



Sanctions Risk Made Simple: Advanced Guide

The 25-Page Playbook for
Managing Sanctions Compliance
and Mitigating Risk



COMPLY SPHERE
ADVISORY
STAY COMPLIANT

By Mayur Jethwa

For informational purposes only. Not legal advice

Table of Contents

Part I: The Global Sanctions Landscape

- 3-4 The Sanctions Landscape in 2025
- 5-6 Secondary Sanctions – The U.S. Reach Beyond Borders

Part II: Core Compliance Risks

- 7-8 Understanding Ownership & Control
- 9-10 The Real-World Consequences
- 11-12 The 5 Common Gaps That Lead to Disaster

Part III: Emerging Risks

- 13-14 Sanctions & Crypto: A 2025 Reality Check
- 15-16 Key Sanctions Risks in Crypto
- 17-20 Sector-Specific Sanctions Risks

Part IV: Case Studies – Lessons from the Field

- 21-24 Case Studies

Part V: Compliance in Action

- 25-26 Advanced Compliance Toolkit
- 27-28 Compliance Essentials: A Practical Checklist

Part VI: Moving Forward

- 29 How Comply Sphere Can Help
- 30 Conclusion & Key Takeaways

Introduction

In today's interconnected world, sanctions compliance is no longer just a "banking problem." Corporates of every size from manufacturers to energy companies to tech firms are increasingly in the crosshairs of regulators. This guide will help you understand the key sanctions risks.

I have over two decades of experience in financial crime and sanctions compliance, advising leading financial institutions and multinational corporations across the UK, EU, US, and GCC. Through this work, I've seen firsthand how small gaps in compliance can lead to major operational and reputational consequences.

"Compliance isn't about ticking boxes. It's about enabling business to thrive within the rules."



At ComplySphere Advisory, our mission is simple: to help companies operational efficiency, compliance without sacrificing growth, not stifle it and this guide reflects that philosophy

The aim of this guide is clear: to highlight the most common sanctions compliance gaps that could cost your business dearly, and to provide straightforward, practical steps to avoid them.

Mayur Jethwa
Founder, ComplySphere Advisory
www.complysphereadvisory.com

Executive Summary

Sanctions are designed to restrict business with individuals, entities, or countries involved in terrorism, corruption, human rights abuses, or other illicit activities. But for companies, the real challenge lies not in understanding the purpose of sanctions, but in navigating the hidden risks of non-compliance.

In 2025, the risks have intensified:

-  Global Enforcement – Regulators in the UK, EU, US, and GCC are now coordinating more closely than ever.
-  Ownership & Control Rules – Companies are increasingly held liable for indirect links to sanctioned parties.
-  Crypto & Digital Assets – Regulators are targeting emerging technologies and sanction evasion through crypto.
-  Operational Failures – Weak screening, poor data, and limited training are still driving multi-million-dollar fines.



“Sanctions risk is no longer a problem for governments alone – every business is exposed.”

Key Takeaway

Sanctions risks are manageable if they are simplified and structured properly. This guide highlights:

The major global trends shaping sanctions compliance in 2025
The five most common compliance gaps to avoid
Practical steps your business can take to reduce risk

The Sanctions Landscape in 2025

Sanctions are not one-size-fits-all. Each jurisdiction applies its own rules, often with subtle but critical differences. Businesses operating internationally must understand how these regimes interact.

United Kingdom

Post-Brexit: maintains its own sanctions list, independent from EU.
Can issue civil monetary penalties without proof of intent .
Example: Wise fined £350,000 in 2023 for indirect ownership breach.



European Union

- The EU collectively adopts sanctions but enforcement depends on each member state.
- Germany and the Netherlands are seen as proactive enforcers.
- Businesses face risks from inconsistent enforcement across borders.



United States

Most extraterritorial reach – applies to non-US firms using USD, tech, or US links.
Aggressive enforcement with billion-dollar fines.
Example: Coinbase fined \$100M for weak sanctions/AML controls.



