details, inconsistent transliterations, or weak data fields, then the first filtering layer is already compromised. In such a situation, even diligent firms may generate both false negatives and false positives. The practical result is that data weakness becomes a multiplier of every later weakness in the chain. High-quality compliance cannot be built on low-quality identity information[4].

A second weak point is beneficial-ownership opacity. The compliance chain increasingly depends on determining who truly owns, controls, or benefits from an entity, because sanctioned actors often rely on formally non-listed intermediaries and legal vehicles. Yet the EBA's final report explicitly records that access to beneficial-owner registers differs from one Member State to another, while FATF's 2025 report states that proliferation-financing and sanctions-evasion vulnerability deepens in countries with weak national laws on transparency of beneficial ownership for legal entities. FATF also warns that obfuscation techniques become even harder to detect in unregulated sectors or sectors with inadequate oversight. This combination is highly problematic. It means that even when operators know that beneficial ownership matters, they may not have timely, reliable, or harmonised access to the necessary information. Where ownership data are dispersed, stale, or legally difficult to obtain, control-based sanctions become harder to apply consistently. The weak point here is not only concealment by evaders. It is the uneven transparency environment in which compliance institutions must work. That

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

environment introduces systemic uncertainty into one of the most important sanctions tests in modern compliance practice[1,2].

A third weak point lies in the decentralised and uneven institutional architecture of implementation across the EU. The European Parliament's 2023 study states that the decentralised nature of sanctions enforcement has produced a mosaic of implementation and enforcement practices across the Union, with more than 160 designated competent authorities in Member States. The same study adds that Member States rely on widely different national sanctions implementation systems, varying in the number of NCAs, the degree of centralisation or decentralisation, the coordination forums they use, and even the mandates available for granting authorisations and licences to private actors. This is a major structural issue because compliance depends heavily on clear expectations about where firms should escalate cases, how rapidly authorisations are processed, and what kinds of interpretation are likely to be accepted. A fragmented public architecture inevitably transmits fragmented expectations to the private sector. It also makes cross-border firms more difficult to govern coherently, because they encounter different institutional logics inside what is formally the same Union regime. The problem is not decentralisation as such. The problem is decentralisation without strong enough convergence mechanisms to keep implementation patterns aligned. In sanctions compliance, that produces uncertainty at precisely the points where firms most need clarity[3,4].

A fourth weak point concerns public-sector coordination within Member States themselves. The Council's 2024 Best Practices state that Member States should ensure efficient national coordination and communication mechanisms between all relevant government agencies, bodies, and services with competence in restrictive measures. The fact that this recommendation must be stated so explicitly is already revealing. It signals that sanctions' implementation frequently spans multiple authorities with different mandates, including ministries, customs, supervisors, FIUs, law-enforcement bodies, prosecutors, and judicial actors, and that weak coordination between them can easily degrade the effectiveness of the regime. Where information does not travel efficiently across these bodies, firms may receive incomplete or inconsistent signals, reporting may not reach the most operationally relevant authority quickly enough, and intelligence may not translate into action. This is especially damaging in the Russia context, where circumvention frequently crosses domains: trade, banking, logistics, ownership, maritime services, and professional facilitation. A fragmented state response to a networked sanctions-evasion scheme creates precisely the blind spots on which the scheme depends. The compliance chain therefore depends not only on public–private interaction but also on public–public coherence[5,6].

A fifth weak point is limited administrative capacity. The European Parliament's 2023 study reports that, in several Member States, NCAs operate with relatively small teams dedicated to sanctions implementation, and that rising documentation and reporting requirements, together with the rapidly increasing scale and scope of EU sanctions regimes, have put significant strain on their limited resources. The study also notes that, as with most national implementation systems across the EU, Danish NCAs had only limited capacities for proactive monitoring and controlling the actions of individuals, financial institutions, and economic operators in order to pre-empt possible sanctions violations. These findings are analytically important because they reveal the difference between nominal responsibility and practical capacity. A system can assign implementation duties to NCAs, customs, or supervisory agencies and still remain weak if those authorities are understaffed, overloaded, or structurally reactive. In such circumstances, sanctions enforcement tends to depend too heavily on

[1] Ibid.
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[4] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[5] Ibid.
[6] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

private reporting and too little on proactive public detection. Resource constraints therefore shift the burden of vigilance downstream while simultaneously weakening the public side's ability to assess and act on what it receives. Capacity scarcity, in other words, is not merely an administrative inconvenience. It is a structural weak point in the enforcement chain[1].

A sixth weak point lies in the quality and timeliness of guidance. The modern sanctions regime depends heavily on FAQs, best-practice documents, national guidance notes, and sectoral support channels because legal texts alone do not provide enough operational specificity for firms. Yet the need for frequent guidance itself signals a vulnerability: whenever interpretative support lags behind legal updates or circumvention patterns, operators are left to improvise under pressure. The European Parliament study recommended that the EU ensure adequate guidance for economic operators and work toward clearer definitions and more coherent implementation structures. The European Commission's sanctions implementation article of June 2025, which promotes the EU Sanctions Helpdesk and stresses support for SMEs, implicitly recognises the same problem. If a major Helpdesk is necessary to make the sanctions regime practically usable, then operator capability and interpretative accessibility remain uneven. Guidance overload can also become its problem, especially for smaller actors who lack dedicated sanctions teams. The weak point here is not only absence of guidance, but the difficulty of converting frequent, layered, and sometimes technically dense guidance into confident day-to-day decisions[2,3].

A seventh weak point is uneven sectoral competence outside the best-resourced parts of the financial system. FATF's 2025 report states that complex sanctions-evasion schemes are harder to detect in unregulated sectors or sectors with inadequate oversight, and that many designated non-financial businesses and professions are unaware of their responsibilities in monitoring and reporting proliferation-financing-related activities. FATF also notes that private-sector entities across sectors reported a lack of public-sector feedback on relevant SARs and STRs, which may make the challenge even harder to address. This has broad relevance to the sanctions chain. Sanctions regimes increasingly rely on actors such as freight forwarders, customs intermediaries, high-value goods dealers, art market participants, service providers, and VASPs, but those sectors do not always possess the same institutionalised compliance culture as large banks. The result is a compliance landscape in which sophistication is highly uneven. Some nodes in the chain may screen intensively, while others may barely understand what patterns should concern them. That unevenness is operationally dangerous because circumvention networks will naturally migrate toward the weakest-supervised or least-experienced nodes[4,5].

An eighth weak point concerns the calibration of screening systems themselves. The EBA's 2024 report identifies limited fuzzy matching, inadequate calibration, and poor understanding of screening systems by PSPs and CASPs as recurring supervisory concerns. This is highly significant because it means sanctions risk does not arise only from not having a system. It also arises from having a system that is technically present but misconfigured. Inadequate fuzzy matching can miss transliterated or slightly altered identifiers. Excessive sensitivity can swamp analysts with weak alerts. Poor system comprehension means that staff may trust or distrust alerts for the wrong reasons. In a sanctions context shaped by multilingual names, frequent updates, and layered beneficial-ownership risks, calibration is not a cosmetic tuning exercise. It is part of the legal-operational integrity of the screening process. Where calibration is weak, the chain becomes noisy in the wrong places and silent in the wrong places[6].

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*
[2] Ibid.
[3] European Commission. (2025, June 11). *Sanctions implementation*.
[4] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[5] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

A ninth weak point is overreliance on vendors and external systems. The EBA states that competent authorities observed overreliance on vendors' screening systems together with a poor understanding of those systems by PSPs and CASPs. This is an important operational failure mode. Outsourced tools can improve efficiency and scale, but they do not eliminate the need for institutional judgement, calibration choices, data governance, and internal ownership of compliance outcomes. A firm that does not understand how its external screening system matches names, updates lists, handles aliases, treats free-text fields, or prioritises alerts cannot meaningfully defend its decisions. It becomes dependent on black-box logic at precisely the moment when sanctions enforcement increasingly demands reasoned and documentable control choices. The weak point, therefore, is not outsourcing per se. It is outsourcing without interpretative control. In such cases, the firm appears compliant by infrastructure while remaining weak in governance[1].

A tenth weak point concerns incomplete scope of screening. The EBA reports that supervisors found weaknesses in the scope of screening, with not all customers and beneficial owners being captured by the screening process. It also records that incomplete or mistaken customer and beneficial-owner data lead to inefficient and inaccurate outcomes, even where the screening system itself is technically sound. This problem is more serious than it may first appear. If some parties, owners, or transaction participants are not in the screening perimeter at all, then improvements in alert management or escalation cannot repair the omission after the fact. The weak point lies at the boundary of the system itself: who is screened, when, and on the basis of which fields. In Russia-related sanctions, where evasive actors deliberately shift the visible nexus to less obvious persons, representatives, intermediaries, or beneficial owners, scope weakness can be fatal. It creates the very blind spot that circumvention strategies seek to exploit[2].

An eleventh weak point is the tension between comprehensive screening and alert overload. The EBA consultation feedback records industry concerns that screening the purpose of fund transfers and free-text fields could be too burdensome and would lead to a significant increase in false positives. It also records concerns that interim freezing or rejecting payment instructions where information is insufficient would considerably slow the processing of funds, given the high number of false positives. This is one of the clearest windows onto what is often called alert fatigue, even where the document does not use that exact phrase. Institutions face a practical dilemma. If they widen the screening field aggressively, they may generate so many alerts that genuine risk becomes harder to distinguish. If they narrow the field too much, they miss evasive signals embedded in narrative fields, routing details, or ancillary identifiers. The weak point here is therefore not simply technical. It is organisational and economic. Excessive noise can degrade human review capacity, slow legitimate business, and create pressure to downgrade sensitivity[3].

A twelfth weak point is the mirror-image problem of false negatives. The EBA does not label a separate section "false negatives", but the logic is clear from its findings on inadequate calibration, limited fuzzy matching, poor data quality, and incomplete screening scope. False negatives arise when designated persons, controlled entities, or suspicious transactions pass through the system without meaningful challenge. In the Russia sanctions environment, this risk is increased by transliteration variants, beneficial-ownership opacity, route complexity, and the use of intermediaries who appear commercially plausible on the surface. FATF's 2025 report strengthens this point by warning that sanctions-evasion schemes exploit jurisdictional differences, new technologies, and weaknesses in beneficial-ownership transparency. The weak point, therefore, is not just that some bad actors may escape detection. It is that the structural conditions of detection are themselves uneven and often inadequate. A compliance chain

[1] Ibid.
[2] Ibid.
[3] Ibid.

burdened by data gaps and fragmented oversight will tend to under-detect precisely the more sophisticated forms of circumvention[1,2].

A thirteenth weak point lies in the speed-pressure mismatch between modern finance and sanctions review. EBA feedback on instant payments and payment-transfer screening shows that institutions worry about the operational burden created when sanctions review must occur in extremely compressed timeframes. OFAC's guidance on instant payment systems, while U.S.-based, reinforces the same point by insisting that systems need exception-processing features and communication tools so that potential sanctions concerns can be investigated despite real-time or near-real-time execution. The weak point here is structural. Financial infrastructure is built around speed, but sanctions control often requires pause, inquiry, and cross-checking. Where the system cannot be slowed in a disciplined way, either violations may slip through or institutions may overcompensate by blocking too broadly. Speed thus becomes a compliance vulnerability when the architecture of the payment rail is not aligned with the architecture of sanctions control. In a Russia-related environment marked by alternative payment channels and routed value flows, that vulnerability becomes particularly salient[3,4].

A fourteenth weak point concerns fragmented reporting and the limited usefulness of what is reported. The European Parliament study notes that enhanced documentation and reporting obligations can become an additional burden for NCAs that already face strained human resources. The same study also states that information-sharing and accountability among stakeholders involved in monitoring and evaluation need to be improved, including by ensuring that institutions' information requests are specific and concise and that NCAs respond in a timely and comprehensive manner. FATF's 2025 report adds a private-sector perspective by noting that firms reported a lack of public-sector feedback on relevant SARs and STRs. This combination is highly revealing. Reporting can be both too burdensome and not informative enough. Authorities may receive more material than they can process usefully, while firms may receive too little feedback to refine future judgement. The weak point is therefore not the absence of reporting channels as such. It is the absence of a sufficiently high-quality, reciprocal reporting ecosystem[5,6].

A fifteenth weak point is public–private information-sharing friction. FATF's 2025 report states that private-sector entities identified uneven implementation of data-privacy provisions, regulatory restrictions, confidentiality and trust concerns, delays in dissemination of intelligence, inconsistent data formats, and resource constraints as information-sharing challenges. The report also notes that sanctions-evasion actors exploit jurisdictional differences in approach and enforcement. This has direct relevance for the EU compliance chain. Even where firms are willing to report and authorities are willing to act, useful information may not travel quickly, in a compatible format, or with sufficient legal confidence. Data-protection concerns and sector-specific confidentiality rules can further complicate the exchange of ownership, payment, or transaction information across borders. The weak point therefore lies not simply in what each actor knows, but in what actors can legally and practically exchange with one another. In a networked sanctions-evasion environment, slow or fragmented information-sharing can neutralise otherwise solid controls[7,8].

A sixteenth weak point is the uneven level of proactive monitoring. The European Parliament study explicitly states that many national implementation systems have only limited capacities for proactive monitoring and controlling the actions of individuals, financial institutions, and economic operators in

[1] Ibid.
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] U.S. Department of the Treasury, Office of Foreign Assets Control. (2022, September). *Sanctions Compliance Guidance for Instant Payment Systems*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[7] Ibid.
[8] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.

order to pre-empt possible sanctions violations. This matters because a system overly dependent on ex post detection and private reporting can still fail even when firms make genuine efforts. Complex Russia-related circumvention schemes often cross multiple jurisdictions, sectors, and service layers. If authorities intervene only after a firm has already identified the issue, then enforcement remains reactive to the private sector's detection perimeter rather than broader than it. Proactive monitoring, by contrast, allows authorities to test sectors, identify recurring patterns, and push typologies back into compliance guidance before the private system encounters them alone. A weak proactive capacity therefore means that the public side of the compliance chain becomes too passive. That, in turn, increases the probability that sophisticated evasion will remain invisible longer than it should[1,2].

A seventeenth weak point is the dependency of the whole chain on sectors that remain partially under-supervised or rapidly evolving. FATF's 2025 report highlights the role of VASPs and other new technologies as areas where obfuscation is harder to detect and where regulatory weaknesses remain significant. It states that three quarters of FATF Global Network countries were assessed as non-compliant or only partially compliant with international standards on virtual assets and VASPs, leaving the sector vulnerable to abuse. This is directly relevant to sanctions compliance because evasive actors seek out not only permissive jurisdictions but also permissive sectors and technical infrastructures. A compliance chain that is comparatively strong in mainstream banking but materially weaker in adjacent payment, crypto, or trade-service ecosystems will still be vulnerable overall. The weak point here is uneven modernisation. Sanctions controls have evolved quickly in some sectors, but evasive actors do not wait for all sectors to catch up at the same rate[3,4].

These weak points do not operate independently. On the contrary, they reinforce one another. Poor beneficial-ownership data increases the burden on screening systems. Weak calibration increases false positives, which increases workload for already stretched compliance teams. Divergent Member State practice reduces predictability, which encourages defensive over-compliance or inconsistent escalation. Limited NCA resources slow authorisation handling and feedback, which increases private uncertainty. Weak public–private information sharing reduces the value of reporting, which in turn degrades future detection. The compliance chain therefore behaves less like a series of isolated controls and more like an interdependent system in which stress in one node redistributes pressure across the rest. This is why improvements at only one point in the chain often have limited effect if adjacent weak points remain untreated. Effective sanctions implementation requires not only stronger controls, but stronger linkages between controls[5,6,7].

Table 7.3.2-1. Principal Weak Points in the Sanctions Compliance Chain

Weak Point	Operational Manifestation	Primary Consequence	Wider Systemic Effect
Poor data quality	Outdated lists, incomplete customer fields, mistaken BO data, inconsistent transliterations	Inaccurate screening outcomes	Both false negatives and false positives increase
BO opacity	Weak registries, uneven access, opaque legal vehicles, control hidden behind non-listed entities	Ownership/control tests become unreliable	Evasion through front entities becomes harder to detect

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[2] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
[5] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[7] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.

Weak Point	Operational Manifestation	Primary Consequence	Wider Systemic Effect
Divergent Member State practice	Different NCA structures, mandates, processes, and coordination models	Uneven interpretations and authorisation handling	Internal market fragmentation and forum-shopping risk
Limited public-sector capacity	Small NCA teams, reactive monitoring, strained human resources	Slower guidance, weaker proactive detection	Overreliance on private reporting
Weak public–public coordination	Poor inter-agency communication among NCAs, customs, supervisors, FIUs, prosecutors	Delayed or incomplete follow-up	Networked evasion crosses bureaucratic seams
Guidance and usability gaps	Late, dense, or hard-to-operationalise guidance; SME dependence on support services	Private uncertainty and defensive compliance	Lower coalition sustainability over time
Sectoral expertise gaps	Weak sanctions literacy in non-bank and trade-adjacent sectors	Missed red flags and poor escalation	Evasion migrates to weaker sectors
Miscalibrated screening systems	Limited fuzzy matching, bad thresholds, poor system understanding	Either missed hits or excessive alerts	Lower trust in screening outputs
Vendor overreliance	Black-box screening without internal understanding or oversight	Weak defensibility of decisions	Apparent compliance without real governance
Narrow screening scope	Customers or BOs not fully captured; incomplete party coverage	Hidden nexus remains outside the control perimeter	Structural blind spots for indirect sanctions exposure
Excessive false positives	Noisy alerts, burdensome free-text screening, interim-freeze dilemmas	Analyst overload and slower processing	Pressure to weaken screening sensitivity
Fragmented reporting and weak feedback	High reporting burden, limited authority response, poor learning loop	Low informational value of reports	Reduced detection quality in future cases

Authorship: prepared by the author on the basis of official EU institutional materials and documents
Sources:

- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
- European Commission. (2025, June 11). *Sanctions implementation*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
- Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
- Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.

The main conclusion is therefore clear. The weak points in the compliance chain are not confined to one part of the sanctions system and cannot be solved by stronger enforcement rhetoric alone. They lie in data quality, beneficial-ownership transparency, divergent national structures, limited administrative capacity, weak inter-agency coordination, uneven sectoral expertise, miscalibrated screening, vendor dependency, reporting friction, and thin feedback loops. Each of these weaknesses creates room for either under-compliance or dysfunctional over-compliance. Together they generate a compliance environment in which sophisticated Russia-related circumvention can exploit both legal complexity and institutional fatigue. For Part Seven, the analytical implication is decisive: the sanctions regime must be assessed not only by the strength of its prohibitions, but by the resilience of the chain that carries those

prohibitions into operational practice. Where that chain remains patchy, the sanctions architecture remains more vulnerable than its legal surface may suggest[1,2,3,4].

7.3.3. Over-Compliance, De-Risking, and Private-Law Frictions

Over-compliance is the point at which sanctions implementation ceases to be a disciplined translation of legal obligation into operational control and begins instead to function as a broader private-sector withdrawal from risk, counterparties, sectors, or jurisdictions. In the compliance architecture, this phenomenon is not merely the opposite of under-enforcement. It is a distinct implementation pathology. A firm facing legal uncertainty, reputational exposure, strict-liability risk, complex ownership chains, and imperfect guidance may decide that the safest option is not to manage the risk but to exit it. In that sense, over-compliance is often a product of rational institutional self-protection rather than ideological excess. Yet once it becomes systematic, it can distort the sanctions regime's intended targeting logic. The legal rule may remain formally precise, but the market response becomes wider than the law requires. This is why over-compliance must be analysed as part of sanctions effectiveness rather than as a purely private inconvenience. It affects who bears the burden of sanctions, how lawful activity is treated, and whether the coalition can maintain the regime without generating avoidable collateral frictions. In the Russia-related setting, where compliance obligations have become dense and fast-moving, the risk of defensive overreach has become especially salient[5,6,7].

