KSE | Institute

Prepared by KSE Institute Sanctions Team, Fall 2024

Best Practices Handbook for Compliance with Export Controls and Sanctions

Introduction

As geopolitical risks continue to escalate each quarter, it is evident that sanctions and export regulations have become a permanent fixture in the international business landscape. For companies operating in this environment, compliance with these regulations is not merely a legal requirement, but a vital interest. A structured and well-organized internal control process for compliance is essential for mitigating not only legal risks but also reputational and ethical risks. This handbook is designed to provide guidance to companies seeking to navigate the complexities of export controls and sanctions, ensuring that their operations remain in line with both the letter and the spirit of the law.

Compliance Best Practices

Understand the requirements

Stay current with export controls and sanctions by appointing a dedicated person to monitor legal updates and brief management regularly. Depending on a sanctions program, the restrictions may apply to transactions, business partners, products, trades and holdings of securities, including derivatives, and other more complex criteria, such as relationship with governments or a percentage of revenue that an entity received from Russia. The lists of sanctioned entities, persons, or items maintained by regulators might be exclusive or only meant to serve as guidelines to more specific legal definitions.

Classify your products

Identify potential exposure by categorizing materials and technologies, often defined by HS codes. Implement a systematic process in your ERP to flag dual-use or regulated items. Pay special attention to automotive components, communications, navigation, sensors, semiconductors, and electronic equipment, even if the products don’t have an explicit dual-use designation.

Screen your partners

Mitigate risks from customers and distributors reselling to Russia by including re-export, end-use, and end-user clauses in agreements. Emphasize a zero-tolerance policy for sanctions evasion. Use screening solutions that

integrate with your ERP for real-time checks against sanction lists, ensuring a hard stop for any matches. Features such as approximate search, search by address, as well as translation/transliteration of company names are essential when choosing the screening solution. If screening manually, ensure robust documentation, and flag companies with shared addresses or partial ownership with entities of concern.

Address conflict of interest

Separate the sales and due diligence roles to prevent conflicts of interest. If not possible, implement a four-eyes principle for reviewing due diligence and screening documentation. The legal officer should oversee trade compliance and control networks in regional branches. Pay special attention to hubs for sanction circumvention, such as China, Hong Kong, Turkey, UAE, and Taiwan.

Train your team

Educate your team on critical components and battlefield goods that could end up in Russia, common red flags, and sanction evasion practices. Stress the leadership's complete dedication to upholding both the ethical and legal aspects of export controls and sanctions compliance. A lackluster approach from top management could undermine the entire compliance structure, leading employees to prioritize paperwork over a genuine and careful approach to reducing risks and protecting the business. Deliberately avoiding information, failure to resolve a red flag or an escalated concern within the company may be seen as aggravating circumstances by the export controls investigators.

Develop your compliance program

Enhance your compliance process by sequentially building upon these key objectives:

1. **Contractual Language**: Incorporate export controls compliance clauses into contracts and secure written certifications of end-use and end-user.
2. **Internal Training**: Conduct regular and simple training sessions on red flags to foster a culture of vigilance and encourage reporting of concerns.
3. **Partner Screening**: Use automated solutions or manual searches for business partner screening. Avoid conflicts of interest and maintain a clear audit trail.
4. **Building Relationships**: Meet with counterparties in person and develop market knowledge. Report legitimate compliance concerns about competitors to level the playing field.

Each step builds upon the previous one, creating a comprehensive and effective compliance program. While automation and data tools can improve efficiency, the educated judgment and case-by-case analysis by your team are essential to prevent major control failures.

KSE | Institute

Red Flags and Risk Mitigation

Learn patterns of evasion and misdirection to spot bad faith actors and protect your business.

Documentation

- Sales supporting documents (invoices, letters of credit) do not list the actual end-user.
- A customer or re-seller refuses to disclose details to banks, shippers, or third parties.
- Customer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for reexport.
- Bank account number has a country code different from the customer's country.
- Payment details change last-minute to exclude the country or entity of concern.
- After being declined the sale, the customer or re-seller comes back as another entity.

Business model

- Customer has little or no business background, or a recently registered company.
- Ownership structure is not transparent or atypical; minimal share capital.
- Product or software sold is not in line with the customer's line of business.
- Customer is overpaying for a product and/or pushes for urgent delivery.
- Customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- If the product is being paid for or received by a different party, does their relationship make sense?
- Customer is unfamiliar with the product's performance characteristics but still wants the product.
- Product is not in line with the technological level of the country of the end-user, e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- Customer claims to be a manufacturer but has no apparent production facilities (e.g. it is extremely rare to have manufacturing in Hong Kong).
- Search result by alleged address of production facilities look like an office building.
- Routine installation, training, or maintenance services are declined by the customer.

Shipping

- A freight forwarding firm, or virtual company or secretary service provider, is listed as the product's final destination.
- Atypical or illogical shipping routes to reach a destination, e.g. shipping through Hong Kong or Dubai where a more direct route is available.
- Packaging is inconsistent with the stated method of shipment or destination.

Communications and web presence

- Phone numbers' country codes don't match the destination country.
- Map search by address returns locations at or nearby military facilities.
- Entity has no web presence and/or no corporate domain for email accounts (using gmail, hotmail, qq, etc instead).
- English and Chinese language versions of the company website are vastly different in content.
- No company website, or a website only in Russian.
- Website of an alleged Chinese company does not have the MIIT ICP Recording Number on the page.

Conclusion: Fostering the Culture of Compliance

The best defense against the rising tide of risks associated with export controls and sanctions is to foster a culture of vigilance within your company. Leadership's commitment, or the "tone at the top," is paramount in setting the standard for compliance and ethical conduct. It is crucial to educate your team about red flags and evasion patterns to avoid finding your company in the precarious position of explaining to concerned stakeholders and state agents why your components were discovered in Russian weaponry or in the aftermath of strikes on civilian targets in Ukraine and globally. Vigilance, leadership, and knowledge are the cornerstones of a robust compliance strategy that not only protects your company legally and reputationally but also contributes to global peace and security. Proactive compliance and a robust internal control framework are not just legal necessities, they are fundamental to maintaining the integrity and reputation of your business in the challenging terrain of international trade.