

Report on Supply Chain Compliance Volume 2, Number 12. June 27, 2019

An introduction to US Treasury Dept.'s new guidance on building a sanctions compliance program

By Sascha Matuszak

RSCC has previously reported on the United States Department of Treasury's Office of Foreign Assets Control's (OFAC) guidance on sanctions compliance, primarily on the concept of extraterritorial jurisdiction as it relates to secondary sanctions. And on May 2, OFAC published "A Framework for OFAC Compliance Commitments," which focuses on the critical components of a sanctions compliance program and provides clear guidelines for how that program should look.

"OFAC, for the first time, has framed the elements of a sanctions compliance program, in a bevy of ways mirroring many of the tenets of the anti-money laundering (AML) compliance program," wrote the authors of a Steele report on the guidance. "This includes prongs such as crafting stout internal controls, engaging in proactive OFAC risk assessments, adequately training and arming staff with knowledge and resources and testing and auditing systems and their human decision-makers to ensure systemic vulnerabilities are closed quickly."

The five essential components listed in the guidance are: Management commitment, risk assessment, internal controls, training, and testing and auditing. According to the guidance, management commitment is "essential in ensuring the [sanctions compliance program] receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization."

What OFAC is looking for here is a clear and documented demonstration of support and effort from the executive suite and the board of directors. The support and effort should enable the compliance program to communicate its purpose throughout the organization, have the authority to put a stop to certain activities when red flags appear, and be able to bypass the executive suite to communicate directly to the board if necessary. The guidance gives specific examples and steps that management should take in order to meet OFAC requirements.

OFAC describes the risk assessment component as "informing the [sanctions compliance program's] policies, procedures, internal controls, and training ..." The guidance gives examples of the types of risk that organizations should be looking at, including "(i) customers, supply chain, intermediaries, and counter-parties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counter-parties. Risk assessments and sanctions-related due diligence is also important during mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations."

The OFAC guidance calls for policies and procedures that monitor, among other things: updates to OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List), the Sectoral Sanctions Identifications List (SSI List), and other sanctions-related lists; and new, amended, or updated sanctions programs or prohibitions imposed on targeted foreign countries, governments, regions, or persons, through the enactment of new legislation, the issuance of new Executive orders, regulations, or published OFAC guidance or other OFAC actions.

These internal controls must not only effectively monitor the many changes of the OFAC sanctions regimes, but also be able to communicate changes in policy and the corresponding compliance responsibilities across the organization.

Regarding OFAC's definition of the roles of testing and auditing:

A comprehensive, independent, and objective testing or audit function within an SCP ensures that entities are aware of where and how their programs are performing and should be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment, as appropriate. Testing or audit, whether conducted on a specific element of a compliance program or at the enterprise-wide level, are important tools to ensure the program is working as designed and identify weaknesses and deficiencies within a compliance program.

This is typically done by a third party or group outside of the sanctions compliance program "that can review both sanctions screening inputs and outputs and scrutinize the decisions of staff to ensure potential hits are analyzed, escalated and dispositioned. Institutions should consider sanctions review teams with deep law enforcement and federal investigations experience — even former OFAC staff."

The guidance states that "training ... is an integral component of a successful [sanctions compliance program]," and should be able to: "(i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments."

What a good sanctions compliance program needs

In a recent webinar introducing the basics of OFAC and the many sanctions regimes it runs, Robert J. Ward, Jr., Director of Trade Compliance at WESCO International, Inc., outlines several tools that organizations can utilize to help ensure compliance with OFAC's regulations, including screening tools, risk assessment procedures and ideas for training.

Ward wrote, "A 'Best in Class Screening Practice' is one that is fully automated and internalized in the company's enterprise resource planning system, including an automated block imposed for potential blacklist matches. ... Even for companies with a limited budget but poised to launch globally, OFAC provides an updated screening tool link on its website at no cost"

He recommends several tools, including [OFAC's Sanctions List Search](#) and [OFAC Analyzer](#).

Ward also challenges compliance officers to ask a series of questions regarding the program they're building and some of the risks the organization faces. Below are just a few of the questions:

- Do you do business with third parties in known transshipment cities, such as Dubai, Hong Kong, Istanbul or Singapore?
- Is your industry known for involvement in countries neighboring embargoed countries where diversion could easily occur?
- Do you have sensitive goods, technologies and services with both civilian/military dual-use applications?
- What is your process for intervention if and whenever needed? Stop order? Is it effective?

- What is your standard for gauging a false positive versus a match when screening for aliases?
- Can you independently verify ownership?
- If not or if inadequate info is provided, are transaction stops imposed?

These questions are just some of the more important ones that a compliance officer needs to be able to answer. The stakes are very high, in a volatile world in which sanctions can be applied at any moment, and enforcement agencies have ramped up investigations — and penalties — to historic heights. It behooves any organization to take a close look at the OFAC guidance and consider what needs to be done to mitigate risks and avoid issues in a complex, interconnected world.

Takeaways

- Sanctions are being enforced more vigorously, especially by the U.S., and companies need to establish policies and procedures that can mitigate the risk of sanctions violations
- The OFAC guidance released earlier this year is an excellent resource for companies looking to establish a sanctions compliance program – compliance officer should monitor OFAC for updates and clarifications to the guidance.

This publication is only available to subscribers. To view all documents, please [log in](#) or [purchase access](#).

[Purchase Login](#)