Davis Polk

OFAC Publishes Guidance on Sanctions Compliance Programs

May 7, 2019 | Client Update | 5-minute read

On May 3, 2019, the Treasury Department's Office of Foreign Assets Control ("**OFAC**") published ***A Framework for OFAC Compliance Commitments*** (the "**Compliance Framework**"), a guidance document that sets forth OFAC's views of the essential elements of an effective economic sanctions compliance program ("**SCP**"). OFAC encourages, but does not require, organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States or U.S. persons, or that use U.S.-origin goods or services, to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating an SCP.

The publication of the Compliance Framework represents a notable change in approach by OFAC. While the agency has **long encouraged** the adoption of risk-based SCPs, and has treated the existence and adequacy of an SCP as a key part of its analysis of enforcement cases under the **Economic Sanctions Enforcement Guidelines**, 31 C.F.R. Part 501, Appendix A, OFAC has generally not provided detailed prescriptive guidance on the form or content of an SCP. However, following a December 2018 **speech** by Under Secretary for Terrorism and Financial Intelligence Sigal Mandelker, OFAC began incorporating specific compliance undertakings into **settlement agreements resolving enforcement cases**, and has now made clear through the publication of the Compliance Framework that those undertakings reflect OFAC's generally applicable expectations for an effective SCP.

Substantively, the Compliance Framework is broadly consistent with existing standards for SCPs applicable to federally regulated financial institutions set forth in the Federal Financial Institutions Examination Council's **BSA/AML Examination Manual**. As explained in the Compliance Framework, an effective SCP should address the following five elements:

- **Senior Management Commitment:** An organization's senior management should demonstrate commitment to, and support of, the organization's risk-based SCP, including by: (i) reviewing and approving the SCP; (ii) ensuring that compliance units have sufficient authority and autonomy to implement the SCP, including direct reporting lines to senior management; (iii) ensuring that adequate resources, including technology and human capital, are dedicated to the compliance function in a manner commensurate with the company's sanctions risk; (iv) promoting a "culture of compliance;" and (v) taking seriously and appropriately responding to apparent violations of law or identified SCP deficiencies.
- **Risk Assessment:** An organization should conduct an OFAC risk assessment in a manner and with a frequency that accounts for potential sanctions risks relevant to its business. Such risks could be posed by clients and customers, products, services, supply chain, intermediaries, counter-parties, transactions, and geographic locations, depending on the nature of the organization, and should be addressed both in the context of ongoing business activities and mergers or acquisitions. The organization should develop a methodology to identify, analyze, and address the particular risks it identifies, and update the risk assessment to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.
- **Internal Controls:** An organization should implement risk-based internal controls tailored to its business and sanctions risk in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that is prohibited by the sanctions programs administered by OFAC. Among other things, these controls should be flexible enough to respond to rapidly changing sanctions developments.
- **Testing and Auditing**: An organization should employ a comprehensive, independent, and objective testing or audit function to assess whether its SCP is performing effectively or needs to be updated, enhanced, or recalibrated to

account for a changing risk assessment or sanctions environment. In particular, the organization should ensure that negative audit findings are appropriately addressed, including by taking immediate and effective action, to the extent possible, to identify and implement compensating controls until root causes of the deficiency can be determined and remediated.

– **Training:** Training should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (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.

In an Appendix, the Compliance Framework also identifies a number of "root causes" of SCP breakdowns or deficiencies, compiled from recent public enforcement cases, to assist organizations in identifying and correcting certain issues that OFAC has seen contribute to sanctions violations in the past. These include:

– Absence of a formal SCP.

– Failure to understand (or active disregard of) OFAC's regulations or the scope of OFAC's jurisdiction. Among other things, such failures have included: (i) not recognizing the applicability of OFAC sanctions requirements based on status as a U.S. person or a U.S.-owned or controlled subsidiary (in the Cuba and Iran programs); (ii) non-U.S. persons not understanding that they must comply with sanctions in connection with their dealings in or with U.S. persons, the U.S. financial system, or U.S.-origin goods and technology; and (iii) failure on the part of U.S. companies to understand that sanctions prohibitions extend to conduct that facilitates dealings between an organization's non-U.S. locations and OFAC-sanctioned countries, regions, or persons.

– Failure to appropriately update or calibrate sanctions screening software or filters.

– Improper or incomplete due diligence on customers, supply chain, intermediaries, or counter-parties.

– Decentralized or inconsistently applied SCPs.

– The use of non-standard payment or commercial practices.

The Appendix also emphasizes the possibility of individual liability for employees, particularly in supervisory, managerial, or executive-level positions, that play integral roles in causing or facilitating sanctions violations. It remains the case that OFAC has rarely taken enforcement action against individuals in cases involving violations by an organization, but it did recently **name an individual** to the Foreign Sanctions Evaders ("**FSE**") List in connection with **sanctions violations** caused by the individual in his capacity as managing director of a Turkish subsidiary of a U.S. company.

As noted, the Compliance Framework does not impose any legal requirements on U.S. persons or persons doing business in the United States. However, it does set out standards that OFAC will apply in evaluating the adequacy of an SCP under its Enforcement Guidelines, and that will likely inform expectations of other regulators and of financial institutions in certain contexts, such as lending or underwriting. Companies with an existing SCP may wish to use the publication of the Compliance Framework as an opportunity to assess the program's adequacy and consistency with OFAC's recommendations; those without a formal SCP may wish to take the opportunity to conduct a risk assessment to determine whether implementing one is necessary in light of the company's sanctions risks.

View as a PDF

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

John B. Reynolds III
+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa
+1 202 962 7129
will.schisa@davispolk.com