In contemporary regulatory language, the closest general analogue to sanctions over-compliance is de-risking. The EBA's 2022 Opinion states that de-risking occurs across the EU and affects different categories of customers and potential customers, and that it can lead to adverse economic outcomes or amount to financial exclusion. FATF's 2025 financial-inclusion guidance goes further by reiterating that de-risking is, by definition, inconsistent with a proper application of the risk-based approach when it amounts to cutting off entire classes of customers rather than managing individualised risk. That principle is highly relevant to sanctions compliance. Sanctions law generally requires targeted restrictions, targeted freezes, targeted prohibitions, and targeted due diligence. It does not ordinarily require the wholesale abandonment of all relationships touching a country, nationality, or risk category. When financial institutions or service providers stop managing risk and instead retreat from broad classes of exposure, they are no longer merely complying. They are creating an additional private sanctions layer that may diverge from the public legal design. Over-compliance therefore matters not because caution is undesirable, but because wholesale caution ceases to be risk-based in the legally relevant sense[8,9].

It is important, however, not to caricature defensive compliance as irrational. The UK government's 2026 call for evidence on the ownership-and-control test explicitly acknowledges that the control element can be difficult to identify and assess, that this can lead to uncertainty, increased compliance costs, and a tendency towards de-risking, and that firms may limit, withdraw, or refuse services to clients, sectors, or jurisdictions perceived as presenting a higher risk of non-compliance. The same document notes that the language of the control test is purposefully broad in order to strengthen the impact and deterrent effect of financial sanctions, while also acknowledging that this creates challenges for practical application. This is a central analytical point. Over-compliance often emerges where the law

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] Office of Financial Sanctions Implementation. (2025, February). *Sanctions compliance in the financial services sector: threat assessment*.
[5] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.
[6] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[7] Financial Action Task Force. (2025). *Guidance on Anti-Money Laundering, Terrorist Financing Measures and Financial Inclusion*.
[8] Ibid.
[9] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.

intentionally uses broad concepts in order to catch disguised control, indirect benefit, or evasive restructuring. The legal design is therefore not neutral with respect to defensive market behaviour. Where the law broadens the perimeter to prevent circumvention, firms may broaden their risk avoidance perimeter to prevent error. Over-compliance is thus partly the private-sector shadow cast by anti-circumvention ambition[1].

The same UK document is also important because it recognises the unintended consequences of this dynamic in unusually direct terms. It states that, while de-risking may in some circumstances be a prudent response to reduce regulatory risk, it can have unintended negative consequences such as undermining legitimate business activity and disadvantaging entities that are not subject to financial sanctions. It further notes that the same uncertainty may result in inadvertent non-compliance in the opposite direction, where firms fail to identify cases in which financial sanctions should in fact be applied. This dual warning is highly instructive. It shows that over-compliance and under-compliance are not opposite worlds but twin risks generated by the same uncertainty. Where firms cannot confidently determine the legal perimeter, some will over-withdraw while others will miss relevant nexus. Defensive compliance is therefore not simply an excess of caution. It is a symptom of implementation stress. That stress then radiates outward into legitimate business relationships, sectoral access, and the allocation of compliance costs across the economy[2].

The European Commission's Russia FAQs show just how easily lawful activity can be caught inside that private overreach. The consolidated FAQ states that there is no general prohibition for EU citizens to make payments to Russian nationals holding bank accounts in Russian banks, provided the payment does not breach other specific prohibitions. It also states that there is no general prohibition for EU entrepreneurs to make payments to legal entities registered in Russia and no general prohibition on receiving payments from Russian legal entities where the underlying trade is non-prohibited. The same FAQ goes on to say, in relation to a Russian citizen with permanent residence in an EU Member State, that if neither the person nor the client is designated and the services are not prohibited, the Commission sees no reason why a bank should be restricting the account and that the sanctions do not provide a legal basis to refuse payments to that account based on Russian nationality. These clarifications matter because they reveal the gap that can open between the legal perimeter and private practice. Where banks or other institutions generalise from sanctions risk to broad nationality-based or geography-based refusal, they may be creating a layer of exclusion for which the sanctions framework itself offers no legal basis in the case at hand[3].

That same conclusion is reinforced by the Commission's newer payment-services clarification. The March 2026 FAQ on payment services makes clear that Article 5b(2)(b) does not prohibit all payment services, but only specific services such as issuing instruments, acquiring, and initiating. It also states that continued use of existing payment instruments is not prohibited, that EU operators are not required to cancel or freeze existing cards, and that access to online or mobile banking can continue. It further clarifies that direct bank transfers and cash withdrawals are not prohibited by Article 5b(2)(b), although other sanctions rules may still be relevant depending on the case. These clarifications are highly relevant for the analysis of over-compliance because they show that even in politically sensitive Russia-related areas, the law preserves a narrower and more differentiated structure than firms may sometimes assume. Blanket service termination may therefore reflect private caution rather than public legal necessity. The distance between those two can create serious commercial and legal friction[4,5].

The EBA's April 2022 statement on financial inclusion in the context of the war in Ukraine is especially important because it links this problem directly to Russia- and Belarus-related exposure. The statement

[1] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[2] Ibid.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] Ibid.
[5] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.

emphasises that achieving compliance with the EU's financial sanctions regime should not lead to the financial exclusion of legitimate and potentially vulnerable customers, including customers with links to Russia or Belarus who are legally resident in the EU. It also states that compliance should not hamper efforts by EU organisations, including non-governmental organisations, to provide humanitarian relief in those areas. This is one of the clearest institutional acknowledgements that sanctions implementation can overshoot in practice. It also broadens the problem beyond banking inconvenience. Financial exclusion affects participation in ordinary economic and social life, while obstacles to humanitarian transfers can impair lawful relief efforts. Over-compliance, in other words, is not only a cost issue. It can become a problem of access, inclusion, and humanitarian operability[1,2].

Seen in this light, over-compliance is partly a legal-certainty problem and partly a governance problem. The UK cross-government review of sanctions implementation and enforcement, published in May 2025, records that businesses want simplicity and clarity and that the cost of compliance should be proportionate to the size of the business and its sanctions exposure. The same review states that the government's reforms are intended to make sanctions easier to comply with, including through more user-friendly guidance, clearer and better-structured guidance pages, a single sanctions list, and further clarity on ownership and control. These commitments are analytically revealing. They imply that policymakers recognise a causal link between guidance quality and implementation behaviour. Where law is difficult to navigate, defensive compliance becomes more attractive. Where clarity improves, institutions can manage risk more precisely rather than withdrawing indiscriminately. Over-compliance is therefore not only a private behavioural choice. It is also a signal that the interpretative environment remains more costly or ambiguous than policymakers would like[3,4].

One of the clearest private-law frictions generated by over-compliance is contractual disruption. The Commission's FAQ for small entrepreneurs explains that there is no general prohibition on making payments to Russian legal entities or receiving payments from them in relation to non-prohibited trade, and that competent authorities can help determine whether the relevant goods or services are in fact prohibited. The fact that the Commission needs to issue such clarifications indicates that lawful contractual performance can be interrupted by risk-averse financial or commercial intermediaries even where the underlying contract remains legally permissible. In practical terms, a bank may delay or refuse settlement, a service provider may terminate support, or an intermediary may decline to act, not because the contract is unlawful, but because the compliance burden of proving lawfulness is deemed too high. The friction is therefore not only with sanctions law itself. It is also with the private law of performance, continuity, payment, and reliance. Contracts that survive at the level of formal legality may still become commercially unworkable when defensive compliance enters the payment or service chain[5].

A related friction concerns litigation risk and challenge risk. The UK ownership-and-control call for evidence explicitly asks respondents how the challenges of assessing hypothetical control affect due-diligence burdens, resource allocation, the risk of litigation against their assessment, or inconsistent outcomes. This is a notable official acknowledgment that sanctions compliance can generate private-law and procedural disputes even before a regulator intervenes. A firm that blocks a client, terminates a relationship, freezes performance, or declines to act on the basis of its control assessment may later have to defend that judgement against contractual challenge, reputational dispute, or claims of inconsistency. In such circumstances, defensive withdrawal can itself be both a response to legal risk and a source of legal risk. This is one of the distinctive features of over-compliance in the sanctions field:

[1] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.
[2] European Banking Authority. (2022, April 27). *EBA statement on financial inclusion in the context of the war in Ukraine*.
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

it does not simply move institutions away from risk; it redistributes risk into other legal and commercial channels[1].

The EBA's de-risking opinion also shows that these frictions can reach market structure and system stability. It states that unwarranted de-risking has a detrimental impact on the achievement of EU objectives, particularly with regard to fighting financial crime effectively, promoting financial inclusion, and preserving competition in the single market. It further notes that where a Member State's respondent banks are being de-risked, this can affect the stability of that Member State's financial system. This is analytically significant because it shows that over-compliance is not simply about individual customers being inconvenienced. At scale, de-risking can alter market access, weaken competition, and concentrate financial intermediation in ways that may themselves create fragility. In sanctions policy terms, this means the side-effects of defensive compliance can spill beyond the immediate Russia-related risk and affect the resilience of the coalition's internal market. That is one reason why de-risking is not a peripheral concern. It touches the political economy of sanctions implementation itself[2].

The burden of over-compliance is also distributed unevenly. The UK review states that smaller businesses are less able to access specialist advice and that there is a strong appetite for enhanced outreach, while also stating that businesses want compliance costs proportionate to their size and sanctions exposure. The Commission's June 2025 article on sanctions implementation makes a similar point from the EU side by presenting the EU Sanctions Helpdesk as a tool offering free personalised support particularly to SMEs conducting sanctions due diligence. These institutional responses indicate that implementation burdens fall unevenly across the economy. Large multinational banks and major corporates may absorb ambiguity through dedicated legal and compliance teams. Smaller firms, peripheral sectors, and firms with occasional Russia-related exposure are more likely to respond to complexity by over-withdrawing. Over-compliance thus has a distributive dimension: the less compliance capacity an actor has, the more likely it is to substitute caution for calibrated analysis. That can gradually push lawful but sensitive business away from smaller operators and concentrate it either in larger firms or outside the coalition's mainstream channels altogether[3,4].

Another major driver of over-compliance is the interaction between broad legal concepts and strict or near-strict enforcement environments. The UK call for evidence states that the strict-liability model may have contributed to increased de-risking as industry actors seek to avoid the risk of being found in breach, particularly where it is difficult to determine whether control exists. OFSI's revised 2026 enforcement guidance, meanwhile, emphasises a strengthened enforcement framework and updated penalty processes. Read together, these sources show why defensive compliance can seem rational to firms. Where sanctions enforcement is expected to be more active and the underlying test is difficult to apply with confidence, the private incentive to over-screen, over-block, or over-withdraw grows stronger. This does not mean enforcement is the problem. It means that enforcement intensity must be accompanied by interpretative clarity and workable procedural expectations if it is not to generate avoidable chilling effects for lawful activity[5,6].

A further source of friction is reputational contagion. The EBA's 2022 de-risking opinion identifies situations where ML/TF risks or reputational risks exceed institutions' risk appetite as a key driver of de-risking. The same opinion also notes that institutions may de-risk categories of customers with common characteristics, particularly those linked to higher-risk jurisdictions, irrespective of mitigating factors. This is important for sanctions analysis because many Russia-related over-compliance patterns do not arise from a specific prohibition, but from the reputational contamination of a customer profile, nationality, corridor, or business model. Once "Russia-related" becomes a shorthand proxy for high

[1] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*
[2] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] European Commission. (2025, June 11). *Sanctions implementation*.
[5] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[6] Office of Financial Sanctions Implementation. (2026, February 9). *Financial sanctions enforcement and monetary penalties guidance*.

reputational cost, firms may prefer categorical refusal to differentiated assessment. That creates chilling effects well beyond the targeted sanctions perimeter. It also makes rehabilitation difficult, because even legally clean customers may remain commercially unattractive once they fall inside a stigmatised risk category. In this sense, over-compliance can act as a market amplifier of reputational sanctioning beyond the law itself[1].

This problem is especially acute in fast-moving payment environments. The EBA's 2024 restrictive-measures guidelines record consultation concerns about due-diligence burdens, screening challenges, and operational strain in the context of payments and transfers. Although the final guidelines are framed as supervisory standards, they reflect a real implementation dilemma: where transaction speed is high, data are incomplete, and sanctions exposure is uncertain, firms may treat delay or refusal as the safest operational option. The result can be lawful payments slowed, rejected, or subjected to heavy friction simply because the institution lacks enough time or confidence to clear them. Over-compliance, therefore, is not only a high-level strategic posture. It also appears in micro-operational settings as a bias toward interruption wherever the system cannot comfortably combine speed with reliable sanctions assessment. In practice, this can make legitimate low-risk activity expensive, unpredictable, and commercially unattractive[2,3].

Over-compliance also has a humanitarian and civil-society dimension. The EBA's 2022 Ukraine-related statement expressly says that sanctions compliance should not hamper efforts by EU organisations, including NGOs, to provide humanitarian relief in relevant areas. FATF's 2025 financial-inclusion guidance similarly states that countries and financial institutions should ensure that flows of funds for humanitarian assistance, legitimate NPO activity, and remittances are neither disrupted nor discouraged, and that de-risking entire classes of customers is inconsistent with a proper risk-based approach. These points matter because they reveal how defensive compliance can transform legal permissibility into practical inoperability. A humanitarian or civil-society transfer may remain licensable or lawful in principle, yet banks or counterparties may still decline to process it because the risk-management effort is judged disproportionate. The result is a chilling effect that arises not from sanctions text but from uncertainty about how to navigate the sanctions environment safely. Over-compliance can therefore undermine not only commerce but also channels of lawful relief and social support[4,5].

The private-law effects of over-compliance can also be cumulative rather than singular. A bank may keep the account open but refuse certain payment types. A payment intermediary may process direct transfers but refuse card renewal or acquiring. A professional-services provider may keep the client relationship nominally active while refusing ancillary services. A logistics provider may continue ordinary trade but refuse goods or routes requiring more intensive due diligence. None of these decisions necessarily violates the sanctions regime, but taken together they may erode the practical value of lawful rights and contracts. The Commission's FAQs on payments and accounts show clearly that the law distinguishes between prohibited and non-prohibited services in a granular way. Over-compliance collapses that granularity into a broader zone of market inaccessibility. The friction therefore often accumulates through multiple partial withdrawals rather than one dramatic termination. That cumulative withdrawal can be difficult to challenge because each actor points to its risk policy rather than a legally incorrect interpretation of the sanctions text[6,7].

[1] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] European Banking Authority. (2022, April 27). *EBA statement on financial inclusion in the context of the war in Ukraine*.
[5] Financial Action Task Force. (2025). *Guidance on Anti-Money Laundering, Terrorist Financing Measures and Financial Inclusion*.
[6] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

A further systemic cost is that over-compliance can degrade the coalition's policy credibility. If sanctions are experienced by firms and citizens as unpredictable, excessively burdensome, or broader in market practice than in law, support for long-term maintenance becomes harder to sustain. The UK review recognises this implicitly by linking easier compliance, better guidance, improved reporting channels, and proportionate costs to overall sanctions effectiveness. OFSI's 2025 annual review expresses the same logic even more directly by stating that its core objective is to ensure sanctions are targeted and impactful while enabling businesses to operate with clarity and confidence. This is not a pro-business embellishment. It is an acknowledgment that durable sanctions require implementational legitimacy inside the coalition. Over-compliance erodes that legitimacy when it creates the perception that lawful conduct is too difficult to distinguish from prohibited conduct in practice. Once that perception takes hold, political pressure for carve-outs, retreat, or selective relaxation becomes more likely. Defensive compliance therefore has strategic as well as transactional costs[1].

At the same time, it would be analytically wrong to treat every instance of service withdrawal as unwarranted. Some relationships are indeed too opaque, too costly to understand, or too exposed to justify continuation. The UK call for evidence explicitly states that de-risking can in some circumstances be a prudent response to reduce regulatory risk. The difficulty lies in distinguishing legitimate risk-management refusal from indiscriminate category-level retreat. FATF's case-by-case principle and the EBA's warnings against unwarranted de-risking supply the basic normative standard: institutions should manage risk proportionately at the level of the actual customer and transaction rather than cutting off whole classes of exposure by default. In sanctions practice, this means that a documented refusal based on unresolved beneficial-ownership ambiguity or clear circumvention indicators is not equivalent to a blanket refusal of services to all customers with Russian links. The distinction matters because only the latter represents over-compliance in the strict sense. The aim is not to suppress caution, but to keep caution disciplined and legally anchored[2,3,4].

The most effective mitigant against over-compliance is therefore not weaker sanctions, but better implementation conditions. The UK review's emphasis on clearer and more accessible guidance, a single sanctions list, ownership-and-control clarification, simpler reporting channels, and targeted outreach to less familiar sectors points in exactly this direction. OFSI's annual review similarly highlights clear communications, targeted guidance, responsive licensing, and sector-specific support as part of its compliance strategy. On the EU side, the Commission's helpdesk and FAQ architecture serve the same broad function. These are not merely communications improvements. They are anti-over-compliance measures insofar as they lower uncertainty, reduce private guesswork, and make lawful distinctions more operationally usable. The more predictable the guidance environment becomes, the less attractive indiscriminate withdrawal should be. In this sense, reducing unwarranted de-risking is itself part of strengthening sanctions effectiveness[5,6,7].

Table 7.3.3-1. Forms, Drivers, and Effects of Over-Compliance in the Sanctions Compliance Chain

Form of Over-Compliance	Immediate Driver	Typical Manifestation	Main Downstream Effect
Wholesale de-risking of customer categories	Legal uncertainty, reputational fear, weak sectoral expertise	Refusal to onboard or maintain relationships with broad customer groups	Financial exclusion, loss of competition, migration to weaker channels

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*; Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*
[2] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[3] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.
[4] Financial Action Task Force. (2025). *Guidance on Anti-Money Laundering, Terrorist Financing Measures and Financial Inclusion*.
[5] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[6] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[7] European Commission. (2025, June 11). *Sanctions implementation*.

Form of Over-Compliance	Immediate Driver	Typical Manifestation	Main Downstream Effect
Nationality- or geography-based service withdrawal beyond legal requirements	Misreading of Russia-linked restrictions, fear of error	Freezing or restricting accounts, refusing payments, blocking ordinary account use	Equal-treatment concerns, lawful activity impeded, reputational and contractual disputes
Defensive refusal of lawful payments or contract performance	Ambiguous control tests, complex due diligence burden, slow escalation routes	Non-processing of otherwise lawful payments, settlement delays, abrupt service termination	Contractual disruption, working-capital strain, reduced trust in sanctions governance
Overuse of screening-based interruption	Alert overload, insufficient calibration, low confidence in clearing alerts	Excessive transaction holds, repeated false positives, conservative release policies	Operational friction, customer dissatisfaction, reduced payment-system usability
Humanitarian or civil-society de-risking	Fear of sanctions complexity in high-risk corridors	Refusal to process permissible transfers or reluctance to service NGOs	Chilling effects on relief, remittances, and lawful support channels
Sectoral withdrawal by smaller or less specialised firms	Unequal access to expert advice, disproportionate compliance cost	Exit from higher-friction but lawful business lines	Uneven burden distribution and concentration of compliance-intensive activity

Authorship: prepared by the author on the basis of official EU institutional materials and UK official documents
Sources:

- European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.
- European Banking Authority. (2022, April 27). *EBA statement on financial inclusion in the context of the war in Ukraine*.
- European Commission. (2025, June 11). *Sanctions implementation*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
- Financial Action Task Force. (2025). *Guidance on Anti-Money Laundering, Terrorist Financing Measures and Financial Inclusion*.
- HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
- HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
- Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.