Middle East / GCC

- Rapidly aligning with global standards (UAE, Saudi, Qatar).
- Dubai regulators expect robust compliance in fintech/crypto.
- Example: UAE Central Bank fined AED 5.2M for sanctions failings.



Asia-Pacific (China, Singapore, Japan, Australia)

- China: Pushes back against Western sanctions and develops countermeasures, including alternative trade and financial channels.
- Singapore & Australia: Generally align with U.S. and EU sanctions, especially on Russia, North Korea, and terrorism financing.
- Japan: Works closely with G7 partners, with strong emphasis on North Korea and regional security threats.



 Mini-Table for Penalties/Focus by Region

Region	Key Focus	Enforcement Style	Recent Penalties
UK (OFSI)	Ownership & control	Strict, intent not required	Wise – £350k (2023)
EU	Dual-use exports, trust sector	Uneven across states	Dutch trust firm – €1.8M (2023)
US (OFAC)	USD, tech, crypto, global reach	Extraterritorial, aggressive	Coinbase – \$100M (2023)
GCC	Fintech, crypto, exchanges	Increasingly strict	UAE Exchange House – AED 5.2M (2022)

 **Key Point:** Sanctions rules differ across the UK, EU, US, and GCC, but regulators expect firms to follow the strictest standard. A transaction legal in one region could breach rules elsewhere, especially with OFAC’s extraterritorial reach.

 **Takeaway:** Build your compliance framework around the highest bar, not the lowest .

Secondary Sanctions – The U.S. Reach Beyond Borders

What Are Secondary Sanctions?

Unlike primary sanctions, which apply to U.S. persons and entities, secondary sanctions extend U.S. restrictions to non-U.S. companies. They target businesses and financial institutions anywhere in the world that engage with sanctioned countries, entities, or sectors.

“The aim is to deter foreign firms from undermining U.S. sanctions policy by threatening them with loss of access to the U.S. market and financial system.”



How They Differ From Primary Sanctions:

Primary sanctions: Apply directly to U.S. persons, citizens, companies, or transactions with a clear U.S. nexus (e.g., use of USD or U.S. technology). They prohibit specific dealings such as trade, services, or financial transactions with sanctioned parties.

Secondary sanctions: Apply indirectly, even if there is no U.S. connection. The U.S. government can penalize non-U.S. firms by cutting off their access to U.S. markets, banking systems, or counterparties. They are designed to pressure third-country actors to comply, effectively globalizing U.S. sanctions policy.

Key Regions Where They've Been Applied:



Iran – Banking, oil exports, shipping, and insurance sectors.



Russia – Energy projects, sovereign debt, and financial institutions.



North Korea – Shipping companies, insurers, and trading firms facilitating Pyongyang's global trade.



Venezuela – Oil sector and companies supporting state-owned enterprises.

Why Non-U.S. Businesses Must Care:

Even if a business has no direct U.S. operations, it can face severe consequences:

- **Banking Access** – Secondary sanctions often lead to being cut off from U.S. dollar clearing, which underpins global trade.
- **Correspondent Relationships** – Global banks routinely exit clients involved in secondary-sanctioned activities to protect their own U.S. market access.
- **Insurance & Financing** – Insurers, investors, and lenders de-risk by cutting ties with exposed companies.

 **Takeaway: Even without U.S. operations, secondary sanctions can cut off your global market access.**

Understanding Ownership & Control

One of the most misunderstood areas of sanctions compliance is the concept of ownership and control.

Ownership

Ownership rules determine whether an entity is considered sanctioned due to its link with a sanctioned individual. *For example:*

If a sanctioned person owns 50% or more of a company, that company is automatically sanctioned under OFAC rules. In the EU and UK, thresholds may be lower, or sanctions may apply even if control is exercised indirectly.

