Guidepost

IS YOUR RUSSIA–UKRAINE AND OVERALL SANCTIONS COMPLIANCE PROGRAM REALLY WORKING? (DON'T FIND OUT THE HARD WAY)

How do you know if your sanctions compliance program ("SCP") is ***really*** working? Can your firm really afford to find out the hard way – violations with major penalties, especially after regulators uncover your management did not sufficiently invest in the right people, processes, and/or technologies to filter, freeze, and report targeted assets?

As we witness the Russian military assault in (and tremendous courage of) Ukraine, and its citizens, the West is responding with major financial sanctions to freeze assets and payments against Russian entities, activities, and individuals including President Putin. Additionally, SWIFT prohibitions against selected Russian banks are now in place, to further reduce money flows for Russia and its agent states.

- What if your firm's controls are "wobbly at best" to identify, filter, freeze, block, and report transactions involving these targeted Russian assets?
- Indeed, what if your controls are found to be the "***weakest link***" in the interconnected financial front against Russia, enabling it to evade these sanctions? And what if your firm is flat-footed to patch these holes?

Unfortunately, Now is NOT the Right Time to Health-Check Your SCP

Your compliance and operations staff are likely stressed and over-worked because they've worked 24/7 to execute these sanctions – and are on call for the next round(s) against Russia. Indeed, your SCP program should always be in robust health because you and your company should be benchmarking and adapting continuously against leading- and expected compliance practices.

OFAC's Five Components of an Effective Sanctions Compliance Program

As a reminder, the US Treasury Office of Foreign Assets Control ("OFAC") issued its "Framework for OFAC Compliance Commitments" in May 2019 . It's important to benchmark against the framework's five key components: (1) management

commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

Management commitment is the most important.

1. Management Commitment

Isn't this always the case, and hopefully not a surprise, how important management commitment and culture is – especially to OFAC and other regulators which discover, investigate, and then enforce major penalties for sanctions violations. Easy to say, very difficult to demonstrate the right culture.

OFAC expects senior management to:

- Review and formally approve your SCP
- Ensure compliance teams possess sufficient authority and autonomy to deploy your SCP procedures, with direct reporting lines between the SCP function and senior management
- Fund compliance with adequate resources (human capital, expertise, information technology customized to your operations, markets, and other factors affecting your company's overall risk profile)
- Live and breathe a "culture of compliance", including whistleblower processes, and reporting, without retaliation; and disciplines for misconduct and prohibited activities
- Demonstrate prompt corrective action over apparent OFAC and other violations – and report these voluntarily to OFAC and others
- Address the root causes of past apparent violations with systemic solutions

If your firm is global, are your filtering tools and processes enabling you to globally filter, block, and report consistently, fully and timely? What if your SCP program and tools work well in one geography, but not universally, unintentionally allowing Russian (or other) assets to slip through?

2. Risk Assessment

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to OFAC and other violations, negatively affect your reputation and worse, enable evasion. Take a risk-based approach when designing or updating a SCP. Ongoing "risk assessments" should identify potential OFAC issues and should drive your SCP procedures, internal controls, and training to mitigate such risks.

Risk assessment examples include: (i) customers, supply chain, intermediaries, and counterparties; (ii) your products and services, including how and where they fit into other financial or commercial products, services, networks, or systems; and (iii) how the interaction of (i) and (ii) can exacerbate these risks further.

3. Internal Controls

Effective SCPs include internal controls, such as policies and procedures to identify, interdict, escalate, report, and keep records pertaining to prohibited activity by OFAC and others. Internal controls to outline clear expectations, define procedures and processes (including reporting and escalation chains), and minimize the risks identified by your sanctions risk assessments.

For example, are roles crystal clear for your 1st line operations, businesses, 2nd line compliance, and management so that decisions to block, freeze and report Russian (or other) assets are time-critically met? What if they're not? How would you know?

4. Testing and Auditing

Compliance and internal audits assess the effectiveness of current processes and check for inconsistencies between these and day-to-day operations. Objective testing of your SCP ensures you can identify program weaknesses and deficiencies, especially software, systems, and other technology. And you must remediate any identified compliance gaps promptly and fully across your enterprise.

5. Training

Like many other compliance requirements, training for employee awareness and execution is critical. Violations due to lack of awareness is inexcusable and can be fatal.

I've seen the good, the bad and the ugly of sanctions and other compliance programs over intensely stressful times in the world. Iraq invading Kuwait; 9/11; the fallout, remediation, and transformation from painfully expensive sanctions penalties; the Russian incursion into Crimea; and now Ukraine.

ERIC YOUNG

Senior Managing Director

Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks. Throughout his career, Mr. Young has remediated and transformed corporate compliance programs and financial crime compliance programs including sanctions; integrated compliance and ethics cultures between regions, countries and companies to ensure consistency across enterprises; built compliance budgets; enhanced reporting; created governance frameworks and risk assessment, monitoring and testing programs; closed compliance gaps; restructured compliance teams; and mentored junior staff to create a pipeline of future compliance leaders and enable grassroots compliance ideas, solutions and digital upgrades.