The main conclusion is therefore clear. Over-compliance, de-risking, and the resulting private-law frictions are not accidental side notes to the sanctions' regime. They are structural by-products of a compliance environment in which broad legal concepts, strict enforcement incentives, uneven sectoral expertise, and limited interpretative confidence interact. The risk is not that firms become too cautious in the abstract. The risk is that they begin to substitute categorical withdrawal for the risk-based, evidence-sensitive management that sanctions law actually presupposes. When that happens, lawful payments, lawful contracts, legitimate customers, and even humanitarian channels may be impeded without a direct legal requirement to do so. The result is a distortion of targeting, an uneven distribution of burdens, and a reduction in the operational legitimacy of the regime. A durable sanctions architecture therefore needs to control not only evasion and under-compliance, but also unwarranted over-compliance. For the Russia-related track, that means clearer guidance, better ownership-and-control usability, stronger sector-specific support, and more predictable escalation and reporting

environments. These are not softening devices. They are conditions for keeping compliance both rigorous and proportionate over time[1,2,3,4].

7.3.4. Enforcement Coordination and the Limits of Detection Capacity

Enforcement coordination is the stage at which sanctions policy moves from formal obligation and private-sector vigilance into actual public follow-up, investigation, disruption, and punishment. It is also the stage at which the practical limits of the entire compliance architecture become most visible. A sanctions regime may generate lists, guidance, due-diligence expectations, and reporting channels, but none of those instruments is self-executing once a possible breach or circumvention pattern is identified. Detection must still be translated into an institutional response. That response usually requires multiple authorities, multiple jurisdictions, and multiple bodies of law to interact in a time-sensitive and evidence-sensitive manner. In the Russia-related environment, this challenge is intensified by the cumulative nature of the sanctions' regime, the scale of circumvention efforts, and the cross-border distribution of goods, payments, ownership structures, and service providers. The European Commission's materials repeatedly emphasise that effective and diligent implementation of sanctions is key to preventing circumvention and that this remains primarily the responsibility of Member States. The practical implication is clear. The EU can legislate, coordinate, and guide, but the decisive enforcement burden still sits in a nationally implemented and operationally uneven field. That makes coordination capacity, rather than legal design alone, one of the decisive constraints on overall sanctions effectiveness[5,6,7].

A first structural limit is the distribution of enforcement authority across the Member States. The European Parliament's 2023 study states that the decentralised nature of sanctions enforcement has produced a mosaic of implementation and enforcement practices across the Union and that more than 160 designated competent authorities existed across Member States. It also notes that national systems differ markedly in their organisation, degree of centralisation, and institutional mandates, including those concerning authorisations and engagement with private actors. This is not a merely descriptive point. It means that when a suspicious pattern is detected, the path from signal to action depends heavily on where in the Union the case lands and which authorities are expected to take the lead. Some systems may be relatively centralised and co-ordinated, while others may disperse responsibility across finance ministries, customs services, licensing offices, prosecutors, FIUs, and supervisory authorities. Such variety is manageable in low-friction areas of regulation, but it becomes a serious operational constraint in sanctions enforcement, where timing, role clarity, and cross-border consistency often matter greatly. The problem is not that every Member State has a different legal tradition. The problem is that the adversary benefits from those differences whenever they slow or fragment the enforcement response[8,9].

A second limit lies in the simple fact that Member States remain unevenly equipped to investigate and monitor sanctions cases proactively. The European Parliament study reports that, in some jurisdictions, the relevant authorities operate with relatively small dedicated teams and that documentation and reporting requirements have increased significantly as sanctions packages multiplied. It also records that many national systems had only limited capacities for proactive monitoring of individuals, financial

[1] European Banking Authority. (2022, January 5). *Opinion of the European Banking Authority on 'de-risking'*.
[2] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[5] European Commission. (2025, October 23). *Making sanctions effective*.
[6] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[7] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[8] Ibid.
[9] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.

institutions, and economic operators in order to pre-empt possible violations. This matters because sanctions enforcement is not merely about acting once a violation is obvious. It also involves identifying hidden nexus, testing suspicious patterns, following up on weak signals, and converting fragmented information into a structured case. Small teams and reactive systems struggle to do this consistently, especially when they must simultaneously answer guidance queries, process authorisations, maintain stakeholder communication, and handle enforcement-related co-ordination. Resource scarcity therefore shifts the system toward reactive dependence on private reporting rather than active public detection. That is a major limit in a sanctions environment where sophisticated evasion often appears first as a pattern rather than as a completed overt offence[1].

The third limit concerns the shift from administrative implementation to criminal enforcement. The EU's 2024 directive on criminal offences and penalties for the violation of Union restrictive measures sets minimum EU-wide rules for defining criminal offences and penalties for violations and circumvention of EU restrictive measures. The Commission's "making sanctions effective" page explains that, since entering into force in May 2024, the new rules are intended to make it easier to investigate, prosecute, and punish the violation of these measures across all Member States. This is a significant institutional advance, because sanctions enforcement had long been characterised by highly uneven national criminalisation frameworks. Yet the very need for such harmonisation reveals the prior enforcement weakness. Without common minimum rules, the same conduct could trigger very different legal consequences depending on jurisdiction. More importantly, harmonised rules do not automatically create harmonised investigative or prosecutorial capacity. Criminalisation may provide a stronger legal basis for action, but it does not solve evidence-gathering bottlenecks, staff shortages, or divergent case-prioritisation cultures. The directive strengthens the formal enforcement perimeter, but the practical capacity to use it remains a separate question[2].

The persistence of transposition problems confirms that legal harmonisation alone does not guarantee operational readiness. In July 2025, the European Commission opened infringement procedures by sending letters of formal notice to several Member States for failing to fully transpose the directive on criminal offences and penalties for the violation of Union restrictive measures. This is a highly consequential development for the present subsection because it shows that even after the Union establishes minimum rules, actual enforcement convergence remains vulnerable to delays in domestic implementation. If transposition is incomplete or uneven, investigators and prosecutors continue to operate under divergent domestic frameworks, and cross-border cases remain harder to align procedurally. The issue is not only whether the rule exists. It is whether it is in force, usable, and linked to national criminal and procedural law in a timely manner. Detection capacity is weakened when follow-up powers vary across jurisdictions or when authorities do not yet share a common baseline on what counts as a criminal sanctions' offence. Enforcement coordination is therefore constrained not only by institutional complexity, but by legislative latency inside that institutional complexity[3,4].

A fourth limit is evidential. Sanctions cases often require proof not only that a prohibited act occurred, but that it occurred with the relevant nexus, knowledge, ownership, control, destination, or indirect benefit. This is especially difficult where circumvention has been designed to fragment the transaction into multiple jurisdictions and actors. Eurojust's earlier comparative report on the prosecution of sanctions violations is useful precisely because it treats sanctions cases as part of a broader judicial-cooperation challenge and highlights the importance of national inter-authority and international co-operation for prosecuting such violations. That insight has not become less relevant with time. On the contrary, the Russia sanctions environment has made it more acute. A direct shipment or direct payment is easier to prove than a layered deal involving a third-country intermediary, altered beneficial ownership,

[1] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*
[2] EUR-Lex. (2024). *Criminal offences and penalties for the violation of EU restrictive measures*; European Commission. (2025, October 23). *Making sanctions effective*
[3] European Commission. (2025, July 23). *Commission takes action to ensure complete and timely transposition of directives*.
[4] European Commission. (2026, March 20). *March infringements package: key decisions*.

a freight forwarder acting as nominal end user, and parallel payment arrangements. The more circumvention relies on fragmented service provision, the more evidence must be assembled across the seams of the transaction. Detection capacity is therefore limited not only by whether a signal exists, but by whether it can be converted into evidentially durable proof[1,2].

Cross-border evidence exchange is therefore one of the central enforcement bottlenecks. Eurojust's general role in facilitating co-operation between national prosecutors is relevant here, but the key analytical point is broader: sanctions cases often require evidence from customs records, payment data, ownership registers, shipping records, beneficial-owner information, company filings, and private compliance documentation held in multiple jurisdictions. FATF's 2025 report identifies uneven implementation of data-privacy provisions, regulatory restrictions, confidentiality concerns, inconsistent data formats, delays in disseminating intelligence, and resource constraints as barriers to effective information sharing. These are not abstract technical issues. They shape whether a suspicious transaction can be reconstructed before its evidential value decays or before related actors shift assets again. When authorities cannot exchange relevant information quickly and in usable form, detection remains shallow and follow-up becomes patchy. Cross-border cases then tend to favour the evasive actor, because that actor has already designed the scheme to exploit institutional fragmentation. Enforcement coordination is therefore limited not only by legal competence, but by the speed, interoperability, and admissibility of the information that flows between competent bodies[3,4].

A fifth limit lies in customs detection capacity. Customs authorities are central to enforcement of trade restrictions, but customs control operates under high-volume conditions in which individual examination of every consignment is impossible. The Commission's customs action plan explains that risk management is pivotal to customs controls precisely because customs authorities cannot always examine goods on an individual basis and must facilitate legitimate trade while performing enforcement functions. The Commission's dedicated Ukraine-related customs page further reflects the importance of stopped-goods guidance and other sanctions-related customs tools. These materials together underline a basic operational reality: customs enforcement is inherently selective and intelligence-led. That makes it vulnerable to evasive strategies that exploit volume, routings, low-value fragmentation, or documentation that is formally complete but strategically misleading. Detection capacity at the border is therefore bounded by throughput realities as much as by legal authority. This is why customs intelligence, risk profiling, and targeted co-operation with other authorities are indispensable rather than optional enhancements[5,6].

The constraints on customs become even clearer in cases involving blocked or "stopped" goods. The Commission's 2023 guidance note to Member States on stopped goods as a result of sanctions states that the new Article 12e was introduced to provide legal certainty concerning the treatment of goods that become blocked by import prohibitions and to protect legitimate interests of EU importers. Although the measure is framed as a legal-certainty tool, it also reveals a deeper enforcement tension. Customs authorities are not merely detecting prohibited imports or exports; they are also expected to decide what to do with goods once they have been stopped and whether release would create circumvention risk. This moves customs from a simple control point into a risk-adjudication role. The more often such cases arise, the more pressure there is on customs expertise, inter-authority consultation, and case-by-case decision-making. Detection does not end at interception. It must continue into assessment of whether a stopped case can be resolved lawfully without reintroducing evasion risk[7,8].

---

[1] Eurojust. (2021). *Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis*.
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] Ibid.
[4] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[5] European Commission, Directorate-General for Taxation and Customs Union. (2020, September 28). *Customs Action Plan*.
[6] European Commission, Directorate-General for Taxation and Customs Union. (n.d.). *EU measures following the Russian invasion of Ukraine*.
[7] European Commission. (2023, September 4). *Guidance note to Member States on stopped goods as a result of the sanctions*.
[8] European Commission, Directorate-General for Taxation and Customs Union. (n.d.). *EU measures following the Russian invasion of Ukraine*.

A sixth limit concerns prioritisation. Neither public authorities nor private institutions can investigate everything with equal intensity, so enforcement inevitably depends on choices about what matters most. The Commission's 2025 article on the 16th package emphasises that new measures are also aimed at tackling circumvention, while repeated Commission communications on common high priority items and circumvention indicate a deliberate concentration on the goods and channels most relevant to Russia's military-industrial base. This prioritisation is strategically rational, but it also generates blind spots. High-priority targeting means that lower-profile goods, secondary service providers, or less visible value channels may receive less scrutiny. Likewise, customs, prosecutors, and supervisors may prioritise large or politically salient cases while more granular but cumulatively important violations remain under-enforced. Prioritisation is unavoidable, but it is still a limit. Every prioritisation model implies a corresponding non-prioritisation zone that more adaptive actors may try to exploit[1,2].

Supervisory prioritisation in the financial sector creates a similar challenge. The EBA's restrictive-measures guidelines are designed to help competent authorities assess institutions' internal controls and screening systems, but supervisory attention remains finite. A system under which authorities must identify the riskiest firms, the weakest controls, and the most serious alert-management failures will necessarily operate through selective focus. That focus can improve overall effectiveness, yet it can also create predictable enforcement patterns. Firms may anticipate where supervisors are likely to look and where they are less likely to look. Moreover, supervisory assessments often concentrate on governance quality rather than on every individual suspicious case. This is institutionally sensible, but it means that some forms of operational failure may only be detected if they surface through reporting, whistleblowing, or major incident review. Detection capacity is therefore limited not just by resources, but by the need to triage scarce supervisory attention toward the cases and institutions believed to matter most[3,4].

The weakness of follow-up consistency is another important constraint. The Council's Best Practices recommend that competent authorities notify one another and the Commission of rejected authorisation requests, even where not legally required, in order to minimise internal-market distortions. That recommendation is valuable precisely because it recognises that follow-up can otherwise remain uneven. One authority may detect and refuse a high-risk pattern, while another may remain unaware and permit a materially similar application. Similar inconsistency can arise with freezing measures, reporting follow-up, customs interventions, or decisions on whether a case is serious enough for criminal investigation. The issue is not only fairness. It is predictability and deterrence. If like cases produce divergent enforcement responses across the Union, evasive actors gain opportunities to re-route through the softest or slowest point. Follow-up consistency is therefore a substantive enforcement asset, not simply an administrative virtue. Its absence dilutes the pressure effect of the regime even when the legal rules themselves are identical[5,6].

The sanctions chain is also limited by the relationship between reporting and action. Authorities need reporting from financial institutions, exporters, freight actors, and whistleblowers, but too much undifferentiated reporting can overwhelm analytical capacity, while too little feedback to reporters weakens future detection quality. FATF's 2025 report states that private-sector entities reported a lack of public-sector feedback on relevant SARs and STRs. The EBA's 2024 consultation record on restrictive-measures guidelines similarly captures concern that overbroad reporting expectations could flood competent authorities with incomplete or low-value information. These sources reveal a recurring problem of enforcement design. Detection capacity is not simply increased by generating more alerts or

[1] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] European Commission. (2024, April 24). *Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)*.
[5] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[6] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.

more reports. It is increased when reports are sufficiently specific, prioritised, and connected to response mechanisms that allow authorities and firms to learn from outcomes. Without that feedback loop, the system tends to oscillate between overload and passivity. Both states weaken enforcement in different ways[1,2].

A seventh limit is that sanctions enforcement must increasingly compete with the speed and adaptability of modern financial and commercial infrastructures. OFAC's instant-payment guidance, although U.S.-based, is useful because it highlights a general problem: payment rails can now operate in real time or near real time, while sanctions analysis still often requires pause, inquiry, and exception processing. In the EU context, this concern is echoed in EBA discussions around screening transfers of funds and crypto-assets, including the need for systems to interrupt execution where a possible match or circumvention concern arises. This mismatch matters for detection capacity. The faster the transaction environment becomes, the less tolerance there is for slow manual review and the more likely that either true positives are missed or lawful transfers are over-blocked. Enforcement co-ordination is then not just an inter-agency problem. It becomes a problem of whether public and private systems can slow, query, and preserve high-risk activity without paralysing the legitimate infrastructure on which the wider economy relies[3,4].

The role of Europol illustrates both the strengths and limits of EU-level operational support. Europol's European Financial and Economic Crime Centre exists to enhance operational and strategic support in preventing and combating financial and economic crime in the Union. Europol's programming documents also state that the agency contributes to the work of the Commission's Freeze and Seize Task Force and supports Member State investigations with expertise, including on virtual assets. This matters because sanctions evasion increasingly intersects with financial crime, money laundering, and crypto-enabled concealment. Yet Europol's role is one of support and co-ordination, not direct prosecution or direct national enforcement authority. Europol can improve intelligence fusion, analysis, and cross-border operational support, but it does not remove the need for Member States to act, investigate, and prosecute. The agency therefore helps thicken the enforcement network, but it does not dissolve the underlying dependence on national capacities and political will[5].

A similar observation applies to the Commission's Freeze and Seize Task Force. Commission materials describe the Task Force as a mechanism to strengthen co-ordination at operational level to ensure effective enforcement of EU sanctions across all Member States, particularly with regard to asset freezes and links between listed persons' assets and criminal activity. The 2025–2026 materials also indicate that the Task Force remains active, with multiple meetings continuing after the entry into force of the criminalisation directive. This confirms that the Union recognises enforcement co-ordination as an ongoing rather than a settled problem. At the same time, the very persistence of the Task Force signals that coordination needs active maintenance. If enforcement were straightforwardly harmonised and self-sustaining, such an operational task force would be less central. The Task Force should therefore be seen as both a strength and a symptom: a strength because it creates a co-ordination forum, and a symptom because it reflects how much ongoing effort is required to keep national enforcement sufficiently aligned[6,7].

Judicial co-operation presents its specific limits. Eurojust's work on sanctions violations and broader cross-border prosecution co-operation demonstrates the importance of common prosecutorial

[1] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[2] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[3] Ibid.
[4] U.S. Department of the Treasury, Office of Foreign Assets Control. (2022, September). *Sanctions Compliance Guidance for Instant Payment Systems*.
[5] Europol. (n.d.). *European Financial and Economic Crime Centre (EFECC)*; Europol. (2023, November 28). *Europol Programming Document 2024–2026*.
[6] European Commission. (2025, October 23). *Sanctions against individuals, companies and organisations*.
[7] European Commission. (2025, October 23). *Holding Russia accountable*; European Commission. (2025, October 23). *Making sanctions effective*.

understanding, evidence exchange, and co-ordination among national authorities. Yet sanctions cases can still face procedural asymmetries, different evidentiary standards, and different levels of prosecutorial experience across Member States. In October 2025, the Consultative Forum of Prosecutors General discussed sanctions enforcement explicitly, with participants stressing that rigorous enforcement of sanctions requires unity among prosecutorial authorities. The very need to make that point publicly indicates that the judicial dimension of sanctions enforcement remains in development rather than fully stabilised. Cross-border prosecutorial co-ordination can support sanctions cases, but it does not eliminate divergence in domestic priorities, legal cultures, or resource allocation. Detection capacity thus remains partly dependent on whether national prosecutors view sanctions cases as sufficiently strategic to pursue with the same intensity as other forms of economic or organised crime[1,2].

Another enforcement limit lies in the relationship between asset freezing and confiscation. Commission materials on solidarity with Ukraine note that Member States have immobilised over €28 billion in assets belonging to Russian and Belarusian listed persons and that the Union has moved to strengthen both asset recovery and the criminalisation of sanctions violations. This is important, but it also reveals a familiar asymmetry. Freezing is easier to achieve than confiscation, and immobilisation does not by itself resolve longer-term evidentiary and procedural challenges associated with proving criminality, tracing beneficial ownership, or moving from temporary restraint to durable legal consequences. The more sanctions enforcement relies on keeping assets frozen over time, the more important it becomes to sustain accurate records, clear ownership analysis, and admissible evidence. Detection capacity is therefore constrained not only at the moment of finding an asset, but over the much longer horizon of maintaining, litigating, and potentially converting that restraint into confiscation or other enforceable outcomes[3,4].