Control

Control goes beyond shareholding. A sanctioned person may still “control” a company if they:

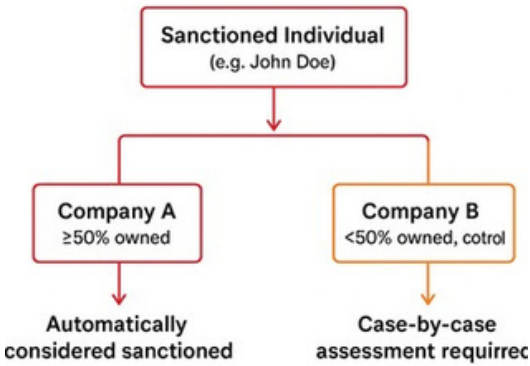
- Hold significant voting rights.
- Have the power to appoint or remove directors.
- Influence decisions through contracts or informal arrangements.

Here’s a comparison chart for ownership and control thresholds in sanctions:

Jurisdiction	Ownership Threshold	Control Considered?	Sanctions Trigger
US (OFAC)	≥ 50% ownership (aggregate across sanctioned persons)	Yes – influence below 50% may still apply	“50% Rule” → automatic designation
UK (OFSI)	No fixed % – looks at “substantial influence or control”	Yes – at any level	Case-by-case; sanctions can extend to controlled entities
EU	≥ 50% ownership by listed person	Yes – control assessed even below threshold	Automatic at 50%+, control risks below

👉 **Takeaway:** US applies a strict numeric rule, while the UK and EU leave more to interpretation — increasing case-by-case risk.

Sanctions Risk Through Ownership Chains



- **Direct Ownership ≥50%:** Any company directly owned 50% or more by a sanctioned individual is automatically treated as sanctioned.
- **Minority Ownership <50%:** Companies controlled but owned less than 50% require a case-by-case assessment of sanctions exposure.

- **Control Through Influence:** Even without majority ownership, placing associates in key board or management positions may trigger regulatory scrutiny.
- **Ownership Chains Matter:** Sanctions risk can flow through complex ownership structures, making ultimate beneficial ownership (UBO) checks critical.
- **Regulatory Implications:** Authorities may consider both direct and indirect control when enforcing sanctions compliance.

Even minority ownership or indirect influence can create sanctions exposure. Regulators may treat companies as sanctioned if a sanctioned individual holds a significant stake, sits on the board, or can influence key decisions, even without majority ownership.

Key Takeaways

1. Ownership and control are critical risk factors.
2. Thresholds differ across jurisdictions:
 - US: 50% ownership triggers automatic sanctions
 - UK: Any substantial influence or control is relevant
 - EU: Typically 50% ownership, with control also considered
3. Screening must account for direct and indirect ownership, including subsidiaries and complex structures

The Real-World Consequences

Sanctions breaches are not just about fines—they carry serious, real-world consequences that can affect businesses of all sizes. Beyond financial penalties, breaches can disrupt operations, damage reputations, and expose executives to personal liability. These risks extend far beyond compliance, threatening a company's survival, eroding client and investor trust, and leaving a lasting mark on its public image. The following examples illustrate the tangible impact of failing to manage sanctions effectively.



Reputational Damage

Impact: Sanctions breaches can permanently tarnish a company's image. Clients, partners, and investors may rethink their relationship. Media coverage can linger for years.

Example: Several international banks fined in the 2010s are still cited in compliance case studies and news articles today, long after paying penalties.

Takeaway: Reputational loss is long-term and harder to fix than financial damage.

Financial Penalties

Impact: Sanctions breaches can trigger fines from thousands to billions, plus reputational and legal consequences. No firm—large or small—is exempt.



Example: US regulators fined a bank \$1.1 billion, while crypto exchanges faced hundreds of millions for weak sanctions controls. Even smaller UK fintechs and EU corporates have been hit with six-figure fines for minor breaches.

Takeaway: No business is “too small” or “too niche” to escape regulatory attention.



Operational Disruption

Impact: Sanctions breaches can halt operations—blocked transactions, frozen assets, or terminated contracts can ripple across the business.

Example: In 2023, a European shipping company lost millions when a vessel was detained for suspected sanctions breaches. No fine was imposed, but client confidence suffered lasting damage.

