The new Russia sanctions: Five actions for sanctions and export-control teams

By Steven Brotherton, Principal, Tax, KPMG LLP
and Jason Rhoades, Senior Manager, Tax, KPMG LLP

The Russian government's invasion of Ukraine has prompted economic sanctions and new export restrictions that could affect a range of U.S. companies. These measures include sanctions targeting Russian and Belarussian individuals and entities, additional end-use requirements for dual-use items and technology, and additional country-specific export control requirements. The Department of the Treasury's Office of Foreign Assets Control (OFAC) promulgates sanctions, and the Bureau of Industry and Security (BIS) administers Export Administration Regulations (EAR) which regulates trade in dual-use items and technology.

Between February 22 and March 7, 2022, OFAC issued 245 new Specially Designated National (SDN) listings against Russian and Belarussian individuals and entities. Seven Russian banks have been removed from SWIFT, the mechanism that allows banks to communicate with each other. In addition to the SDN designations, OFAC took advantage of one of its newer sanctions programs, the Non-SDN Menu-Based Sanctions, to designate numerous other entities for restrictions less severe than those that come with an SDN designation.

For dual-use items and technology, BIS has issued broad prohibitions on export of items controlled under the EAR's Commerce Control List categories 3–9. Further, foreign-made items incorporating U.S. technology may be subject to licensing requirements, and there are expanded end-use prohibitions for exports to Russia and Belarus. Additional details about these actions can be found here, here, and here.[1]

While these sweeping measures seem daunting for compliance professionals, the key is understanding what activities are regulated and how they impact your company. In this briefing paper we review the key activities:

- Supporting executive leadership with understanding business implications
- Identifying risk through data analysis
- Communicating effectively with internal and external stakeholders
- Validating and updating the company's sanctions and export-control automated screening system for efficiency and accuracy
- Updating the company's sanctions and export controls risk assessment and ensuring the implementation of appropriate mitigating controls

Support executive leadership

Top leaders of corporations everywhere are undoubtedly meeting to discuss the implications of the Russia-Ukraine war. Ensuring that sanctions and export compliance teams are in these discussions will help leaders identify the full scope of the impact to the business.

These new regulatory measures are intentionally broad, targeting almost every aspect of Russian business. It takes an expert to provide the proper context for measure. Among other things, sanctions and export-compliance professionals can highlight how supply chain operations are impacted, how sales are affected through new export control and sanctions requirements, and how sanctions might even impact paying employees or even lead to moving operations.

The sanctions and export compliance team is a facilitator that can identify the new rules; provide detailed analysis of potential impacts; and think through the short-, medium-, and long-term implications of any proposed solutions. The team will also understand systems limitations, which can either enhance or limit compliance (and suggest workarounds, as needed).

[1] More general information can be found here.

Know the facts

Systemic, long-term compliance with new regulations requires regular data analysis. Sanctions and export-compliance professionals must start by identifying the data needed to assess and analyze the company's risk posture, and suggest risk-mitigation measures. Relevant data for assessing risks include information about products, sales opportunities, payment platforms, and export authorizations. A comprehensive compliance program can't be developed without a total review of the company's operations.

With the required data in hand, the sanctions and export-compliance team can determine where mitigation efforts should be directed. It can also provide the business with specific information about the ramifications of new sanctions and export-control requirements. Mitigation measures can be highly targeted to prevent unauthorized activities while limiting the impact to other business groups or operations.

When going through this process, the compliance team should document gaps in its data collection. Most frequently, these arise when there are multiple enterprise resource planning (ERP) systems or when transactions occur entirely outside of an ERP in effect hiding potentially unauthorized activities. Another challenge may be systems that are not integrated (where personnel are performing activities with export implications across multiple systems). If these systems do not "talk" to each other, it can be difficult to identify an error or risk. It is important to note that government regulators generally expect technologically sophisticated companies to have sophisticated automation platforms to support compliance. Failure to appropriately manage data may be viewed as an aggravating factor in the event of a violation.