Partner-jurisdiction coordination is another area where both progress and limits are evident. Commission and Council materials highlight the role of the EU Sanctions Envoy and diplomatic outreach to third countries in preventing circumvention, while sanctions packages repeatedly note continued engagement with key third countries and “like-minded partners” to counter re-exports and related evasion. The Commission’s broader Ukraine timeline and sanctions pages also link EU efforts to the REPO framework and other forms of co-operation with G7 partners and Australia. This matters because many Russia-related circumvention schemes rely on jurisdictions outside the EU. Detection capacity inside the Union will remain incomplete if authorities cannot obtain co-operation, trade-monitoring support, or customs vigilance from relevant third countries. Yet diplomacy is not the same as enforcement authority. Outreach can encourage monitoring, controlling, and blocking of suspicious re-exports, but it cannot guarantee equivalent legal commitment or equivalent capacity abroad. Partner coordination is therefore necessary, but it remains structurally softer than domestic enforcement. That softness creates an enduring limit in a regime that increasingly depends on constraining re-routing through non-EU channels[5,6,7].

At the same time, the EU has begun to expand some of its information-sharing architecture in ways that may improve enforcement capacity over time. The Commission’s page on the Directive on Administrative Cooperation states that, as of 1 January 2026, DAC can also be used to combat money laundering and to enforce sanctions in the EU. This is a technically important development because it extends an existing administrative-cooperation framework into the sanctions field. In practical terms, better access to tax and related administrative data may support tracing, ownership reconstruction, and follow-up on suspicious economic activity. Yet the fact that such a step is only now becoming available

[1] Eurojust. (2021). *Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis*.
[2] Eurojust. (2025, October 3). *EU Prosecutors General discuss organised crime and judicial cooperation*.
[3] European Commission. (2025, October 23). *Holding Russia accountable*.
[4] European Commission. (n.d.). *Solidarity with Ukraine*.
[5] Ibid.
[6] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia*.
[7] European Commission. (2025, October 23). *Making sanctions effective*.

also underscores the previous limitations of information sharing. Enforcement capacity improves when authorities can mobilise multiple data regimes, but such integration tends to arrive later than the circumvention patterns it is meant to address. This again illustrates a recurring dynamic in sanctions enforcement: institutional adaptation often lags behind evasive adaptation, even when the direction of reform is sound[1].

The private sector's role in detection also imposes a limit of its own. Compliance systems can produce alerts, reports, freezes, and escalations, but public authorities still have to decide which signals merit a full response. If authority-side follow-up is slow, inconsistent, or non-transparent, the quality of private detection may decline over time because institutions cannot distinguish which kinds of signals are truly useful. FATF's 2025 report identifies lack of feedback from authorities as a problem raised by private-sector entities, while OFSI's threat-assessment initiative reflects an attempt to support firms through more explicit public risk communication. These developments point in opposite directions: one describes a weakness, the other an attempted correction. The broader implication is that detection capacity is co-produced. It depends on a stable feedback loop between private reporters and public responders. Without that loop, institutions either over-report, under-report, or resort to defensive over-compliance. None of those outcomes is ideal from an enforcement perspective[2,3].

The practical limit of detection capacity can therefore be summarised as a tension between scale and granularity. The sanctions regime against Russia covers thousands of listed persons and entities, multiple packages, multiple service sectors, numerous product categories, and a continuously adapting circumvention environment. Enforcement bodies must cope with this scale while still generating case-specific, evidentially defensible, and timely interventions. That is inherently difficult. The more the system scales up, the more it must rely on prioritisation, selective intelligence, and private-sector pre-filtering. Yet the more it relies on those mechanisms, the greater the risk that lower-visibility evasion or inconsistently handled cases slip through. Detection capacity is therefore never absolute. It is a contested balance between coverage, speed, detail, and proof. The question for sanctions policy is not whether all breaches can be detected. It is whether the system can detect enough of the right breaches, fast enough and credibly enough, to preserve deterrence and reduce the payoff from circumvention[4,5,6].

Table 7.3.4-1. Enforcement Coordination Bottlenecks and Detection-Capacity Limits

Bottleneck	Where It Appears in the Chain	Core Operational Problem	Strategic Effect on Sanctions Enforcement
Decentralised Member State architecture	NCA, customs, supervisory, prosecutorial stages	Different mandates, structures, and case-handling models across jurisdictions	Produces uneven follow-up and encourages forum-shopping or re-routing
Limited staffing and proactive capacity	National implementation and investigation stage	Small teams and reactive systems struggle to move from signal to case	Reduces proactive detection and increases dependence on private reporting
Delayed or uneven criminalisation/transposition	Criminal investigation and prosecution stage	Common EU rules exist, but domestic implementation may lag or diverge	Weakens convergence in prosecution and penalty risk
Cross-border evidence and data-sharing frictions	FIU, customs, prosecutorial, and judicial co-operation stage	Confidentiality, legal restrictions, incompatible formats, and delays hinder case-building	Makes networked circumvention harder to prove and slower to disrupt

[1] European Commission, Directorate-General for Taxation and Customs Union. (n.d.). *Directive on administrative cooperation (DAC)*
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance.*
[4] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[5] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes.*
[6] European Commission. (2025, October 23). *Making sanctions effective.*

Bottleneck	Where It Appears in the Chain	Core Operational Problem	Strategic Effect on Sanctions Enforcement
Customs throughput and selective control	Border and trade-control stage	Customs cannot examine all consignments individually and must rely on risk management	Allows volume, routing, and document-based evasion to exploit screening limits
Supervisory prioritisation constraints	Financial-sector monitoring stage	Authorities must triage limited attention across many firms and risk vectors	Some weak controls or smaller-scale breaches remain under-scrutinised
Inconsistent follow-up across authorities	Authorisation, reporting, and enforcement stages	Similar cases may generate different responses in different Member States	Dilutes deterrence and weakens predictability
Weak feedback loops to reporting entities	Public–private interface	Firms receive limited information on which alerts or reports proved useful	Reduces the learning quality of private detection over time
Dependence on third-country cooperation	Anti-circumvention and re-export stage	Diplomatic outreach cannot fully substitute for foreign enforcement powers	Leaves extra-EU diversion corridors harder to police
Asset-freeze-to-confiscation gap	Asset-enforcement stage	Freezing is easier than evidentially durable confiscation or prosecution	Extends enforcement timelines and strains institutional resources

Authorship: prepared by the author on the basis of official EU institutional materials and documents
Sources:

- European Commission. (2025, October 23). *Making sanctions effective*.
- European Commission. (2025, October 23). *Sanctions against individuals, companies and organisations*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- Europol. (2023, November 28). *Europol Programming Document 2024–2026*.
- Eurojust. (2021). *Prosecution of sanctions (restrictive measures) violations in national jurisdictions: a comparative analysis*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
- European Commission, Directorate-General for Taxation and Customs Union. (2020, September 28). *Customs Action Plan*.
- European Commission, Directorate-General for Taxation and Customs Union. (n.d.). *Directive on administrative cooperation (DAC)*.

The main conclusion is therefore clear. Enforcement coordination remains one of the decisive bottlenecks in the sanctions regime because detection is not merely a matter of recognising risk. It is a matter of converting risk signals into coherent, timely, and evidentially sustainable institutional action. In the Russia-related environment, that conversion is constrained by decentralised authority structures, limited staffing, uneven criminalisation and transposition, customs volume realities, supervisory triage, weak feedback loops, and dependence on third-country cooperation. EU-level mechanisms such as the Freeze and Seize Task Force, the criminalisation directive, the Sanctions Envoy's outreach, Europol support, and expanding data-sharing tools all strengthen the architecture. But they do not eliminate the fact that sanctions enforcement still operates through a chain whose weakest links remain national, cross-border, and capacity-bound. For Part Seven, the analytical implication is decisive: the effectiveness of sanctions does not depend only on how much is prohibited or how many red flags are known. It also depends on whether the coalition can organise enough co-ordination, evidence, and

follow-up to make circumvention materially more difficult than compliance. Where that organisational threshold is not met consistently, detection capacity becomes the limiting factor of the regime itself[1,2,3,4].

7.4. Compliance Outlook (2026–2030)

7.4.1. Strategic Functions to Preserve in the Compliance Track

The compliance outlook for 2026–2030 should not be framed primarily in terms of whether the Union adds more guidance documents, more lists, or more supervisory expectations. The more important question is which strategic functions the compliance track must preserve if the sanctions regime is to remain operationally effective under conditions of prolonged confrontation and adaptive circumvention. By this stage, the EU sanctions architecture against Russia is no longer a short-cycle emergency regime. It is a cumulative, cross-sectoral, and administratively dense system that must continue to function across finance, trade, logistics, insurance, customs, and professional services. In such a setting, preservation matters as much as innovation. A compliance architecture may formally expand while functionally degrading if it loses speed, legibility, or coherence. The official materials already point in the opposite direction: the Commission stresses effective implementation, the EBA has introduced common EU standards for restrictive-measures governance, and partner jurisdictions increasingly present compliance as a strategic rather than merely technical field. The outlook for 2026–2030 should therefore be organised around the core functions without which the regime would become slower, less predictable, and more porous. Those functions include predictability, update speed, anti-circumvention responsiveness, private-sector usability, legal defensibility, and cross-border interoperability. Preserving them is not a secondary administrative task; it is part of preserving the coercive value of the sanctions' regime itself[5,6,7].

The first strategic function that must be preserved is predictability. A sanctions regime can remain politically forceful only if economic operators, supervisors, and national authorities can determine with sufficient confidence what is prohibited, what is licensable, and what level of due diligence is expected in a given case. The Commission's sanctions-resources architecture, its consolidated FAQs, and the daily-updated legal access provided through EUR-Lex all reflect the same institutional premise: compliance depends on law being operationally legible. The Commission's "making sanctions effective" page also notes that it has published hundreds of FAQs across the sectors affected by sanctions and continues to work together with national competent authorities that implement EU sanctions, grant authorisations, and prosecute violations. These measures would not be necessary if predictability were self-generating from the regulations alone. Their existence shows that predictability is a strategic function that requires active maintenance. Looking ahead to 2026–2030, this function must be preserved not only in the sense of continuing to publish guidance, but in the more demanding sense of keeping the guidance hierarchy coherent and usable. If predictability weakens, both over-compliance and under-compliance will rise, and the coalition's implementation costs will increase. In a prolonged

[1] Ibid.
[2] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[5] European Commission. (2025, October 23). *Making sanctions effective*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[7] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.

sanctions regime, predictability is therefore not the enemy of pressure. It is one of the conditions under which pressure remains governable[1,2,3].

Closely related to predictability is the second strategic function: operational accessibility of sanctions information. It is not enough for the law to exist and be correctly drafted; firms must also be able to find, understand, and apply the relevant information within real compliance timeframes. The Commission's sanctions-resources page highlights the consolidated list, the sanctions map, the whistleblower tool, EUR-Lex, and the Helpdesk as part of the usable interface of the sanctions' regime. These are not peripheral convenience tools. They are part of the architecture that lowers search costs, improves comparability of information, and reduces the risk that compliance decisions are based on stale or partial legal sources. The Helpdesk model is particularly important because it extends usability beyond large institutions with deep in-house expertise. The June 2025 Commission article explains that the Support Service provides free personalised help to companies conducting sanctions due diligence and that it can respond to questions on counterparties, goods or services, jurisdictions, and end-use issues within two working days. For the 2026–2030 period, preserving compliance usability will be essential because cumulative package growth can easily outpace the interpretative capacity of ordinary operators. A sanctions regime that remains legally valid but practically hard to navigate will become more unevenly implemented over time. Usability is therefore one of the core strategic functions that preserves both reach and fairness in the compliance track[4,5].

A third strategic function that must be preserved is update speed. The sanctions regime against Russia has already shown that the compliance architecture cannot remain static while evasion techniques, sectoral targets, and package scope continue to evolve. The Commission's 16th, 17th, and 19th package communications demonstrate precisely this pattern. In February 2025, the 16th package introduced additional vessel listings and a new listing criterion targeting support for unsafe oil tankers. In May 2025, the 17th package added 189 additional shadow-fleet vessels and expanded the total to 342, linking this directly to reduced Russian ability to evade the oil price cap. By October 2025, the 19th package extended pressure into further sectors and added new transaction bans and payment-system restrictions. These examples matter not only as substantive package developments, but as indicators of the tempo that the compliance system is expected to absorb. The strategic function to preserve here is not package proliferation as such. It is the ability of the compliance track to digest, transmit, and operationalise new measures quickly enough that legal adoption does not outrun market implementation. A slow compliance update cycle would create exactly the lag that adaptive actors need[6,7,8].

This update-speed function is not simply about formal legal acts. It also concerns how quickly guidance, lists, and compliance expectations are revised after those acts are adopted. The Commission's sanctions-resources page notes that the consolidated financial sanctions list is updated whenever necessary and reflects officially adopted texts, while EUR-Lex provides daily updates to legal documents. The OFSI annual review makes the same point from partner practice, emphasising that updated guidance and FAQs enabled businesses to adapt their compliance programmes swiftly and confidently to new regulations. It also highlights the combined e-alert service, which by April 2025 had reached over 56,000 subscribers and provided direct access to critical updates, guidance, and licensing information. This is strategically significant because it shows that update speed must be preserved not only at the level of public decision-making, but at the level of operator notification and implementation. A sanctions regime that updates law quickly but disseminates operational consequences slowly

[1] European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] European Commission. (2025, June 11). *Sanctions implementation*.
[5] European Commission. (n.d.). *Overview of sanctions and related resources*.
[6] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[7] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia*.
[8] European Commission. (2025, October 23). *EU adopts 19th package of sanctions against Russia*.

becomes more vulnerable, not less. For the 2026–2030 outlook, timely diffusion of changes must remain a preserved function of the compliance track if the Union wants to prevent implementation lag from becoming a structural weakness[1,2].

A fourth strategic function is anti-circumvention responsiveness. By 2026–2030, the central challenge is not merely preserving the letter of sanctions restrictions, but preserving the system's ability to adapt when prohibited access is reconstructed through third-country intermediaries, shadow-fleet networks, ownership engineering, or fragmented service provision. The Commission's due-diligence guidance and the dedicated FAQ on enhanced due diligence for operators dealing with common high priority items reflect this logic very clearly. They do not simply restate prohibitions. They identify circumvention risks, promote risk assessment, and connect high-priority goods to targeted anti-circumvention action by customs and partner-country enforcement agencies. The list of Common High Priority Items itself is expressly described as a support tool for due diligence and effective compliance. Preserving anti-circumvention responsiveness therefore means preserving the system's ability to move from static restrictions to dynamic pattern-recognition and targeted follow-up. In outlook terms, this implies that typology-based vigilance must remain central even if the package structure stabilises. If the compliance track loses this adaptive quality, it may remain legally extensive while becoming operationally easier to route around[3,4,5].

The preservation of anti-circumvention responsiveness also requires the system to retain a strong prioritisation function. Not every item, route, or service channel can receive the same compliance intensity, and official sources already show that policymakers understand this. The Commission's CHPI logic, the repeated vessel listings in the 16th and 17th packages, and the integration of shadow-fleet targeting into later packages all point toward prioritised pressure against the most strategically valuable or most frequently abused channels. The strategic function to preserve is therefore selective intensity. Compliance resources must continue to be concentrated where battlefield relevance, circumvention propensity, or revenue significance are highest. This is not a departure from comprehensiveness. It is what makes comprehensiveness administratively workable over time. A regime that loses prioritisation may become overloaded and diffuse its enforcement energy across too many low-impact nodes. For the 2026–2030 compliance outlook, preserving focused pressure on high-priority goods, risky maritime channels, and core financial conduits will remain essential[6,7,8].

A fifth strategic function is private-sector usability. Modern sanctions implementation relies structurally on private actors—banks, insurers, exporters, freight operators, compliance departments, and platform intermediaries. The public side can legislate and co-ordinate, but the daily points of interruption remain overwhelmingly private. This means the system must preserve the practical usability of its compliance obligations for those actors if it is to remain operationally effective. The Commission's Helpdesk article is especially important here because it shows the Union moving beyond generic guidance toward a service model tailored in particular to SMEs. The article explains that firms can submit general sanctions questions or detailed due-diligence requests and receive support on counterparties, goods, jurisdictions, end-use, specific actions, and internal programme design. This is not merely a support measure for smaller firms. It is a strategic compliance function because it helps preserve a wider implementation base. If only large financial institutions and multinational corporates can operate confidently inside the sanctions' regime, the coalition's compliance capacity becomes more

[1] European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] European Commission. (2024, February 19). *Guidance on due diligence*.
[4] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[5] European Commission. (2024, February 22). *List of common high priority items*.
[6] Ibid.
[7] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[8] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia*.

concentrated, more unequal, and more brittle. Preserving usability therefore supports both effectiveness and distributional sustainability[1,2].

Private-sector usability must also remain sector-sensitive. The OFSI annual review reports tailored support across financial services, legal services, cryptoasset, charity, and maritime sectors, while the EBA guidelines distinguish between common standards for financial institutions and specific expectations for PSPs and CASPs handling transfers of funds and crypto-assets. These official approaches matter because they reject the idea that a single generic compliance model is adequate for all sectors. For 2026–2030, preserving private-sector usability will therefore mean preserving the capacity to translate sanctions obligations into sector-specific operational language. Maritime risk, payments risk, export-control risk, and humanitarian-risk handling do not present themselves in identical forms. A strategically durable compliance track must retain the ability to tailor guidance, outreach, and supervisory expectations to the actual transaction environments in which firms operate. Otherwise, the regime will become either too abstract to use well or too blunt to use proportionately[3,4].

A sixth strategic function is legal defensibility. A compliance track that acts quickly but cannot justify its decisions under legal or supervisory review will lose credibility over time. The EBA's 2024 guidelines are important precisely because they transform restrictive-measures compliance into a governance and control discipline. They require clear internal governance, role allocation, risk management, and procedures that institutions and supervisors can assess. Partner-jurisdiction practice reinforces the same logic. The UK government's strategic approach to sanctions enforcement, published in March 2026, explicitly presents the relationship between compliance and enforcement, clarifies roles and responsibilities, outlines enforcement principles, and explains the range of enforcement tools and the mitigating and aggravating factors considered in enforcement decisions. This is more than a deterrence document. It is part of the legal-defensibility function of the compliance track. Firms are better able to act decisively when they understand both the obligations and the consequences, and when enforcement appears principled rather than erratic. Preserving legal defensibility therefore means preserving robust records, structured escalation, and clear relationships between guidance, licensing, reporting, and enforcement consequences[5,6].

Legal defensibility is also what allows the compliance track to preserve proportionality. A regime that cannot distinguish reliably between prohibited, licensable, and permissible conduct will drift toward either over-compliance or under-enforcement. The Commission's FAQs on payment services, its broader consolidated FAQs, and its Russia-related sanctions pages all show that the legal structure remains more differentiated than raw political rhetoric might suggest. This means that preserving a defensible compliance track for 2026–2030 also requires preserving the ability to act with nuance. Compliance should remain strong, but it must also remain legally bounded and reviewable. This is not a softening of the regime. It is a way to prevent the market from creating an uncontrolled second layer of private restrictions that exceeds the law and undermines targeting discipline. A sanctions regime that

[1] European Commission. (2025, June 11). *Sanctions implementation*.
[2] European Commission. (n.d.). *Contacts on EU sanctions*.
[3] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[5] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[6] Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.

becomes unpredictable in private practice will eventually face resistance, litigation, and reduced coalition confidence. Legal defensibility thus feeds directly into long-term durability[1,2,3].