Takeaway: The indirect costs of disruption often outweigh the fine itself.

“Sanctions are not abstract rules, they are real-world risks with real-world consequences.”

Criminal Liability

Impact: Serious sanctions breaches can lead to personal liability for directors and officers, including prison. In the US, some violations carry up to 20 years.



Example: In 2020, an Iranian sanctions case led to individual executives being indicted in the US, with extradition requests issued overseas.

Takeaway: Sanctions are not just a corporate risk—they can also affect individual decision-makers personally.

🔥 **Key Message:** Sanctions risk is not just a regulatory issue, it's a business survival issue. The costs financial, operational, reputational, and personal are simply too high to ignore.

The 5 Common Gaps That Lead to Disaster

Even well designed compliance programs can collapse when critical gaps are overlooked. Weak transaction screening, reliance on opaque third parties, emerging asset risks, and limited oversight in global operations all create blind spots that sanctioned actors can exploit. These five common pitfalls highlight where businesses are most exposed and why addressing them is essential to avoid regulatory fines, reputational damage, and operational disruption.

Ineffective Screening

Reliance on outdated or incomplete screening tools. Systems not configured to capture subsidiaries, spelling variations, or indirect ownership.



 **ComplySphere Tip:** Regularly audit and update your screening tools. Ensure they capture corporate hierarchies, variations in spelling, and indirect ownership structures. Automate checks where possible to reduce human error.



High False Positives

Overly broad filters generating thousands of meaningless alerts by noise, leading to real risks being overlooked.

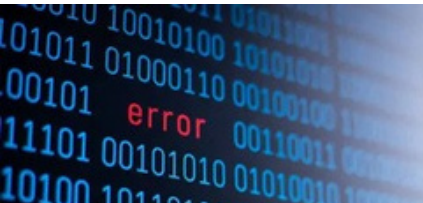
 **ComplySphere Tip:** Calibrate thresholds and prioritize high-risk matches. Implement a triage process to separate actionable alerts from noise, and ensure staff have clear procedures for escalation.

Lack of Ongoing Due Diligence

Screening only performed at onboarding, not during the relationship. Sanctions lists update daily—yesterday’s clean client may be today’s risk.



ComplySphere Tip: Implement continuous monitoring of clients, vendors, and counterparties. Automate daily list updates and periodic rescreening to catch new risks in real time.



Poor Data Quality

Incomplete or misspelled customer records. Transliteration issues in non-Latin alphabets (e.g., “Muhammad” vs. “Mohamed”).



ComplySphere Tip: Maintain clean, standardized, and validated customer data. Use robust data-matching software and incorporate transliteration and alias checks to reduce missed hits.

Inadequate Training

Frontline staff unaware of how sanctions work. No clear escalation process for potential matches.



ComplySphere Tip: Conduct regular, scenario-based training for all staff interacting with customers or transactions. Define clear escalation paths, and ensure employees understand both the regulatory requirements and the business impact of non-compliance.

Sanctions & Crypto: A 2025 Reality Check

Sanctions regulators have moved aggressively into the world of crypto. Unlike the early days, when enforcement was largely symbolic. 2025 has seen regulators treating crypto businesses exactly like banks, with real penalties and public enforcement.



US (OFAC): Designated multiple crypto mixers (e.g., Tornado Cash) and blacklisted wallets tied to North Korea's Lazarus Group. OFAC's stance is clear: if your platform touches sanctioned funds, even indirectly, you are on the hook .

EU: Issued its 8th sanctions package including prohibitions on providing crypto-asset wallets, custody, or trading services to sanctioned persons, closing loopholes exploited in 2022–2023.

UK (OFSI): Expanded sanctions rules to explicitly include crypto exchanges and custodians, mandating screening, reporting, and asset freezes. Enforcement guidance highlights crypto as a priority risk area.