Communicate the message

The company should communicate its ongoing commitment to compliance. However, stakeholders should carefully consider how information will be presented to internal and external parties.

Employees should understand that the company may impose more stringent compliance measures immediately, while the organization assesses its unique risk factors. This may include a review of every transaction involving a Russian entity, regardless of the nature of the relationship. However, employees should also know that these measures may be modified once the company has a more thorough understanding of its risk posture. The message should emphasize that each employee is responsible for compliance. And leaders should acknowledge the importance of flexibility in the coming months. A regular communication cadence should be established coupled with periodic training.

Companies will also need to communicate with potentially impacted third parties, such as distributors, suppliers, banks, and logistics providers. Each should be engaged directly with tailored communications and every party should understand the company's expectations for their compliance. Further communication may include providing clarity about whether relationships will continue, new procedures or limitations will be adopted, and who will be the point of contact for future discussions or questions. Additionally, prior to communicating a change to the relationship, a thorough contract review should be performed to identify liability that might be incurred if a contract is terminated or modified. If the relationship will continue, the company should anticipate being engaged in the third party's activities and should drive compliance with their partner.

For both internal and external groups, communications from senior stakeholders provide an opportunity to alleviate concerns while providing direction. Frustration around new compliance activities or terminating business opportunities can be best mitigated by regular engagement with senior leaders.

Validate automated tools

Once the universe of at-risk activities has been established, a thorough system review should be conducted. The compliance team should evaluate the automated Restricted Party Screening (RPS) system to confirm that it is calibrated to flag potentially prohibited transactions and parties. This review should include a deep dive into customers, but must also include non-customer relationships that could be subject to sanctions or export controls.

Screening master data is an additional step to fortify compliance. This will include screening for newly sanctioned parties as well as the more complicated task of identifying the cities in the Donetsk People's Republic and the Luhansk People's Republic regions that are now sanctioned. Using open-source data, the compliance team should identify those cities then validate that the RPS tool will alert them to potential transactions with parties from those areas.

The export-compliance team should also validate that license information is accurate, regardless of whether an automated system is used. This includes examining the process for license decrements, provisos, and expiration dates. Where only manual processes are in place, such as tracking licenses via spreadsheet, careful guidance should be issued to prevent version control

issues, validate formulas, and set calendar notifications when a license is nearing expiration. In either scenario, discussions with the business should begin early to develop mitigation strategies in the likely event of a license denial or revocation.

The most effective approach for sustained compliance is through routine risk assessments that identify specific risk drivers. Sanctions-focused risk assessment should be framed through the touchpoint inventory, which identifies third-party relationships—specifically products, services, geographic footprints, customer bases, and transaction types—to pinpoint potential compliance challenges. Once this is in place, a risk and control matrix (RACM) should be developed using the results of the touchpoint inventory. The RACM identifies key risks, quantifies them, and provides a risk rating for compliance teams. For companies with items or technology subject to the new export-control requirements, the RACM should additionally include an updated evaluation of export controls. This step is as important as the sanctions evaluation because products that were previously only lightly controlled now may be subject to broader licensing requirements. While a comprehensive review takes significant planning, a well-run risk assessment will enable the export compliance team to develop a targeted strategy that prevents violations.

Looking ahead

It is impossible to predict how the trade environment will change in the coming months. Given this uncertainty, export-compliance teams should elevate their visibility across the organization. This includes contributing to senior stakeholder meetings, gathering and analyzing export data, developing targeted mitigation strategies, and effectively communicating with internal and external stakeholders. While the sanctions and export controls are sweeping, a methodical approach to managing them will help preserve compliance.

Contact us

Steven Brotherton
Principal, Tax
M: 415-271-0827
E: sbrotherton@kpmg.com

Jason Rhoades
Senior Manager, Tax
M: 571-695-5040
E: jrhoades@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.