A seventh strategic function is cross-border interoperability. The compliance track cannot remain effective if each Member State, each supervisory authority, and each sector effectively develops its operational dialect of the sanctions regime. The Council's 2024 Best Practices document is particularly important because it expressly states that the paper is under constant review and is intended to identify key elements for the effective implementation of restrictive measures within the EU legal system. The Commission's "making sanctions effective" page then points to a regular expert group meeting on sanctions implementation, the Freeze and Seize Task Force, a high-level group bringing together all 27 Member State authorities with industry and business representatives, and ad hoc stakeholder meetings to discuss implementation. Together, these structures show that cross-border interoperability is already treated as a core function of EU sanctions administration. For 2026–2030, that function must be preserved because the pressure of cumulative packages, criminalisation rules, and anti-circumvention measures will otherwise increase national divergence rather than reduce it. Interoperability is what allows the regime to function as a Union-wide system rather than as a patchwork of parallel national practices[4,5].

The EBA's restrictive-measures guidelines reinforce this same outlook from the supervisory side. The EBA states that, for the first time, it has set common EU standards on governance arrangements and on the policies, procedures, and controls financial institutions should have in place to comply with Union and national restrictive measures. This is strategically important because common standards reduce the risk that institutions operating across borders will face radically different control expectations in different parts of the Union. Preserving this convergence function through 2026–2030 will be crucial. Without it, the increasing complexity of sanctions controls would likely produce more supervisory arbitrage, more uncertainty for cross-border groups, and more room for evasive actors to exploit weaker implementation points. Interoperability in this sense is not only about co-operation between authorities; it is also about keeping supervisory expectations sufficiently aligned that firms can build durable compliance systems at scale[6].

An eighth strategic function is enforcement-linked co-ordination. Compliance and enforcement cannot be treated as separate worlds in the next phase of the regime. The UK's March 2026 strategic approach document explicitly links compliance to enforcement consequences and defines how departments, regulators, and enforcement bodies relate to one another. The May 2025 cross-government review had already focused on improving compliance, increasing deterrence, strengthening the cross-government toolkit, harnessing systemic efficiencies, improving information sharing, and minimising the administrative burden of compliance. These documents matter for the EU outlook not because the UK model is directly transferable, but because they express a principle that applies equally on the Union side: compliance works better when firms understand not only how to comply, but also how enforcement is likely to operate when they do not. For 2026–2030, the strategic function to preserve is therefore the visible and credible relationship between compliance expectations, reporting obligations,

[1] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[2] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[5] European Commission. (2025, October 23). *Making sanctions effective*.
[6] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

enforcement roles, and consequences. If that relationship weakens, compliance drifts either into formality or into defensive over-withdrawal[1,2].

A ninth strategic function is sustained public–private interface quality. The Commission's structures for expert meetings, high-level groups, stakeholder meetings, Helpdesk support, FAQs, and whistleblower tools all indicate that the sanctions regime now depends on continuous interaction with firms and other stakeholders rather than only on unilateral state commands. This function will remain critical through 2026–2030 because the regime increasingly operates through distributed detection and distributed interruption. Private operators are the ones who see payment anomalies, route deviations, documentary inconsistencies, and ownership opacity in real time. Public authorities provide legal authority, cross-border co-ordination, and criminal follow-up. Preserving the quality of this interface means preserving not only channels for reporting and support, but a broader climate in which firms view guidance, escalation, and communication as usable rather than futile. A degraded public–private interface would weaken detection, increase over-compliance, and reduce the overall learning capacity of the regime[3,4,5].

A tenth strategic function is data and identifier integrity. The consolidated list, daily EUR-Lex updates, and common standards for internal controls all matter because the compliance track ultimately acts on names, identifiers, ownership records, payment fields, and transaction attributes. The sanctions-resources page explains that the consolidated list reflects the officially adopted texts and that EUR-Lex provides the official and most comprehensive access to EU legal documents in all official languages. This function must be preserved through 2026–2030 because a compliance system with weak data integrity becomes slower, noisier, and less reliable, even if its legal design remains strong. The more the regime relies on targeted controls, beneficial-ownership analysis, and cross-border screening, the more important it becomes that the data layer remain current and operationally usable. Poor data quality does not merely reduce efficiency; it increases the probability of both missed nexus and needless friction. Data integrity is therefore a foundational strategic function, even if it often appears in practice as a technical one[6,7].

An eleventh strategic function is preservation of learning loops. The Council's Best Practices document is explicitly described as being under constant review, which shows that the sanctions regime is expected to evolve through experience rather than only through package adoption. The UK's annual review makes a parallel point when it highlights targeted advisories, sector-specific outreach, e-alert services, and tailored support across sectors as ways of helping firms adapt and strengthen compliance programmes. These official materials suggest that the future compliance track must remain able to learn from operational feedback, sectoral threat assessments, evasion typologies, and implementation bottlenecks. In the 2026–2030 period, a compliance system that no longer learns quickly from its cases will become progressively more formalistic and less responsive. Learning loops, therefore, are not merely nice-to-have managerial refinements. They are one of the strategic functions that preserve relevance as the adversary adapts[8,9].

A twelfth strategic function is coalition-side burden management. The UK review's emphasis on minimising the administrative burden of compliance and keeping that burden proportionate to firm size

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[2] Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.
[3] European Commission. (2025, October 23). *Making sanctions effective*.
[4] European Commission. (2025, June 11). *Sanctions implementation*.
[5] European Commission. (n.d.). *Overview of sanctions and related resources*.
[6] Ibid.
[7] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[8] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[9] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*).

and exposure is highly relevant to the EU outlook as well. Sanctions can only remain durable if the costs of lawful implementation do not become unnecessarily chaotic or socially concentrated. The Commission's SME-focused Helpdesk model and the OFSI annual review's emphasis on clarity and confidence both point in the same direction. For 2026–2030, burden management should be treated as a preserved strategic function rather than as an external business concern. A sanctions regime whose compliance burdens become too opaque or too uneven will lose legitimacy inside the coalition even if it remains aggressive toward the target. Preserving burden manageability is therefore part of preserving coalition durability. It reduces the risk that firms and national authorities alike begin to treat the compliance track as administratively unsustainable[1,2,3].

A thirteenth strategic function is the preservation of lawful narrow flexibility. The sanctions regime has become more robust in anti-circumvention terms, but it still relies on derogations, humanitarian channels, licensing processes, and other tightly governed permissions to remain proportionate and legally credible. The Commission's "making sanctions effective" page notes the EU-level humanitarian contact point, while the wider guidance ecosystem continues to provide practical information relevant to derogations and sectoral exceptions. The point for 2026–2030 is not that the compliance track should become more permissive. It is that it must preserve the ability to process lawful exceptions without undermining the restrictive core of the regime. A sanctions system that cannot distinguish reliably between prohibited and lawfully authorised activity will either over-block or invite political pressure for broader relaxation. Preserving narrow flexibility is therefore part of preserving overall discipline. It allows the regime to remain hard where it needs to be hard and workable where law already recognises justified exceptions[4,5].

A fourteenth strategic function is outward-facing interoperability with partner jurisdictions. Official EU materials increasingly link sanctions effectiveness to work with partner countries, especially where anti-circumvention and re-export control are concerned. The common high-priority-items logic and the package communications on shadow-fleet listings both implicitly rely on coordination beyond the Union itself. The 17th package communication is especially relevant because it notes that vessel listings were identified together with Member States and the European Maritime Safety Agency and that EU vessel listings, together with efforts from partners such as the UK and the US, were reducing Russia's ability to gain revenues from evading the oil price cap. This demonstrates that, for 2026–2030, preserving the compliance track will also mean preserving its ability to function inside a broader coalition architecture. If interoperability with partners erodes, circumvention space widens through external routing and service substitution. Sanctions compliance must therefore remain outwardly connected, not only internally coherent[6,7].

A fifteenth strategic function is preserving the connection between operational detail and strategic purpose. One of the risks in mature sanctions regimes is that compliance becomes so proceduralised that it loses sight of why particular items, routes, or service channels matter. The common-high-priority-items materials help guard against this by linking specific goods directly to battlefield recovery and military use. The later package communications perform a similar role for shadow-fleet vessels, unsafe tankers, banks, and payment systems. In other words, the compliance track remains stronger when it can still tie its operational priorities to the strategic objectives of degrading Russia's war-sustaining capabilities and reducing circumvention rents. For 2026–2030, preserving this connection will matter because procedural complexity alone does not motivate disciplined implementation. Compliance

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[2] European Commission. (2025, June 11). *Sanctions implementation*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] European Commission. (2025, October 23). *Making sanctions effective*.
[5] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[6] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia*.
[7] European Commission. (2025, October 23). *Making sanctions effective*.

works better when institutions can still see the strategic logic behind the operational burden. The more visible that logic remains, the easier it is to sustain targeted vigilance rather than diffuse fatigue[1,2,3].

A sixteenth strategic function is preservation of visible state capacity behind the compliance regime. The Commission's "making sanctions effective" page highlights expert groups, the Freeze and Seize Task Force, and industry-facing forums. The UK's March 2026 enforcement strategy similarly clarifies departmental roles and the range of enforcement tools. These state-capacity signals matter because private compliance is more reliable when public institutions appear organised, active, and coherent. Firms are more likely to escalate difficult cases, invest in controls, and accept short-term compliance burdens if they believe public authorities can process information, issue usable guidance, and follow up violations in a principled way. A weakly visible state presence, by contrast, tends to encourage either private over-withdrawal or quiet risk tolerance. For the compliance outlook, preserving visible enforcement-support capacity is therefore part of preserving compliance quality itself[4,5].

A seventeenth strategic function is preserving simplicity wherever simplicity does not weaken substance. This is not the same as deregulation. It is the recognition, reflected in the UK review and in the Commission's usability measures, that the administrative form of compliance matters for its long-term sustainability. Simpler guidance architecture, more intuitive list access, clearer reporting routes, and more standardised supervisory expectations reduce avoidable transaction costs without necessarily reducing sanctions pressure on the target. For the 2026–2030 track, simplification should therefore be understood as a preservation strategy. It helps maintain disciplined uptake of a complex regime by preventing the regime from becoming unnecessarily opaque to its implementers. In a cumulative sanctions system, simplification at the interface level can actually preserve hardness at the strategic level. The less energy firms spend deciphering avoidable complexity, the more energy they can spend identifying real circumvention risk[6,7,8].

The strategic conclusion for 2026–2030 is therefore not that the compliance track should simply become larger. It is that the compliance track must retain the functions that make a mature sanctions regime governable under pressure: predictability, rapid update capability, anti-circumvention responsiveness, private-sector usability, legal defensibility, proportionality, cross-border interoperability, enforcement-linked coherence, and continuous learning. These functions already exist in embryonic or developed form across the EU's current architecture and in partner-jurisdiction practice. The challenge of the next period will be to preserve them while the regime continues to adapt to Russia's evolving circumvention techniques and to the coalition's accumulated administrative load. If these functions are preserved, the compliance track can remain a durable operating layer of sanctions pressure. If they degrade, the regime may remain extensive in law yet progressively less effective in practice. That is why the strategic outlook for compliance should be framed not around volume of regulation, but around preservation of operational capacity where it matters most[9,10,11,12].

---

[1] European Commission. (2024, February 22). *List of common high priority items*.
[2] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[3] European Commission. (2025, October 23). *EU adopts 19th package of sanctions against Russia*.
[4] European Commission. (2025, October 23). *Making sanctions effective*.
[5] Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.
[6] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[7] European Commission. (2025, June 11). *Sanctions implementation*.
[8] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[9] European Commission. (2025, October 23). *Making sanctions effective*.
[10] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[11] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[12] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.

Table 7.4.1-1. Strategic Functions to Preserve in the Compliance Track, 2026–2030

Strategic function	Why it must be preserved	Principal operational carriers	Main erosion risk if weakened
Predictability	Keeps firms and authorities aligned on what is prohibited, licensable, and expected	Consolidated FAQs, legal-access architecture, interpretative guidance	Rising over-compliance, under-compliance, and divergent practice
Operational accessibility	Ensures sanctions law is usable in real compliance timeframes	EU Sanctions Helpdesk, sanctions map, consolidated list, EUR-Lex	Smaller operators withdraw or misapply rules
Update speed	Prevents legal adoption from outrunning implementation	List updates, e-alerts, rapid guidance revision, package communication	Implementation lag creates circumvention windows
Anti-circumvention responsiveness	Keeps the regime adaptive against changing evasion patterns	Due-diligence guidance, CHPI/CHPL logic, shadow-fleet targeting	Static compliance becomes easier to route around
Targeted prioritisation	Concentrates scarce compliance effort where strategic impact is highest	High-priority items, vessel listings, payment-system targeting	Diffused enforcement effort and reduced coercive yield
Private-sector usability	Preserves the distributed implementation base of the regime	Helpdesk support, sector-specific guidance, outreach and training	Excessive concentration of compliance in large institutions only
Legal defensibility	Allows fast action to remain reviewable and sustainable	Governance standards, reporting rules, enforcement guidance	Arbitrary practice, challenge risk, and reduced credibility
Cross-border interoperability	Keeps the regime functioning as a Union-wide system	Council best practices, EBA convergence, expert groups, task forces	Forum-shopping, uneven enforcement, fragmented expectations
Enforcement-linked coherence	Links compliance obligations to credible and intelligible state follow-up	Enforcement strategies, criminalisation, reporting routes	Compliance drifts into formality or defensive withdrawal
Continuous learning	Allows the system to adapt from cases, typologies, and sectoral experience	Constant review of best practices, advisories, outreach, feedback loops	Procedural stagnation and rising mismatch with evasion tactics
Burden manageability	Sustains coalition-side willingness to implement the regime over time	Simpler interfaces, proportionate obligations, SME support	Fatigue, resistance, and declining implementation quality
Narrow lawful flexibility	Preserves proportionality without weakening the restrictive core	Humanitarian contact points, derogation handling, licensing pathways	Either excessive blockage or political pressure for broader relaxation

Authorship: prepared by the author on the basis of official EU institutional materials and UK official documents
Sources:

- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Commission. (2025, June 11). *Sanctions implementation*.
- European Commission. (2025, October 23). *Making sanctions effective*.
- European Commission. (2024, February 22). *List of common high priority items*.
- European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
- European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia*.
- European Commission. (2025, October 23). *EU adopts 19th package of sanctions against Russia*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
- European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

- HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
- HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
- Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.

7.4.2. Expected Evolution of Compliance Architecture

The most plausible evolution of the compliance architecture in 2026–2030 is not toward a radically different system, but toward a denser, more data-dependent, more networked, and more continuously supervised version of the system that has already emerged since 2022. The official materials do not present this as a single master plan, yet the institutional direction is clear. The European Commission's implementation pages stress that effective and diligent implementation remains a standing priority, while the EBA has already moved from general expectation-setting to common EU standards on governance, procedures, and controls for restrictive measures. The UK's 2025 cross-government review similarly frames the next phase in terms of systemic efficiencies, information sharing, and lower administrative friction. The implication is that compliance architecture is expected to evolve less through occasional doctrinal restatement and more through operational refinement. In this sense, the next period is likely to be characterised by architectural consolidation rather than conceptual reinvention. The compliance track will remain risk-based, but it will increasingly rely on structured data, better-integrated supervisory logic, and faster public–private feedback mechanisms. This is not speculation in the abstract; it is the trajectory already visible in the institutional materials published by EU and partner authorities[1,2,3].

A first expected shift is from document-heavy compliance toward more structured-data-dependent compliance. The EBA's 2024 sanctions guidelines are especially revealing here because they do not simply ask institutions to "check" sanctions. They require governance over screening datasets, customer data, transfer information, and the policies and controls used to manage them. The same materials distinguish between general restrictive-measures governance and the more specific requirements applied to payment service providers and crypto-asset service providers handling fund and crypto transfers. This indicates a move toward a compliance model in which data fields, transaction attributes, and screening logic matter as much as legal awareness. The likely 2026–2030 evolution is therefore toward a more formalised data architecture underpinning compliance decisions. This will not eliminate the need for legal interpretation, but it will increasingly shift practical emphasis toward data integrity, standardisation, and field-level usability. The more sanctions depend on detecting indirect nexus, layered ownership, and fragmented service chains, the more compliance will need structured data rather than improvised documentary review alone. That trend is already visible in the supervisory grammar of the EBA rules[4,5].

A second expected shift is toward more machine-readable and operationally synchronised legal content. The Commission already maintains a consolidated list, sanctions FAQs, guidance documents, and EUR-Lex access to the legal acts, and its sanctions-resources page is clearly designed as an operational entry point rather than a purely descriptive portal. This suggests that the compliance architecture will continue moving toward systems in which legal change, list change, and guidance change are more tightly connected in time and format. The logic is straightforward. If sanctions packages continue to evolve quickly, the cost of implementation lag rises. A future-ready compliance architecture

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[3] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[4] Ibid.
[5] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.

will therefore need legal content that is not only authoritative, but easier to ingest into internal workflows and digital controls. This is likely to mean greater emphasis on standardised reference points, clearer update cascades, and more seamless transitions from formal amendment to operational deployment. The expected evolution is thus not merely more law, but law rendered in forms better suited to rapid compliance uptake[1,2,3].

A third expected shift is toward typology-based supervision rather than purely rule-recitation-based supervision. FATF's 2025 report on complex proliferation-financing and sanctions-evasion schemes is especially important here because it frames current threats in terms of techniques, vulnerabilities, and risk indicators intended to support both public and private actors. The report explicitly states that the indicators are designed to enhance the ability of public- and private-sector entities to identify suspicious transactions and activity linked to relevant sanctions-evasion risk. This suggests a broader supervisory evolution: authorities are increasingly likely to assess not only whether institutions have a sanctions manual, but whether they can identify and respond to the typologies that matter most in practice. In the 2026–2030 period, compliance architecture is therefore likely to become more pattern-sensitive and less satisfied with formal control presence alone. Firms will still be judged on governance and procedures, but those procedures will increasingly be expected to reflect real evasion methods rather than generic risk statements. This is one of the clearest expected evolutions of the system as it adapts to a more networked circumvention environment[4].

A fourth expected shift is toward sector-specific threat intelligence being built directly into the compliance architecture. The OFSI collection of threat assessments states that these reports are published as sector-specific assessments addressing threats and vulnerabilities relating to UK financial sanctions and are intended to assist stakeholders in key sectors as part of a broader risk-based approach to sanctions compliance. This is a highly instructive development because it shows compliance architecture evolving from general guidance to differentiated risk communication by sector. The logic is likely to spread further. Financial services, cryptoassets, legal services, property, art-market participants, high-value goods, maritime services, and other sectors do not face the same risk shape. A mature compliance architecture for 2026–2030 is therefore likely to rely increasingly on threat-assessment models that push typology-relevant intelligence toward the sectors that actually need it. This would amount to a more granular supervisory ecosystem, in which risk communication becomes more tailored and operationally useful. It is a natural next step for a regime that already depends on private actors to detect the first signs of circumvention[5,6,7].