UAE & GCC: Regulators such as the UAE's Virtual Assets Regulatory Authority (VARA) and the Central Bank of Bahrain require crypto firms to apply bank-level AML/sanctions controls, including transaction monitoring, customer due diligence, and reporting suspicious activity

Key Sanctions Risks in Crypto

1. Mixers & Tumblers

How they work: Mixers pool crypto transactions from multiple users, then redistribute them in a way that breaks the transaction trail. Tumblers add further obfuscation by fragmenting transactions into smaller amounts before redistributing.



- **Sanctions Risk:** Mixers are used by ransomware groups, darknet markets, and sanctioned actors (e.g., North Korea's Lazarus Group) to launder funds.
- **Regulatory Risk:** OFAC has sanctioned mixers like Tornado Cash, showing that "technical neutrality" is no defence, platforms enabling evasion are liable.
- **Operational Risk:** Exchanges or custodians processing deposits linked to mixers may unknowingly handle sanctioned transactions.

2. Decentralised Finance (DeFi)



How it works: DeFi allows users to lend, borrow, and trade assets directly through smart contracts—without a central operator or traditional compliance oversight.

- **Sanctions Risk:** With no central control, sanctioned actors can access DeFi using only a wallet address.
- **Regulatory Risk:** US Treasury and OFAC may hold developers, token holders, or operators liable if they're seen as exercising control.
- **Operational Risk:** Screening is difficult, wallets under a false name and smart contracts can expose firms to sanctioned funds without human involvement.

3. Anonymous / Non-Custodial Wallets

How they work: Unlike exchange-hosted wallets (custodial), non-custodial wallets allow users to hold their own private keys and transact directly on the blockchain. Some are designed for privacy, with no customer data collected.



- **Sanctions Risk:** Non-custodial wallets lack KYC, making UBOs untraceable and attractive to sanctioned actors, terrorists, and cybercriminals.
- **Regulatory Risk:** Exchanges, custodians, and OTC desks are expected to screen wallet addresses, monitor activity, and apply enhanced due diligence.
- **Operational Risk:** Without screening, firms risk facilitating payments for sanctioned individuals using anonymous wallets.

Key crypto tools carry different layers of Sanctions risk:

How it Works	Sanctions Risk	Regulatory Risk	Operational
Mixers	Process funds from sanctioned entities	OFAC penalties for users	Funds lost if mixer shut/hacked
DeFi	Exposure to sanctioned wallets	SEC/FCA fines for unregistered activity	Smart contract exploits
Wallets	Holding sanctioned assets	KYC/AML breaches	Provider hacks or downtime

👉 **Key Takeaway:** Each of these vectors creates opacity in financial flows. Regulators see this as the exact opposite of sanctions compliance, which depends on transparency and traceability. Businesses that engage with these technologies without building robust screening, monitoring, and escalation controls are exposed to serious regulatory enforcement, reputational fallout, and even criminal liability.

Sector-Specific Sanctions Risks

Every sector interacts with global markets, supply chains, or financial flows in ways that can expose them to sanctions violations. Each industry has unique blind spots that require tailored risk management.

Finance & Fintech

- **Transaction Screening Gaps:** Fast payments, especially instant or cross-border, often bypass thorough sanctions checks.
- **Correspondent Reliance:** Smaller fintechs and banks depend on global partners but can't always see where funds truly come from or go.
- **New Assets:** Crypto, e-wallets, and alternative finance are under pressure from regulators for not applying strong, bank-level controls.



Sanctions Risk: Regulators expect the same level of compliance sophistication from fintechs as they do from global banks. Failure to demonstrate equivalent controls can quickly lead to penalties or de-risking by partners.

Corporate Supply Chains



- **Third-Party Risk:** Vendors, subcontractors, distributors may be tied to sanctioned entities without the buyer knowing.
- **Oversight Risk:** Global supply chains in high-risk regions often lack visibility into local partners.
- **Dual-Use Risk:** Everyday goods like electronics, chemicals, or software can be diverted for military use.

Sanctions Risk: Even if the company itself has no direct sanctions exposure, liability can arise through suppliers. Enforcement cases increasingly show that “I didn’t know” is not a defence, expectations are for end-to-end due diligence.

Shipping & Trade

- AIS Gaps: Ships switch off tracking systems to hide activity in sanctioned waters.
- Flag Changes: Vessels re-register under new flags to mask links to sanctioned states.
- Cargo Diversions: Goods are routed through third countries to disguise origin or destination.
- Insurance Risks: Insurers face liability if they cover ships involved in sanctions breaches.



Sanctions Risk: Shipping is one of the most heavily scrutinised sectors due to its role in oil, weapons, and dual-use goods transport. Regulators increasingly use satellite data, trade analytics, and AI to spot violations.



Energy & Natural Resources



- Joint Venture Risk: Partnerships with foreign firms can quickly fall under new sanctions.
- Export Control Risk: Energy sectors like oil, gas, and mining are prime targets.
- Technology Risk: Equipment, parts, and software for extraction often face restrictions.

Sanctions Risk: Exiting joint ventures or projects in sanctioned jurisdictions can result in billions in stranded assets. Firms face both financial loss and reputational fallout when geopolitical winds shift.

Technology & Telecoms

- **Restricted Exports:** Chips, software, and advanced telecoms infrastructure are frequently restricted under dual-use controls.
- **Digital Services:** Cloud hosting, SaaS, and data transfer may expose providers to sanctioned jurisdictions without their knowledge.
- **Encryption & Surveillance Tools:** Increasingly scrutinised when sold to high-risk governments.



Sanctions Risk: Tech firms often underestimate their exposure, but regulators see them as critical choke points in modern sanctions enforcement.

Lesson: Tailoring a Risk-Based Approach

Every sector has its **unique blind spots**, areas where sanctions exposure can lurk unnoticed. A one-size-fits-all compliance program is no longer sufficient. Businesses must adopt a **risk-based approach**, which involves:

1. Identifying Exposure Points
2. Assessing Risk Level
3. Tailoring Controls
4. Testing & Monitoring
5. Proactive Response Planning

Key Takeaway: A proactive, sector-specific, risk-based approach doesn't just reduce fines or reputational damage it protects operational continuity, investor confidence, and long-term business strategy. Waiting until a breach occurs is far more costly than identifying and closing gaps in advance.

Case Studies - 1: European Bank



Background:

A large European bank processed multiple trade finance transactions that unknowingly involved sanctioned Russian entities. The transactions were routed through intermediary banks in other jurisdictions, creating a blind spot in compliance monitoring.



What Went Wrong:

- Screening was limited to customer-level checks, ignoring transaction-level risks.
- Reliance on outdated sanctions lists and incomplete data mapping led to missed matches.
- Internal alerts were generated but not escalated promptly to the compliance team.



Consequences:

- Fined over €5 million by the European regulator.
- Significant reputational damage, with investors questioning the bank's risk controls.
- Compliance overhaul required, including new transaction monitoring systems and staff retraining.

Lesson Learned:

Transaction-level due diligence is critical. Screening only at onboarding is insufficient. Every payment, trade, or transfer must be assessed for sanctions exposure.

Case Studies - 2: Global Shipping Company



Background: A shipping company transported goods for an entity indirectly linked to sanctioned parties. The vessel's ownership was masked through a series of flag changes, and the cargo route included multiple transshipment points.



What Went Wrong:

- Compliance team relied on vessel registration and ownership data that was incomplete or outdated.
- Automated tracking systems failed to flag unusual route changes.
- Limited due diligence on third-party charterers and freight forwarders.



Consequences:

- Vessel detained for several weeks, resulting in millions in delayed cargo costs.
- Contractual penalties triggered due to breach of delivery schedules.
- Regulatory investigation increased scrutiny on other fleet operations.

Lesson Learned:

Monitoring vessel movements and trade routes is essential. Even indirect involvement with sanctioned entities can trigger enforcement. Advanced tracking and verification of shipping partners mitigate risk.