A fifth expected shift is toward stronger beneficial-ownership analytics and ownership-structure reconstruction. This follows directly from the fact that both sanctions compliance and sanctions evasion increasingly turn on control, hidden benefit, and indirect influence rather than only on listed names. FATF's 2025 report emphasises that significant vulnerabilities remain across the global financial system and highlights techniques that exploit weak transparency and uneven understanding of relevant vulnerabilities. The EU side is moving in a similar direction through its AML/CFT reforms. The Commission's 2024 AML/CFT Q&A explains that the new framework is designed to modernise enforcement and improve detection and that coherent EU-level answers are needed more than ever. The likely implication for sanctions compliance is deeper integration between restrictive-measures screening and beneficial-ownership analysis, especially where cross-border groups, opaque vehicles, and intermediary jurisdictions are involved. In other words, BO verification is likely to become more

[1] European Commission. (n.d.). *Overview of sanctions and related resources*.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
[4] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[5] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
[6] Office of Financial Sanctions Implementation. (2025, February 13). *Sanctions compliance in the financial services sector: threat assessment*.
[7] Office of Financial Sanctions Implementation. (2025, July 21). *Sanctions compliance in the Cryptoassets sector: Threat Assessment*.

analytical and less registry-dependent in the narrow sense. The compliance architecture will increasingly have to think in terms of relationship mapping rather than only static entity identification[1,2].

A sixth expected shift is toward more explicit network mapping of sanctions risk. This is already visible indirectly in the way authorities discuss circumvention through intermediaries, service chains, proxy structures, and cross-border arrangements. But the architecture is also evolving institutionally in that direction. The Commission's "making sanctions effective" page refers to the Freeze and Seize Task Force as a mechanism to explore links between assets belonging to listed persons and criminal activity, while its implementation structures bring together Member States, industry, and stakeholder groups to discuss operational issues. That language of "links" is important. It suggests that the future compliance architecture will increasingly treat sanctions risk as a network phenomenon rather than as a simple one-to-one relation between a listed person and a direct counterparty. In practice, this points toward greater use of networked case analysis, chain-of-transaction logic, and asset-link reconstruction. The likely result for 2026–2030 is a compliance environment that expects institutions not merely to recognise direct hits, but to understand how sanctioned nexus may travel through connected structures[3,4].

A seventh expected shift is toward stronger EU-level supervisory convergence in the financial sector, driven above all by AMLA. The Commission's AMLA Q&A states that, as direct supervisor, AMLA will check compliance with sanctions-related measures by the riskiest cross-border groups in the financial sector, contribute to a common supervisory approach to verification of compliance with sanctions-related requirements, and provide critical input into the understanding and mitigation of risks of sanctions evasion and non-implementation at Union level. This is one of the most consequential indicators of likely future evolution. It means that sanctions compliance is set to become more deeply embedded in the EU's broader supervisory architecture rather than treated as a partly detached foreign-policy overlay. For 2026–2030, this points toward more consistent expectations for large cross-border groups, more centralised risk visibility, and a more harmonised language of supervisory assessment. It does not eliminate Member State responsibility, but it does suggest a thicker EU-level layer of convergence in the financial domain. That is likely to be one of the defining institutional changes of the period[5].

An eighth expected shift is toward more integrated financial-intelligence ecosystems. The Commission's February 2025 article on the 'Next-Generation' FIU.net states that the system went live on 3 February 2025 and provides FIUs and Europol with a significantly improved, state-of-the-art IT solution enabling quicker, more efficient exchange and cross-matching of information. It also states that the new system improves the handling, processing, and transfer of large datasets and enhances interoperability with FIUs' systems. This is highly relevant for the sanctions outlook because it points toward an architecture in which suspicious patterns, sanctioned nexus, and financial-intelligence signals can be processed faster and across more connected systems. The likely 2026–2030 evolution is therefore toward greater use of intelligence-style cross-matching in sanctions-related investigations and compliance support. This should strengthen the public side of the feedback loop on which private detection increasingly depends. It also suggests that structured data and interoperability will not remain purely private-sector matters; they will be equally central to public enforcement capacity[6].

A ninth expected shift is toward more digitally embedded screening and control in payment and crypto environments. The EBA's 2024 sanctions work and the underlying transfer-of-funds and crypto-asset logic already show that compliance expectations now extend to how transfers are screened, interrupted, and evaluated in digital-value environments. The EBA press release explicitly states that its second set of final guidelines is specific to PSPs and CASPs and specifies what those actors should do to comply

[1] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[2] European Commission. (2024, April 24). *Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)*.
[3] European Commission. (2025, October 23). *Making sanctions effective*.
[4] European Commission. (2025, October 23). *Sanctions against individuals, companies and organisations*.
[5] European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
[6] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.

with restrictive measures when performing transfers of funds or crypto-assets. This points to a future in which payment-system compliance will increasingly depend on real-time or near-real-time control logic, digital exceptions handling, and structured analysis of transfer data rather than retrospective manual review. The likely evolution is therefore toward greater technical integration of sanctions controls into payment rails and crypto-service workflows. This does not imply full automation of legal judgement. It implies that the architecture will increasingly have to combine speed with interruption capability, especially as circumvention strategies move further into fast-moving value channels[1].

A tenth expected shift is toward expanded sector-specific guidance rather than a return to broad generic instructions. OFSI's annual review states that, in 2024–25, it prioritised clear communications, targeted guidance, proactive industry engagement, and responsive licensing, and that it provided tailored support across financial services, legal services, cryptoasset, charity, and maritime sectors. This is one of the clearest official signals about future architecture. The likely next-stage model is not a single sanctions manual for all sectors, but a layered environment in which common legal principles are paired with sector-specific operational translation. For 2026–2030, this means the compliance architecture is likely to become more modular: general framework, sector guidance, threat assessments, and issue-specific updates working together. That approach is a rational response to the reality that sanctions risk now appears very differently in banking, shipping, crypto, property, professional services, and trade-control contexts. The future architecture will therefore likely depend on specialisation without fragmentation[2,3].

An eleventh expected shift is toward tighter integration of trade-control compliance with anti-circumvention analytics. The Commission's July 2025 enhanced due-diligence materials for operators dealing in common high priority items are explicitly focused on strengthening due diligence in response to re-export risk and on giving national competent authorities a better tool to curb circumvention through third countries. This suggests a future architecture in which export controls, sanctions screening, route analysis, and end-use due diligence are treated less as parallel exercises and more as parts of a single anti-diversion system. In practical terms, operators are likely to face more expectations around stakeholder mapping, route plausibility, end-user verification, and downstream control over high-priority items. The expected evolution is therefore toward a more tightly coupled trade-compliance architecture, especially where battlefield-relevant goods and third-country re-export risk are concerned. This is consistent with the broader shift from static prohibitions to dynamic anti-circumvention design[4,5].

A twelfth expected shift is toward stronger public–private implementation support as a permanent feature rather than an emergency add-on. The Commission's June 2025 implementation article presents the Support Service as a standing mechanism through which companies can obtain tailored help on sanctions due diligence, counterparties, jurisdictions, goods, end use, and internal programme design. It also notes that many SMEs lack the specialised legal expertise needed to assess complex or changing sanctions situations quickly and accurately. This is highly relevant for the architecture outlook. It indicates that the sanctions regime increasingly recognises its dependence on the operational capacity of ordinary market participants. The likely 2026–2030 evolution is therefore toward a more service-oriented public interface: more support channels, more targeted guidance, more direct assistance to less-resourced firms, and a greater attempt to reduce preventable implementation asymmetries. In effect, the architecture is likely to become more participatory in its operation, even while remaining coercive in its purpose[6].

A thirteenth expected shift is toward stronger interoperability and standardisation across Member States. The Commission's "making sanctions effective" page refers to regular expert-group meetings

[1] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
[4] European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
[5] European Commission. (2024, February 22). *List of common high priority items*.
[6] European Commission. (2025, June 11). *Sanctions implementation*.

with national authorities, the Freeze and Seize Task Force, a high-level group involving all 27 Member State authorities together with industry and business representatives, and ad hoc stakeholder meetings on implementation. The Council's Best Practices are explicitly under constant review. These are strong indicators that the Union expects compliance architecture to evolve through iterative convergence rather than through one-off harmonisation. For 2026–2030, this likely means more pressure toward common operational assumptions, more standardised expectations around controls and reporting, and greater use of shared forums to reduce national divergence. This will not eliminate all differences, but it should strengthen the Union-wide character of compliance practice. That is likely to matter especially where firms operate across multiple Member States and where evasive actors exploit variation between them[1,2].

A fourteenth expected shift is toward closer integration between compliance and enforcement architectures. The UK's 2025 cross-government review framed reform around compliance, deterrence, powers, systemic efficiencies, and better information sharing, while the March 2026 UK strategic approach to sanctions enforcement explicitly links compliance and enforcement as parts of a single strategic logic. The likely significance for the broader compliance outlook is that compliance systems will increasingly be judged by how well they support enforceability: whether they preserve evidence, generate useful reporting, and map risk in a form that supervisory or investigative authorities can use. In other words, the expected evolution is from "compliance as internal control" toward "compliance as enforcement-enabling control". The stronger this integration becomes, the more sanctions implementation will resemble a continuous governance loop rather than a sequence of disconnected legal and private actions[3,4].

A fifteenth expected shift is toward more disciplined use of outsourced RegTech and vendor systems. The current trajectory does not suggest a retreat from technology. It suggests a stronger expectation that firms understand, govern, and be able to explain the technology they use. The EBA's 2024 materials are revealing here because they link sanctions controls to governance and risk-management frameworks, while also identifying weaknesses in internal policies and procedures as risks that undermine the effectiveness of restrictive measures and can lead to circumvention. The implication for 2026–2030 is that institutions will likely be expected to demonstrate not merely that they have a vendor or screening engine, but that they understand its calibration, scope, and integration into decision-making. The architecture is therefore likely to evolve toward more accountable digitalisation rather than naïve automation. Technology will become more central, but also more scrutinised as a governed part of the compliance chain[5].

A sixteenth expected shift is toward more systematic burden management and simplification at the interface layer. The UK cross-government review explicitly focused on improving information sharing and minimising the administrative burden of compliance, while OFSI's annual review framed its work in terms of clear communications, targeted guidance, and helping firms adapt to regulatory change and strengthen compliance programmes. This suggests that the future architecture will not simply add obligations indefinitely. It will also seek to manage the cost of those obligations so that the regime remains sustainable. The expected evolution is therefore paradoxical only on the surface: compliance architecture is likely to become both more demanding in substance and simpler in interface. More structured data, more targeted alerts, more tailored guidance, and better-organised public resources

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] Council of the European Union. (2024, July 3). *EU Best Practices for the effective implementation of restrictive measures*.
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.
[5] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.

can reduce friction for legitimate operators even as the anti-circumvention perimeter hardens. That is likely to be a defining feature of the 2026–2030 phase[1,2].

A seventeenth expected shift is toward real-time or near-real-time alert ecosystems that combine public updates, sectoral risk information, and operator-side response capacity. The OFSI annual review highlights the combined e-alert service and direct communications model, while the Next-Generation FIU.net points to faster public-sector information exchange and cross-matching. Read together, these developments suggest a future architecture in which sanctions compliance becomes less dependent on periodic static review and more dependent on faster alert circulation across both public and private networks. This would fit the operational reality of a regime confronting fast-moving payment systems, evolving shipping patterns, and rapid reconfiguration of intermediary structures. The compliance architecture of 2026–2030 is therefore likely to become more event-driven and less episodic. It will still rely on baseline controls, but it will increasingly depend on rapid signal propagation and response[3,4].

Table 7.4.2-1. Expected Evolution of Compliance Architecture, 2026–2030

Expected evolutionary vector	Institutional signals already visible	Likely operational consequence
More structured-data-dependent compliance	EBA common standards for governance, controls, and payment/crypto screening	Greater reliance on field-level data quality, standardisation, and system governance
More machine-readable and synchronised legal content	Consolidated lists, FAQs, guidance architecture, daily legal updates	Faster conversion of package changes into operational controls
Typology-based supervision	FATF typology and risk-indicator focus; sectoral threat assessments	Supervisory attention shifts from formal presence of controls to their relevance against actual evasion patterns
Stronger BO and network analytics	AML/CFT reform, AMLA role, sanctions-evasion focus	More graph-style analysis of ownership, control, and indirect nexus
Faster intelligence exchange	Next-Generation FIU.net and interoperability improvements	Better public-sector cross-matching and more usable financial intelligence
Sector-specific compliance ecosystems	OFSI targeted guidance and sector threat assessments; Helpdesk model	More differentiated compliance expectations by risk environment
Tighter trade–finance–logistics integration	CHPI due diligence, anti-circumvention focus, payment/crypto screening rules	More holistic transaction review across previously separated control domains
Stronger EU-level convergence	EBA guidelines, expert groups, best-practice updates, AMLA supervisory role	Reduced Member State divergence and more scalable cross-border compliance
More event-driven alert systems	E-alert models, rapid public updates, FIU information exchange	Shift from periodic review to responsive real-time or near-real-time compliance posture
Simpler interface with harder substantive expectations	Review focus on systemic efficiencies and burden reduction	Lower friction for legitimate operators alongside stronger anti-circumvention discipline

Authorship: prepared by the author on the basis of official EU institutional materials and UK official documents
Sources:

- European Commission. (2024, April 24). *Questions and Answers: Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT)*.
- European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
- European Commission. (2025, February 4). *'Next-Generation' FIU.net*.

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] Ibid.
[4] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.

- European Commission. (2025, June 11). *Sanctions implementation*.
- European Commission. (2025, October 23). *Making sanctions effective*.
- European Commission. (2025, July 23). *Enhanced due diligence for operators manufacturing and/or trading with CHP items*.
- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
- HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
- HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
- Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.

The main conclusion is therefore clear. The expected evolution of compliance architecture in 2026–2030 is toward a more integrated, data-rich, typology-sensitive, and continuously updated system. It is likely to rely more heavily on structured data, beneficial-ownership analytics, sector-specific threat intelligence, digital screening capability, cross-border supervisory convergence, and faster intelligence exchange between public and private actors. At the same time, the interface presented to operators is likely to become more support-oriented and more simplified where simplification does not weaken substance. The overall direction is therefore not bureaucratic inflation for its sake. It is the attempt to make a mature sanctions regime more adaptive without making it less governable. For the purposes of this report, the decisive point is that the compliance track is expected to evolve from a predominantly rule-translation layer into a more dynamic risk-governance layer. That evolution is already visible in the institutional sources examined above. The question for 2026–2030 is not whether the architecture will change, but whether that change will be coherent enough to preserve both pressure on Russia and manageability inside the coalition[1,2,3,4].

7.4.3. Risk Outlook: Fragmentation, Fatigue, and Adaptive Circumvention

The risk outlook for the sanctions' compliance track in 2026–2030 is best understood not as a question of whether the regime will survive formally, but whether it can continue to function coherently under cumulative strain. The main threats are unlikely to come from a sudden collapse of legal authority. They are more likely to arise through progressive administrative fragmentation, compliance fatigue across public and private actors, and increasingly adaptive circumvention ecosystems that learn from the system's routines. Official materials already point in this direction. The European Commission presents effective implementation as a continuing priority and highlights the need for expert groups, the Freeze and Seize Task Force, industry-facing meetings, and support for operators. The UK's 2025 cross-government review similarly frames the next-stage challenge in terms of improving compliance, information sharing, systemic efficiency, and burden reduction. Those institutional signals are significant because they imply that the central problem is no longer only package design. It is the resilience of the implementation layer. In forward-looking terms, the compliance track is therefore likely to be tested less by legal insufficiency than by operational wear, unevenness, and adaptation pressure. That is the core frame within which fragmentation, fatigue, and circumvention should be analysed[5,6].

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[3] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[4] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[5] European Commission. (2025, October 23). *Making sanctions effective*.
[6] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.

A first major risk is persistent fragmentation across Member States. The Commission itself states that effective and diligent implementation of sanctions is primarily the responsibility of Member States, while the Commission supports them through coordination structures and stakeholder engagement. That allocation of responsibility is manageable only so long as implementation remains sufficiently convergent. Yet the European Parliament's 2023 study shows that EU sanctions enforcement operates through a highly decentralised architecture with more than 160 designated competent authorities and markedly different national systems. Even if this architecture becomes somewhat more co-ordinated over time, the basic risk remains: cross-border firms still face multiple national authorities, multiple administrative cultures, and multiple enforcement tempos inside one formally common regime. In the 2026–2030 period, any increase in package density, sectoral complexity, or licensing nuance will make this fragmentation risk more consequential rather than less. The more detailed the regime becomes, the more costly divergence becomes for both firms and authorities. Fragmentation therefore remains one of the most durable structural risks to compliance coherence[1,2].

A second fragmentation risk concerns supervisory divergence rather than administrative structure alone. The EBA's 2024 guidelines were presented precisely because, for the first time, common EU standards were needed on governance arrangements and on policies, procedures, and controls to ensure implementation of Union and national sanctions. The fact that this step was necessary is itself revealing. It implies that prior approaches remained too heterogeneous to support sufficiently consistent supervisory expectations. The likely 2026–2030 risk is that even with common standards on paper, actual supervisory practice may still diverge in the depth of review, the tolerance for deficiencies, the treatment of screening weaknesses, or the expectations around escalation and documentation. If that occurs, institutions operating across borders will still face fragmented compliance incentives, even under a more harmonised formal rulebook. The system will then preserve convergence in language while remaining uneven in enforcement reality. That kind of partial convergence is better than none, but it still leaves room for uncertainty, arbitrage, and uneven burden distribution[3,4].

A third risk is guidance overload. The compliance architecture has become progressively richer in FAQs, package explanations, best-practice notes, sector guidance, advisories, and support services. That development is broadly rational, but it also creates a forward-looking burden problem. The Commission's sanctions-resources page shows a layered ecosystem of consolidated lists, FAQs, sanctions maps, Helpdesk functions, and topic-specific guidance, while the Helpdesk article itself highlights that many SMEs need tailored support to understand what sanctions changes mean in practice. This points to a basic tension: the regime becomes more usable through guidance, but also more demanding to track, interpret, and integrate. In 2026–2030, the risk is that guidance volume itself becomes a source of fatigue, especially for firms without large in-house teams. If too many updates, clarifications, and sector notes accumulate without clearer hierarchy and prioritisation, operators may find it harder rather than easier to identify which changes matter operationally. Guidance can therefore be both a remedy for uncertainty and a generator of implementation overload[5,6].

A fourth risk is burden inflation across the private sector. The UK's 2025 cross-government review states that businesses want the cost of compliance to be proportionate to the size of the business and its sanctions exposure, and that businesses also want greater simplicity and clarity. The same review focuses on harnessing systemic efficiencies and minimising the administrative burden of compliance. These points matter because they show that burden accumulation is already recognised officially as a strategic problem. In a long-horizon regime, firms do not experience complexity only as a legal issue.

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[3] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[4] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[5] European Commission. (n.d.). *Overview of sanctions and related resources*.
[6] European Commission. (2025, June 11). *Sanctions implementation*.

They experience it as staffing cost, workflow redesign, screening load, outside-counsel expense, delayed revenues, and repeated internal escalation. The 2026–2030 risk is that these costs continue to rise faster than the capacity of firms—especially mid-sized and smaller firms—to absorb them. Where that happens, lawful risk management may gradually give way either to withdrawal from higher-friction activity or to perfunctory formal compliance. Burden inflation is therefore not only a business complaint. It is a direct risk to implementation quality[1,2].