Case Studies - 3: Crypto Exchange



Background:

A cryptocurrency exchange processed transactions for wallets linked to a sanctioned group operating overseas. The breach was not intentional; it resulted from inadequate screening and weak escalation protocols.



What Went Wrong:

- The exchange relied on manual checks and basic transaction flags, which failed to detect complex wallet layering.
- No enhanced due diligence for high-risk geographies.
- Staff were undertrained in sanctions obligations for digital assets.



Consequences:

- Fined by OFAC for failing to prevent sanctioned transactions.
- Heightened scrutiny by banking partners and potential de-risking of fiat on/off ramps.
- Urgent investment required in blockchain analytics and staff training.

Lesson Learned:

Crypto requires the same compliance rigor as traditional finance. Firms cannot treat digital assets as “different” or assume sanctions don’t apply.

Case Studies - 4: Secondary Sanctions in Practice



Background:

A mid-sized European engineering firm supplied parts to a Russian energy project in 2023. The project itself was not sanctioned under EU law, and the firm believed it was compliant with local regulations



What Went Wrong:

- The project was linked to a Russian state-owned enterprise covered by U.S. secondary sanctions.
- U.S. banks refused to process payments related to the project.
- The firm’s European banking partners terminated accounts, citing “secondary sanctions exposure.”
- Insurance providers also withdrew coverage, citing compliance risks.



Consequences:

- Loss of access to U.S. dollar clearing.
- Supply chain disruption as shipping partners refused to transport goods.
- Major reputational damage, with investors questioning governance and risk controls.

Lesson Learned:

Compliance with EU rules alone was not enough. The U.S. extraterritorial reach meant that ignoring secondary sanctions put the company’s global financial access at risk. A proper sanctions risk assessment should have flagged the exposure before contracts were signed.

Sanctions Exposure Checklist:

Ask these questions before engaging in high-risk business: They help identify hidden exposure points and prevent costly regulatory surprises.



- **Do we rely on U.S. dollar clearing?** Even if all parties are non-U.S., USD transactions flow through U.S. banks and can create exposure.
- **Do our suppliers, customers, or partners have a U.S. nexus?** (e.g., U.S. offices, U.S. shareholders, or U.S.-origin technology). **Could indirect exposure occur?** Think freight forwarders, insurers, distributors, or joint ventures linked to sanctioned jurisdictions.
- **Are we screening for secondary sanctions risks?** Standard screening may only catch primary sanctions; secondary risks need enhanced monitoring.
- **Are we tracking ownership/control chains?** Even minority stakes by sanctioned persons can trigger secondary exposure.
- **Do we understand sectoral hotspots?** Energy, shipping, aviation, defense, and financial services are under heightened U.S. scrutiny.

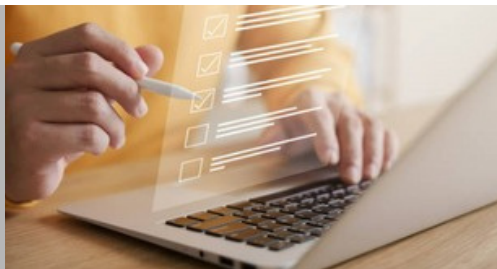
Practical Mitigation Steps:

- 1. Enhanced Due Diligence (EDD):** Go beyond name screening: map out ownership structures, beneficial owners, funding sources, and supply chain touchpoints.
- 2. Banking Strategy:** Engage with relationship banks early to gauge their sanctions tolerance. Some banks “de-risk” entire sectors (e.g., shipping or crypto).
- 3. Escalation & Governance:** Create a documented escalation policy with thresholds for compliance and board review. Ensure senior management visibility.
- 4. Scenario Planning:** Run “what if” drills (e.g., What if our logistics partner is sanctioned tomorrow?). Stress-test the financial and operational impact.
- 5. Contractual Protections:** Include sanctions clauses in supplier, distributor, and JV agreements allowing termination if sanctions are triggered.
- 6. Training & Awareness:** Tailor training for procurement, trade, treasury, and legal teams to spot indirect sanctions risk.
- 7. Seek Specialist Advice:** For high-risk sectors (energy, shipping, commodities trading, correspondent banking), obtain independent legal or compliance reviews.