A fifth risk is public-sector fatigue. The European Parliament's study already documented that, in several Member States, competent authorities were operating with limited dedicated staffing and only modest proactive monitoring capacity relative to the scale of the sanctions challenge. There is little reason to assume that cumulative package growth, expanding anti-circumvention expectations, and criminalisation follow-up will reduce that strain by themselves. On the contrary, more rules, more reporting, and more cross-border co-ordination tend to increase the administrative load on authorities already expected to guide firms, process authorisations, handle breaches, and engage with counterparts across jurisdictions. The risk outlook here is one of institutional fatigue rather than sudden breakdown. Authorities may remain formally active while becoming increasingly selective, slower, or more dependent on triage. In such a setting, the enforcement system may continue to exist but become progressively less able to turn weak signals into timely action. Public-sector fatigue therefore threatens the depth of implementation even where formal commitment remains unchanged[3,4].

A sixth risk is weak feedback density between public and private actors. The compliance track increasingly depends on private institutions to identify suspicious patterns, yet the value of that detection depends on whether authorities can process, prioritise, and learn from what they receive. FATF's 2025 report is especially useful here because it notes that private-sector entities reported limited public-sector feedback on relevant suspicious transaction reporting and other reporting, while also identifying broader information-sharing challenges linked to confidentiality concerns, inconsistent data formats, and delays in dissemination. This suggests a forward-looking risk in which private reporting continues to expand, but the informational return to the reporting entities remains too thin to improve future judgement. In such a model, firms may continue to report because the rules require it, but the learning function of reporting becomes weak. Over time, this can produce both fatigue and declining report quality. An architecture with insufficient feedback loops becomes noisier without necessarily becoming smarter[5,6].

A seventh risk is data strain. The expected evolution of the compliance architecture points clearly toward more structured-data-dependent control, but that very dependence creates vulnerability where data remain incomplete, inconsistent, or difficult to align. The EBA's 2024 work on restrictive measures and its broader AML/CFT risk work both point toward increasing reliance on supervisory data, authority reporting, and structured information about customers, transfers, and controls. This means that data quality, field standardisation, and systems integration will become even more consequential than they already are. In 2026–2030, the risk is that the architecture becomes more sophisticated in principle than the underlying data environment can consistently support. If structured-data ambitions outrun data quality, compliance may generate more alerts, more documentation, and more apparent control, while still struggling with indirect nexus, ownership ambiguity, or cross-system reconciliation problems. The more the architecture relies on data, the more fragile it becomes where data remain uneven[7,8].

---

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[2] European Commission. (2025, June 11). *Sanctions implementation*.
[3] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[4] European Commission. (2025, October 23). *Making sanctions effective*.
[5] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[6] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[7] European Banking Authority. (2024, November 14). *Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures*.
[8] European Banking Authority. (2025, July 28). *Opinion and Report on money laundering and terrorist financing risks affecting the EU's financial sector*.

An eighth risk is screening fatigue inside financial and payment institutions. The more the regime depends on structured screening, event-driven updates, and broad party coverage, the more firms face the operational challenge of managing alert volumes without degrading decision quality. The EBA's sanctions guidelines were designed partly to address such weaknesses, but their very specificity reveals how serious the problem has become. In the next phase, the risk is that firms continue to widen screening scope—across customers, transfers, beneficial owners, crypto-assets, and transaction data—while internal review capacity grows more slowly. This can produce exactly the alert-fatigue dynamic already visible in other parts of the compliance literature: too many low-value signals weaken attention to the higher-value ones. In a mature sanctions' regime, fatigue will often manifest not as abandonment of screening but as a fall in marginal review quality. The system still moves, but it becomes less discriminating[1,2].

A ninth risk is compliance fatigue in sectors newly drawn into sanctions implementation. The OFSI collection of sector-specific threat assessments is revealing because it spans financial services, legal services, property, art-market participants and high-value goods, and cryptoassets. That breadth shows that sanctions compliance is no longer concentrated only in banks, export-control teams, and classic trade intermediaries. More sectors are being drawn into the orbit of sanctions risk because more sectors are now recognised as possible facilitators or weak links. The forward-looking risk is that the compliance culture necessary to absorb these responsibilities will remain uneven. Some sectors may still lack mature internal controls, staff training, or escalation pathways. Others may simply be less used to operating inside a high-pressure sanctions' environment. Fatigue in this context is not only about volume of work. It is about adaptation costs in sectors that were not historically organised around sanctions as a core operational field[3,4].

A tenth risk is implementation fatigue caused by repeated legal and operational change. The EU package communications of 2025 show continued expansion and updating across vessel listings, financial restrictions, anti-circumvention measures, and sectoral prohibitions. The sanctions-resources page also displays repeated FAQ and guidance updates across 2025 and 2026. This indicates a regime that remains highly active and responsive, but it also creates a forward-looking challenge: every update requires internal communication, list refreshes, system adjustment, staff clarification, and sometimes contract or workflow revision. In an extended sanctions environment, the risk is not simply that updates stop coming. It is that the accumulation of updates becomes normalised in a way that erodes organisational attention. Once change becomes constant, institutions may find it harder to distinguish high-impact changes from lower-impact ones. Update cycles can then become less effective even if they remain frequent. Compliance fatigue, in this sense, is partly a problem of adaptation tempo[5,6,7,8].

An eleventh risk is that adaptive circumvention will continue to exploit intermediary jurisdictions and regulatory asymmetries. FATF's 2025 report is explicit that sanctions-evasion schemes exploit jurisdictional differences, uneven implementation, weak transparency regimes, and emerging technologies. This is highly relevant to the 2026–2030 outlook because those enabling conditions are not likely to disappear quickly. Even if the EU strengthens internal convergence, evasive actors can still seek out jurisdictions or service ecosystems where ownership is opaquer, information-sharing is slower, or supervisory attention is thinner. The risk therefore lies not only in the existence of third-country channels, but in the persistence of uneven global governance conditions that make those channels useful. Adaptive circumvention will remain attractive wherever the coalition's internal hardening outpaces

[1] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] Ibid.
[4] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance.*
[5] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[6] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia.*
[7] European Commission. (2025, October 23). *EU adopts 19th package of sanctions against Russia*.
[8] European Commission. (n.d.). *Overview of sanctions and related resources*.

external co-operation. In practical terms, this means the compliance track will continue to face a moving frontier of indirect exposure rather than a stable boundary of risk[1,2].

A twelfth risk is the continuing professionalisation of enabler and intermediary ecosystems. FATF's 2025 report treats complex evasion as an area requiring up-to-date understanding of typologies and vulnerabilities, and OFSI's threat-assessment model itself reflects a growing assumption that different sectors are being used in differentiated ways by those seeking to evade sanctions. The future risk here is not simply more circumvention, but better-camouflaged circumvention distributed across legal, financial, trade, property, and digital channels. As compliance controls become more standardised, evasive actors are likely to become more selective in their use of softer nodes, less visible facilitators, and cross-sector combinations that make the true economic objective harder to reconstruct. The more mature the compliance architecture becomes, the more valuable intermediary innovation becomes to the evasive side. This means that adaptation pressure is likely to remain endogenous to the system rather than episodic[3,4].

A thirteenth risk is the persistence of maritime adaptation. The 2025 package communications already show that the EU continued expanding vessel listings and tightening shadow-fleet-related pressure, which indicates that maritime circumvention had not been neutralised by earlier measures. The fact that the 17th package alone added 189 additional vessels and brought the total to 342 demonstrates that vessel-based adaptation remained dynamic enough to require repeated response. For the 2026–2030 outlook, this implies that maritime risk will likely remain evolutionary rather than static. Vessel ownership, flagging, routing, service ecosystems, and ship-to-ship practices can all be modified more quickly than the regulatory and listing process can fully stabilise them. The risk is therefore not only that shadow-fleet structures persist, but that they continue to mutate in ways that demand repeated public and private adjustment. Maritime circumvention should thus be treated as a continuing adaptation theatre rather than a mostly solved subfield[5,6].

A fourteenth risk is digital acceleration of evasion methods. FATF's December 2025 Horizon Scan on AI and Deepfakes is relevant here because it presents a forward-looking perspective on AI-related risks and vulnerabilities in the AML/CFT/CPF space and frames the study as part of FATF's staged approach to emerging technologies. Even though the horizon scan is broader than sanctions alone, it signals an institutional recognition that emerging technologies may change the speed, scale, and sophistication of illicit adaptation. In the sanctions' context, the implication is not that AI has already transformed all circumvention. It is that the enabling environment for more professionalised deception, synthetic identity support, automated research into weak-jurisdiction strategies, or faster documentation manipulation may become more permissive. For 2026–2030, the risk outlook should therefore include not only current circumvention typologies, but the possibility that technological tools will lower the cost of evasive experimentation. Adaptive circumvention may become not only more distributed, but more iterative and faster to redesign[7,8].

A fifteenth risk is regulatory arbitrage between sectors rather than only between jurisdictions. The OFSI threat-assessment collection shows that the UK is already treating legal services, property, art-market participants and high-value goods, cryptoassets, and financial services as distinct sanctions-risk sectors. That institutional choice implies recognition that sanctions pressure can be displaced laterally across the economy when one channel hardens more quickly than another. The likely 2026–2030 risk is therefore not just re-routing via another country, but re-routing via another professional or service domain. If trade compliance hardens, value may move through alternative payment structures. If banks

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[3] Ibid.
[4] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance.*
[5] European Commission. (2025, February 24). *EU adopts 16th package of sanctions against Russia*.
[6] European Commission. (2025, May 20). *EU adopts 17th package of sanctions against Russia.*
[7] Financial Action Task Force. (2025, December 22). *Horizon Scan AI and Deepfakes*.
[8] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes.*

become more cautious, asset holding may move into property, luxury goods, or service arrangements that are harder to standardise. If traditional intermediaries become more visible, new facilitators may emerge in sectors only recently brought under stronger compliance expectations. The architecture will therefore face cross-sector displacement pressure as well as cross-border displacement pressure[1,2].

A sixteenth risk is that interoperability gains may still be too slow relative to evasion speed. The Next-Generation FIU.net is a significant improvement because it offers quicker and more efficient exchange and cross-matching of information, improved handling of large datasets, and better interoperability with FIUs' systems. AMLA is also expected to manage and further develop FIU.net and to play a role in sanctions-related compliance by the riskiest cross-border groups in the financial sector. These are important institutional advances. Yet they also reveal that the system is still in transition. FIU.net only went live in February 2025, AMLA's full sanctions-related supervisory role will mature over time, and operational learning in these new structures will continue into the next phase. The forward-looking risk is therefore not that no progress exists, but that integration gains may arrive more slowly than the adaptation cycle of sanctions-evasion networks. Architectural improvement remains necessary, but it may not immediately neutralise the asymmetry between institutional reform and private innovation[3,4].

A seventeenth risk is that simplification efforts may lag behind complexity growth. The UK review's recommendation to move to a single sanctions list was explicitly tied to industry feedback that a single list would remove duplication of effort and simplify checks. The UK did in fact move to a single list on 28 January 2026, which shows that policymakers recognised interface complexity as a real compliance issue. The broader lesson for the EU outlook is that simplification cannot be treated as a one-off interface improvement. As sanctions regimes proliferate, package structures evolve, and new sectoral tools are added, duplication and layered complexity can re-emerge unless interface design is continually revisited. The risk for 2026–2030 is therefore that the architecture becomes substantively stronger but operationally heavier faster than simplification reforms can compensate. If that occurs, fatigue and fragmentation will reinforce one another rather than offset one another[5,6].

An eighteenth, and final, risk is cumulative interaction. Fragmentation, fatigue, and adaptive circumvention should not be treated as separate threat families. They are likely to intensify one another. Fragmentation raises compliance costs and weakens clarity. Higher costs and weaker clarity increase fatigue in both public and private institutions. Fatigue, in turn, creates more exploitable seams for adaptive circumvention. Adaptive circumvention then forces further package updates, guidance revisions, and sector-specific controls, which can deepen the very overload that produced fatigue in the first place. This circular dynamic is the central risk logic of the next phase. The compliance track can remain formally intact while still losing sharpness through iterative strain. The strategic challenge for 2026–2030 will therefore be to break this cycle by improving coherence, reducing avoidable burden, preserving rapid learning, and keeping the anti-circumvention perimeter adaptable without letting the interface become unmanageable[7,8,9].

[1] Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
[2] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[3] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[4] European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*
[5] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[6] Office of Financial Sanctions Implementation. (2026, January 28). *Moving to a single list for UK sanctions designations*.
[7] European Commission. (2025, October 23). *Making sanctions effective*.
[8] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement.*
[9] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes.*

Table 7.4.3-1. Principal Compliance Risks for 2026–2030

Risk vector	Core mechanism	Main actors affected	Strategic consequence if unmanaged
Member State fragmentation	Divergent implementation structures, priorities, and interpretation channels	NCAs, cross-border firms, supervisors	Uneven enforcement and higher arbitrage opportunities
Guidance overload	Rising volume of FAQs, updates, sector notes, and package communications	SMEs, mid-sized firms, less specialised sectors	Higher implementation error, slower uptake, defensive withdrawal
Private-sector fatigue	Accumulated screening, reporting, training, and escalation burdens	Banks, exporters, insurers, intermediaries, service providers	Declining review quality and more over-compliance or formalism
Public-sector fatigue	Limited staffing, reactive monitoring, stretched investigative capacity	NCAs, customs, FIUs, prosecutors, supervisors	Slower follow-up and weaker proactive detection
Weak feedback density	Reporting without sufficiently useful authority-side learning loops	Firms, regulators, FIUs, enforcement bodies	Lower future signal quality and more reporting noise
Data strain	Structured-data ambitions outrunning data quality and interoperability	Financial institutions, supervisors, enforcement bodies	More false positives, hidden nexus, and system friction
Intermediary-jurisdiction circumvention	Exploiting uneven transparency and enforcement outside the coalition	Exporters, banks, customs, trade-finance actors	Re-routing of risk beyond the strongest internal controls
Sectoral displacement	Moving activity toward less mature compliance sectors	Property, legal services, crypto, art/HVG, logistics	New weak nodes emerge even as older ones harden
Maritime adaptation	Continued mutation of shadow-fleet ownership, routing, and service structures	Shipping, insurers, financiers, maritime authorities	Persistent price-cap and transport-evasion pressure
Technology-assisted evasion	Lower-cost experimentation with digital deception and operational redesign	Compliance teams, FIUs, digital-service providers	Faster evasive iteration relative to institutional adaptation
Simplification lag	Interface reforms failing to keep pace with regulatory complexity	All operators, especially smaller firms	Coalition-side legitimacy and usability deteriorate

Authorship: prepared by the author on the basis of official EU institutional materials and UK official documents
Sources:

- European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
- European Commission. (2025, February 4). *'Next-Generation' FIU.net; European Commission. (2025, June 11). Sanctions implementation*.
- European Commission. (2025, October 23). *Making sanctions effective*.
- European Commission. (n.d.). *Overview of sanctions and related resources*.
- European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
- Financial Action Task Force. (2025, December 22). *Horizon Scan AI and Deepfakes*.
- HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
- Office of Financial Sanctions Implementation. (2025, June 6). *Threat assessments to support sanctions compliance*.
- Office of Financial Sanctions Implementation. (2026, January 28). *Moving to a single list for UK sanctions designations*.

The main conclusion is therefore straightforward. The compliance-risk outlook for 2026–2030 is not dominated by one single threat. It is dominated by a cluster of mutually reinforcing pressures: fragmentation across authorities and sectors, fatigue generated by cumulative burden and constant adaptation, and circumvention strategies that continue to learn from the system's routines. The compliance architecture is already evolving in response, and that evolution is significant. But the risk landscape will remain demanding precisely because institutional hardening and private adaptation are moving in parallel. For the purposes of this report, the decisive analytical point is that long-term effectiveness will depend less on adding ever more formal obligations than on preserving coherence, reducing avoidable overload, and ensuring that adaptive circumvention remains more costly than lawful compliance. That is the threshold the compliance track will need to hold through 2030 if it is to remain a credible component of the wider sanctions' regime[1,2,3].

7.4.4. 2026–2030 Effectiveness Outlook and Adjustment Triggers

The 2026–2030 effectiveness outlook for the sanctions compliance track should be assessed less by the sheer number of packages adopted and more by whether the system can continue to convert legal pressure into durable operational restraint. At this stage, the EU sanctions regime against Russia is already broad enough that its future effectiveness will depend primarily on implementation quality, not on formal breadth alone. The Commission's framing supports that conclusion: it states that effective and diligent implementation is key to ensuring sanctions objectives are met and describes an implementation architecture built around expert groups, the Freeze and Seize Task Force, high-level coordination with Member States and industry, and anti-circumvention work with third countries. The UK's 2025 cross-government review expresses the same logic from a partner-jurisdiction perspective by focusing on compliance, deterrence, information sharing, and burden reduction rather than on legal proliferation alone. The most realistic outlook, therefore, is conditional. The compliance track can remain effective through 2030, but only if certain enabling functions are maintained and if the system reacts quickly when observable stress indicators show that those functions are weakening. In that sense, the question is not whether the regime will formally continue. It is whether it will remain operationally sharp enough to make circumvention more difficult than compliance over time[4,5].

The first condition of long-term effectiveness is clearer drafting and clearer operational translation of that drafting. A cumulative sanctions regime can only remain effective if firms and authorities know where the legally relevant line lies, what is prohibited, what is licensable, and what specific control is expected in the case at hand. The UK review is especially instructive because it identifies clearer and more accessible guidance, a single sanctions list, and further clarity on ownership and control as concrete reforms needed to support effective compliance. The fact that these issues were highlighted officially shows that legal ambiguity is not a theoretical inconvenience but an implementation risk. In the EU context, the Commission's consolidated FAQ architecture performs the same function, supplying practical interpretative support precisely because regulations alone are not enough for uniform use. For 2026–2030, clearer drafting should therefore be treated as an effectiveness condition rather than as a stylistic improvement. A sanctions regime that remains legally forceful but operationally obscure will generate more over-compliance, more under-compliance, and greater enforcement inconsistency. That combination erodes effectiveness even if the formal rulebook remains intact[6,7].

The second condition is speed of operational updating. The sanctions regime has already entered a phase in which package changes, new anti-circumvention tools, vessel listings, and new service

[1] European Commission. (2025, October 23). *Making sanctions effective*.
[2] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[3] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[4] European Commission. (2025, October 23). *Making sanctions effective*.
[5] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[6] Ibid.
[7] European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.

restrictions can alter risk conditions faster than many firms can naturally adapt. The Commission's 19th package communication is especially telling because it couples new financial restrictions, crypto-related measures, new transaction bans, service bans, and 117 additional vessel listings, taking the EU shadow-fleet list to 557 vessels. This is not only a substantive escalation. It is also an operational challenge to the compliance track, which must update lists, workflows, screening logic, stakeholder communication, and escalation criteria quickly enough to prevent lag from becoming exploitable space. The likely effectiveness outlook is positive only if the compliance system continues to absorb change at near-regulatory speed. Where update cycles slow, circumvention gains time and legitimate operators lose confidence. A durable sanctions regime must therefore preserve not just legislative agility, but implementation agility[1,2].

The third condition is stronger feedback loops between public authorities and private operators. Modern sanctions compliance depends heavily on private detection, but private detection only improves over time if it is connected to some meaningful degree of public response and learning. The UK review explicitly recommends making reporting easier, improving information sharing, and increasing collaboration with industry, while also recording strong stakeholder demand for earlier and more useful information exchange, especially with key financial institutions. The Commission's Helpdesk model and its stakeholder meetings serve a similar function at Union level. The deeper point is that effectiveness in 2026–2030 will require the compliance architecture to behave more like a learning system than a one-way command system. When firms receive clearer signals about what types of alerts, patterns, or control failures matter most, their future detection becomes better targeted. Where that feedback remains weak, reporting quality deteriorates and fatigue increases. Faster feedback loops are therefore not a procedural luxury. They are a condition of adaptive effectiveness[3,4].