 **Key Message: Secondary sanctions are not just a U.S. legal issue, they are a global market access issue. Businesses that ignore them risk losing correspondent banking, financing, and trade partners, effectively cutting themselves off from the international financial system.**

Compliance Essentials: A Practical Checklist

To simplify sanctions compliance, every business should ensure it has these core elements in place. These are not optional—regulators expect them across sectors, from banking and fintech to shipping, trade, and corporate supply chains.



Customer Due Diligence (CDD)

- Verify ownership, control, and beneficial ownership of all clients and partners.
- Understand corporate structures, ultimate beneficial owners, and any politically exposed persons (PEPs).
- Example: Check shareholder chains for indirect links to sanctioned individuals or entities.



Sanctions Screening

- Apply screening to customers, payments, vendors, vessels, contracts, and counterparties.
- Include both direct and indirect exposure, such as offshore entities or intermediaries.
- Ensure your system can handle multi-jurisdictional lists (UK, EU, US, UN).
- Example: A supplier in a third country may indirectly connect your business to a sanctioned party



Escalation Procedures

- Have clear rules for handling potential matches.
- Define who reviews alerts, timelines for escalation, and documentation requirements.
- Example: A flagged payment should immediately go to the compliance officer before execution.



Ongoing Monitoring

- Update sanctions lists daily, not just at onboarding.
- Rescreen existing clients, vendors, and counterparties regularly.
- Automate alerts for new matches but always have human verification before action.
- Example: Yesterday's compliant client could appear on today's updated OFAC or OFSI list.



Training

- Conduct regular sessions for compliance teams, front-line staff, and management.
- Include sector-specific scenarios (e.g., shipping routes, crypto wallets, trade finance).
- Reinforce the consequences of sanctions breaches—financial, operational, reputational, and criminal.



Governance & Oversight

- MLRO or Compliance Officer should report directly to the board on sanctions exposure.
- Maintain formal policies, procedures, and record-keeping to demonstrate compliance diligence.
- Example: Regulators often check whether the board was informed when enforcement issues arise.



Record-Keeping & Audit Trails

- Maintain comprehensive and accurate documentation of all sanctions checks, UBO verifications, and transaction reviews. Ensure that audit trails are easily retrievable for internal reviews and regulatory inspections.
- Keep records of all decisions, escalations, and actions taken to demonstrate compliance and accountability.



Practical Tip:

- Think of compliance as risk management in action. Tools, systems, and staff are critical but so is a culture where everyone understands sanctions obligations and takes responsibility.

How ComplySphere Can Help



Our Services:



Sanctions Health Checks: Assessments of your current framework.



Advisory & Consulting: Policies, procedures, and governance tailored to your sector.



Training: Staff training delivered in plain language.



Toolkits: Ready made frameworks for startups, fintechs, and corporates

Why ComplySphere?

Multi-jurisdictional expertise (UK, EU, US, GCC).
Decades of experience across banking, fintech, and law enforcement.
Neutral, independent, and practical guidance.

If you would like to discuss how ComplySphere can support your business, contact us today:

 **Email:** info@complysphereadvisory.com
 **Website:** www.complysphereadvisory.com

Conclusion: Taking Control of Sanctions Risk

Key Takeaways

- Key Takeaways
- Sanctions are dynamic and global; staying informed is essential.
- Blind spots exist in every sector; a tailored, risk-based approach is critical .
- Transaction-level due diligence, continuous monitoring, and escalation procedures save businesses from costly mistakes.
- Crypto and emerging technologies carry new risks, but with the right controls, they can be safely integrated into operations.
- Compliance is not just about avoiding penalties, it is about building trust with clients, partners, and regulators, and safeguarding long-term business success.

By understanding these principles and implementing robust controls, your business can navigate the complex sanctions landscape with confidence and resilience.



www.complysphereadvisory.com