The fourth condition is stronger enforcement convergence across Member States and across the compliance–enforcement boundary. The Commission's "making sanctions effective" page states that, since the new rules entered into force in May 2024, the EU has easier tools to investigate, prosecute, and punish violations across Member States. Yet later Commission actions show that transposition and convergence are still incomplete. In July 2025, the Commission opened infringement procedures against numerous Member States for incomplete transposition of the directive, and in March 2026 it was still tracking compliance with those obligations. This illustrates a key point for the outlook: effectiveness does not depend only on stronger rules, but on whether those rules are brought into national systems quickly and used coherently. If enforcement convergence strengthens, the compliance track becomes more credible and more predictable. If it weakens, or remains too slow, the private sector will continue to face uneven incentive structures and adaptive actors will continue to exploit the weakest national link. The 2026–2030 outlook is therefore favourable only if criminalisation and administrative convergence move from formal adoption toward genuinely aligned operational practice[5,6,7].

The fifth condition is better data-sharing and more integrated financial-intelligence support. The "Next-Generation" FIU.net, which went live on 3 February 2025, provides a much stronger basis for faster exchange, cross-matching, cross-border reporting, and more effective handling of larger datasets by FIUs and Europol. The same official material states that AMLA will assume management, maintenance, and development of FIU.net by 10 July 2027. These are not only technical improvements. They are direct effectiveness conditions because many Russia-related sanctions cases now depend on linking partial financial signals across borders and institutions. If data-sharing improves, detection of indirect nexus, payment rerouting, and cross-border structuring should become more effective. If it remains too slow or too fragmented, sophisticated circumvention will continue to outpace formal restrictions. For 2026–

[1] European Commission. (2025, October 23). *EU adopts new sanctions against Russia*.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] European Commission. (2025, June 11). *Sanctions implementation*.
[4] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[5] European Commission. (2025, October 23). *Making sanctions effective*.
[6] European Commission. (2025, July 23). *Commission takes action to ensure complete and timely transposition of directives*.
[7] European Commission. (2026, March 20). *March infringements package: key decisions*.

2030, then, data-sharing is not an ancillary optimisation. It is one of the main conditions under which the compliance architecture can remain genuinely cross-border rather than merely nationally compartmentalised[1,2].

A sixth condition is stronger supervisory convergence in high-risk cross-border finance. The Commission's AMLA Q&A states that AMLA, as direct supervisor, will check compliance with sanctions-related measures by the riskiest cross-border groups in the financial sector, contribute to a common supervisory approach, and provide critical input to the understanding and mitigation of risks of sanctions evasion or non-implementation at Union level. This is one of the clearest signs of where the system is heading and what long-term effectiveness will require. The sanctions compliance track has become too central to financial integrity and cross-border risk management to remain governed entirely through disparate national supervisory cultures. If AMLA succeeds in producing a more common supervisory approach, then the compliance track should become more predictable, more scalable for cross-border groups, and more resistant to arbitrage. If that supervisory role remains partial or delayed, the fragmentation risk analysed in Section 7.4.3 will remain high. The effectiveness outlook is therefore tied closely to whether supervisory convergence becomes real in practice and not just formal in mandate[3,4].

A seventh condition is the preservation of narrowly targeted safe operating space for lawful conduct. This point should be stated carefully. A durable sanctions regime does not need broad exemptions that hollow out the regime. However, by inference from the official materials, it does need narrower and more explicit "safe operating assumptions" in areas where ambiguity would otherwise produce defensive over-withdrawal. The UK's February 2026 call for evidence on the ownership-and-control test acknowledges that industry finds control difficult to assess in practice and that this difficulty creates costs and legal risk. The UK review likewise highlights the need for more clarity on ownership and control. In the EU context, the payment-services FAQ preserves differentiated legality across payment functions rather than endorsing blanket service denial. From these sources, it is reasonable to infer that targeted safe harbours—or, more precisely, clearer bounded zones of low-dispute lawful conduct—will be important to preserving effectiveness. Without them, over-compliance will continue to absorb capacity, damage lawful channels, and blur targeting discipline. Targeted safe harbours in this sense are not concessions. They are tools for keeping enforcement effort focused on higher-value risk[5,6,7].

An eighth condition is sustained anti-circumvention prioritisation. The Commission's implementation page is explicit that the EU monitors redirection of trade flows from third countries acting as possible gateways to Russia, gathers information on circumvention patterns from the private sector, and uses measures such as transit bans, "No Russia" clauses, and high-risk-good tools to address circumvention. It also highlights an 18th-package catch-all tool to support Member States in stopping and investigating suspicious shipments of advanced technology items. This matters because the future effectiveness of the compliance track will depend less on total coverage than on whether it continues to identify and press hardest against the channels that matter most: shadow-fleet vessels, high-priority goods, risky payment infrastructures, and enabling third-country nodes. A future compliance architecture that becomes less prioritised would likely become more bureaucratic but less strategically effective. The 2026–2030 outlook is favourable only if prioritisation remains sharp and linked to actual circumvention patterns rather than diluted by procedural sprawl[8,9].

---

[1] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[2] European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
[3] Ibid.
[4] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[5] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[6] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[7] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
[8] European Commission. (2025, October 23). *Making sanctions effective*.
[9] European Commission. (2025, October 23). *EU adopts new sanctions against Russia*.

A ninth condition is manageable compliance burden for the coalition's private sector. The UK review is particularly explicit that compliance costs should be proportionate to firm size and sanctions exposure, while also arguing for clearer guidance, targeted outreach, simplified reporting channels, and a single sanctions list. The UK then implemented one of those recommendations by moving to a single sanctions list on 28 January 2026, explicitly stating that this change responded to industry feedback that a single list would remove duplication of effort and simplify screening. This does not prove that the EU should mechanically adopt the same model, but it does illustrate the broader effectiveness condition: simplification at the interface layer can strengthen rather than weaken substantive sanctions pressure. If the EU compliance track preserves burden manageability, then operator capacity remains broader and more durable. If it does not, implementation will gradually become more concentrated in the largest and best-resourced institutions, while smaller operators retreat. Over time, that narrows the coalition's operational base[1,2].

The effectiveness outlook is therefore positive but conditional: the compliance track can remain materially effective through 2030 if it becomes clearer, faster, better connected, more convergent, and more disciplined in distinguishing high-value circumvention risk from ordinary lawful friction. It becomes materially less positive if those conditions are only partially met. In that case, the likely result is not formal collapse, but a slower erosion of precision through fatigue, fragmentation, and the spread of private defensive withdrawal. In analytical terms, the real question is not whether the sanctions regime survives. It is whether the compliance architecture remains sharp enough to preserve deterrence and disruption while the system itself ages. That is why effectiveness must be monitored through observable adjustment triggers rather than inferred from package counts alone[3,4].

The first major adjustment trigger should be interpretative strain. When authorities find themselves repeatedly issuing clarifications on the same concepts, or when consultations are opened specifically because industry struggles to apply a core test, that is a signal that the drafting–guidance interface has become too uncertain to support efficient implementation. The February 2026 UK call for evidence on ownership and control is precisely such a signal. So too was the UK review's identification of ownership and control as an area needing further clarity. In analytical terms, repeated ambiguity around the same concepts should trigger recalibration before the uncertainty hardens into market over-withdrawal or inconsistent enforcement. That recalibration could take the form of clearer drafting, revised official examples, structured interpretative guidance, or more explicit decision criteria. The key point is that interpretative stress should itself be treated as an operational metric. When one concept begins to consume disproportionate compliance resources, it is no longer just a legal issue. It has become an effectiveness issue[5,6].

The second trigger should be implementation lag between legal change and operational uptake. Repeated need for emergency clarifications, growing dependence on ad hoc explanations, or observable delays in transposition and rollout are all signs that the system's update cycle is under strain. The infringement procedures opened in July 2025 and the Commission's continued follow-up in March 2026 over incomplete transposition of the criminalisation directive are concrete examples of such lag at the Member State level. In a mature sanctions' regime, these delays matter because they create windows in which enforcement remains less coherent than the formal legal framework suggests. By inference, repeated delays in domestic implementation, guidance revision, or screening adaptation should trigger a review of update mechanisms and not merely another incremental legal fix. Adjustment in such cases

[1] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[2] Foreign, Commonwealth & Development Office, HM Treasury, & Office of Financial Sanctions Implementation. (2025, October 13; updated January 28, 2026). *Moving to a single list for UK sanctions designations, 28 January 2026*.
[3] European Commission. (2025, October 23). *Making sanctions effective*.
[4] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[5] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[6] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.

should prioritise synchronisation, implementation timetables, and rapid translation of legal change into operational practice[1,2,3].

The third trigger should be information-flow congestion. The Commission's FIU.net reform shows that faster exchange and cross-matching of information, including large datasets, was already considered necessary in early 2025. FATF's 2025 sanctions-evasion report likewise identifies information-sharing frictions, confidentiality constraints, inconsistent formats, and lack of public-sector feedback as significant barriers. These official signals imply that when reporting volumes rise, but usable intelligence and feedback do not rise proportionately, the system has entered a congestion zone. In practical terms, signs of that zone include repetitive low-value reporting, weak authority response times, and limited improvement in sectoral detection quality over time. By inference, such congestion should trigger procedural simplification, better triage, clearer reporting channels, and stronger feedback to the private sector rather than merely exhortations to report more. A sanctions regime does not become more effective simply by generating more data. It becomes more effective when data become more actionable[4,5,6].

The fourth trigger should be persistent divergence in enforcement or supervisory treatment across jurisdictions. The EBA's common standards and AMLA's future sanctions-related supervisory role both exist because the system recognises that a highly cross-border financial sector cannot operate effectively under radically divergent national compliance expectations. By inference, when comparable institutions or comparable cases continue to produce materially different supervisory outcomes, or when firms must build different control assumptions for broadly similar risks within the same Union market, that divergence should trigger further convergence action. That action might take the form of new EBA or AMLA guidance, more detailed supervisory benchmarks, stronger peer review, or more structured exchanges among national authorities. The key principle is that persistent divergence should be treated as an adjustment signal in its right, not merely as an unfortunate but tolerable by-product of decentralisation. Left untreated, it gradually creates arbitrage, inconsistency, and declining deterrent credibility[7,8,9].

The fifth trigger should be growth of defensive over-compliance. This is partly an inference from the official sources, but a well-grounded one. The UK review, the ownership-and-control consultation, and the Commission's narrow clarifications on lawful payment services all point to the same underlying risk: when institutions cannot easily distinguish unlawful exposure from merely difficult exposure, they begin to substitute broad withdrawal for risk-based control. Such behaviour is not always visible in headline sanctions data, yet it can progressively damage the lawful channels the regime intends to preserve. Signs of this trigger would include repeated category-level service withdrawals, growing demand for clarifications in areas already legally addressed, or evidence that firms are declining lawful business primarily because interpretative risk is too costly to manage. Where those patterns become persistent, targeted safe harbours, clearer bounded examples, or refined derogation and guidance mechanisms should be considered as corrective tools. The goal would not be relaxation, but a restoration of precision[10,11,12].

---

[1] European Commission. (2025, July 23). *Commission takes action to ensure complete and timely transposition of directives*.
[2] European Commission. (2026, March 20). *March infringements package: key decisions*.
[3] European Commission. (2025, October 23). *Making sanctions effective*.
[4] European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
[5] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
[6] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[7] European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
[8] European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
[9] European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
[10] HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
[11] European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*
[12] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.

The sixth trigger should be repeated emergence of new circumvention infrastructures. The 19th package is especially important here because it did not merely add more names. It moved decisively into new payment-system restrictions, sanctions on the developer and issuer of a rouble-backed stablecoin, sanctions on an offshore crypto exchange, transaction bans on third-country banks, additional service restrictions, and a much larger shadow-fleet list. This demonstrates that by late 2025 the circumvention ecosystem was already evolving into new financial and offshore configurations. The obvious implication for 2026–2030 is that each major emergence of a new operational circumvention channel should trigger targeted recalibration before that channel becomes institutionalised. New channels need not be dominant before they become strategically relevant. Where they are clearly being used to preserve access to payments, energy revenues, or sensitive goods, waiting for them to scale may be more costly than early targeted adjustment. In this area, repeated pattern emergence is itself the trigger[1,2].

The seventh trigger should be periodic signs that simplification has fallen behind complexity. The UK review's call for clearer guidance, a single list, and simpler reporting channels, followed by the actual January 2026 move to a single list, shows that simplification can be treated as a deliberate policy response rather than as an afterthought. By inference, the EU compliance track should likewise treat repeated user-facing complexity problems as an adjustment trigger. Where firms, especially SMEs or less specialised sectors, increasingly need support simply to find the right rule or understand which channel applies, the interface layer has become too heavy. Adjustment in such cases should focus on simplification of access, hierarchy, and routing, not on weakening substance. The purpose would be to preserve the system's hardness toward the target by reducing avoidable hardness toward its implementers[3,4,5].

The eighth trigger should be sustained evidence that the public side of the architecture is not keeping pace with the private side's compliance burden. The Commission and partner authorities have already responded to this risk through task forces, Helpdesks, threat assessments, and enforcement strategies. But if public institutions continue to require more structured controls, more reporting, and more sector-specific vigilance without a parallel increase in convergence, support, and timely decision-making, then the compliance track will gradually become more formalistic and less effective. The appropriate response in such circumstances would be not merely to urge better private compliance, but to reinforce public capacity, streamline public interfaces, and prioritise the points at which authority-side bottlenecks are degrading overall system performance. In a long-duration sanctions regime, public-capacity strain is itself an adjustment trigger because the private sector cannot indefinitely compensate for a slow or overloaded state layer[6,7,8].

Table 7.4.4-1. 2026–2030 Effectiveness Conditions and Adjustment Triggers in the Compliance Track

Strategic area	Effectiveness condition	Observable adjustment trigger	Priority response
Legal-operational clarity	Clearer drafting and usable interpretative architecture	Repeated ambiguity around the same concepts, recurrent consultations, rising guidance demand on settled issues	Clarify drafting, revise FAQs, provide bounded examples, refine official interpretative criteria

[1] European Commission. (2025, October 23). *EU adopts new sanctions against Russia*.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] Foreign, Commonwealth & Development Office, HM Treasury, & Office of Financial Sanctions Implementation. (2025, October 13; updated January 28, 2026). *Moving to a single list for UK sanctions designations, 28 January 2026*.
[5] European Commission. (2025, June 11). *Sanctions implementation*.
[6] European Commission. (2025, October 23). *Making sanctions effective*.
[7] HM Treasury, Office of Financial Sanctions Implementation. (2025, October 15). *OFSI Annual Review 2024 to 2025: Effective Sanctions*.
[8] Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.

Strategic area	Effectiveness condition	Observable adjustment trigger	Priority response
Update discipline	Fast translation of package changes into lists, guidance, and workflows	Implementation lag, delayed transposition, slow screening adaptation, repeated emergency clarifications	Tighten update cascades, align implementation timetables, accelerate legal-to-operational rollout
Public–private learning	Faster feedback loops and more useful reporting ecosystem	High reporting volume with weak feedback, low learning value, repeated low-grade alerts	Improve triage, simplify reporting, create better authority-side feedback mechanisms
Supervisory and enforcement coherence	Stronger convergence across Member States and sectors	Persistent divergence in supervisory outcomes or enforcement handling	Issue common standards, deepen peer review, reinforce AMLA/EBA/NCA coordination
Proportionality and lawful usability	Targeted safe operating space for lawful activity	Category-level withdrawal from lawful business, repeated over-compliance patterns	Introduce narrow safe harbours, clearer bounded permissions, better ownership/control usability
Anti-circumvention responsiveness	Rapid reaction to new evasive channels	Repeated emergence of new payment, crypto, maritime, or third-country circumvention structures	Targeted recalibration, fresh listings, new transaction bans, updated sector guidance
Interface manageability	Simpler access to the rules without weakening substance	Rising operator confusion, duplicative list use, support overload, SME dependence on ad hoc help	Simplify list architecture, guidance hierarchy, alerts, and reporting entry points
Public-side capacity	State institutions able to process, guide, and enforce at sufficient speed	Slow authorisations, overloaded NCAs/FIUs/supervisors, weak follow-up consistency	Increase capacity, prioritise high-value nodes, streamline authority workflows

Authorship: prepared by the author on the basis of official EU institutional materials and UK official documents
Sources:

- European Commission. (2025, October 23). *Making sanctions effective*.
- European Commission. (2026, March 13). *Consolidated version of the frequently asked questions concerning sanctions adopted following Russia's military aggression against Ukraine and Belarus' involvement in it*.
- European Commission. (2026, March 13). *Frequently asked questions on the provision of payment services concerning sanctions adopted following Russia's military aggression against Ukraine*.
- European Commission. (2025, February 4). *'Next-Generation' FIU.net*.
- European Commission. (2024, April 24). *Questions and Answers: The new EU Anti-Money Laundering Authority (AMLA)*.
- European Commission. (2025, October 23). *EU adopts new sanctions against Russia*.
- European Banking Authority. (2024, November 14). *The EBA issues final guidance on internal policies, procedures and controls to ensure the implementation of Union and national sanctions*.
- European Parliament. (2023, October). *Implementation and monitoring of the EU sanctions' regimes, including recommendations to reinforce the EU's capacities to implement and monitor sanctions*.
- Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.
- HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
- HM Government. (2026, February 16). *Ownership and Control Test in UK Financial Sanctions Regulations*.
- Foreign, Commonwealth & Development Office, HM Treasury, & Office of Financial Sanctions Implementation. (2025, October 13; updated January 28, 2026). *Moving to a single list for UK sanctions designations, 28 January 2026*.
- Foreign, Commonwealth & Development Office, Department for Transport, HM Revenue & Customs, National Crime Agency, Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, & Stephen Doughty MP. (2026, March 10). *Sanctions enforcement: cross-government approach, March 2026*.

The overall conclusion for 2026–2030 is therefore measured but definite. The compliance track can remain an effective component of the sanctions regime if it continues to preserve operational clarity, update speed, data-sharing capability, enforcement convergence, manageable burden, and high-priority anti-circumvention responsiveness. Its effectiveness should not be judged by regulatory

accumulation alone, but by whether it keeps the cost of lawful compliance lower than the expected cost of evasive adaptation. The most important adjustment triggers are already visible in the institutional sources: ownership-and-control uncertainty, transposition lag, information-sharing bottlenecks, growing dependence on support services, and the emergence of new circumvention infrastructures in shipping, payments, and crypto-enabled channels. If those triggers are recognised early and addressed through targeted recalibration, the compliance architecture should remain durable enough to support sanctions pressure through 2030. If they are ignored, the regime is more likely to erode through fragmentation, fatigue, and private defensive withdrawal than through formal repeal. That is the main analytical lesson of Part 7's outlook section: compliance effectiveness is sustainable, but only under active and repeated recalibration[1,2,3,4].

[1] Ibid.
[2] European Commission. (2025, October 23). *Making sanctions effective*.
[3] HM Treasury. (2025, May 15). *Cross-government review of sanctions implementation and enforcement*.
[4] Financial Action Task Force. (2025, June 20). *Complex Proliferation Financing and Sanctions Evasion Schemes*.