



Regulatory Alert

Regulatory Insight Center



May 2019

OFAC Framework for Sanctions Compliance Programs

Continued focus on effective compliance programs.

Key points

- The Department of the Treasury's OFAC released a framework for sanctions compliance that is applicable to U.S. organizations and foreign entities doing business in or with U.S. parties or goods and U.S. persons.
- The framework strongly encourages organizations to develop, implement and routinely update a Sanctions Compliance Program that includes five (5) essential components: management commitment, risk assessment, internal controls, testing and auditing and training.
- The publication also outlines several root causes that have led to violations of sanctions in the past.

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities in accordance with national security and foreign policy goals and objectives.

OFAC has released a [Framework for OFAC Compliance Commitments](#) (Framework), which outlines what OFAC believes to be the essential components of a sanctions compliance program (SCP). The framework applies to organizations subject to U.S. jurisdiction, and foreign entities operating in or with the U.S., U.S. persons, or using U.S.-origin goods and services. This is the first time OFAC has issued guidance setting forth how it evaluates an SCP framework. OFAC strongly encourages organizations to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating an SCP.

OFAC outlines five essential components for an SCP, including:

1. **Management commitment.** "Management" is defined broadly as including senior leadership,

executives, and/or the board of directors. Effective senior management support includes:

- **Review and approval** of the SCP.
- Delegation of **sufficient authority** and **autonomy** to compliance units to deploy its policies and procedures, with direct reporting lines between the SCP Function and senior management with a regular cadence of meetings.
- Allocation of **adequate resources** (human capital, expertise, IT and other resources) to the compliance units, including a dedicated OFAC sanctions compliance officer.
- Promotion of a "**culture of compliance**," including through an ability to report misconduct without fear of reprisal, senior management messaging, and SCP oversight of actions.
- Demonstrated recognition of compliance failings and implementation of necessary measures to reduce future occurrences, including through addressing **root causes** and implementing **systemic solutions**.



2. **Risk assessment.** The assessment exercise should generally consist of a holistic review of the organization from top-to-bottom and an assessment of its external touchpoints where the organization may potentially, directly or indirectly, violate sanctions.
 - The assessment may include risks posed by **clients, customers, products, services, supply chain, intermediaries, counterparties, transactions, and geographic locations**. The risk assessment should be updated to account for the root cause of any violations or systemic deficiencies identified.
 - Assessments should **inform** the extent of **due diligence** to be conducted at various points in a relationship or in a transaction, such as at onboarding or merger and acquisition activity.
 - A developed risk assessment methodology should identify, analyze, and address particular risks, and be **updated to account for** the conduct and root cause of any **violations** or systemic deficiencies identified.
3. **Internal controls.** The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance (including reporting and escalation chains), and minimize the risks identified by risks assessments. In particular, the organization's internal controls should include:
 - **Policies and procedures** that outline the SCP, and capture the organization's day-to-day operations and procedures; designed to prevent misconduct.
 - Internal controls that enable the organization to clearly and effectively identify, interdict, escalate, and report potentially prohibited transactions and activities.
 - Use of internal and/or external audits, including to reinforce policies and procedures.
 - Recordkeeping policies and procedures that account for its sanctions requirements.
 - Processes to take immediate and effective action, as possible, to identify and implement compensating controls until a root cause is determined and remediated.
 - **Clear communication** of its policies and procedures to all relevant **staff** including gatekeepers, and **business units** operating in high-risk areas as well as **external parties** performing on behalf of the organization.
 - Personnel to integrate SCP's policies and procedures into daily operations.
 - To the extent technology solutions are part of an organization's internal controls, solutions should be calibrated to the organization's risk profile and compliance needs, and routinely tested.
4. **Testing and auditing.** Testing and auditing ensures organizations are aware of where and how their programs are performing, and should be updated or recalibrated to account for changing risk assessments or sanctions environments. An organization should commit to ensuring:
 - The testing or audit function is **accountable** to senior management, **independent** of the audited activities and functions, and has **sufficient authority, skills, expertise, and resources**.
 - Testing and audit procedures are appropriate to the level and sophistication of the SCP and the assessments are objective.
 - Confirmed **negative testing results** or audit findings pertaining to an SCP are **addressed immediately** and action is taken to identify and implement compensating controls until the root cause is determined and remediated.
5. **Training.** The training program should be provided to all appropriate employees at least annually and should accomplish the following: i) provide job-specific knowledge, ii) communicate sanctions compliance responsibilities, and iii) hold employees accountable for training. Further, a training program should:
 - Provide **adequate** information and instruction to employees and stakeholders (e.g., clients, suppliers, business partners, and counterparties), with tailored training for high risk employees.
 - Be appropriate for the scope of the organization's products and services; customers, clients, and partnerships; and geographic regions.
 - Have a frequency that is appropriate for the organization's risk assessment and risk profile.
 - **Use negative testing results** or audit findings, to provide corrective training or other corrective actions.
 - Include easily accessible resources and materials, available to all applicable personnel.

OFAC notes that some common compliance program breakdowns can be tied to root causes that include, the lack of a formal OFAC SCP, misinterpretation or failure to understand the applicability of OFAC regulations, facilitating transactions by non-U.S. persons (including through or by overseas subsidiaries or affiliates), limitations in sanctions screening software or filters, improper due diligence of customers or clients, decentralized compliance functions and inconsistent application of SCPs, and senior level employee misconduct.

KPMG Perspectives

Sanctions compliance is a fundamental element to an overall well-functioning ethics and compliance program. The establishment of a framework by OFAC reiterates its importance and sets forth minimum expectations in the five core areas of: management commitment, risk assessment, internal controls, testing

and auditing, and training. While not new areas, this issuance clearly denotes the importance of the development, implementation, and continuous improvement of sanctions compliance. Importantly, the OFAC Framework is intended to span across not just customers but also to supply chains, intermediaries, and all counterparties. As such, all organizations should look to enhance sanctions compliance both within their organization but as well to their supply and distributor providers. OFAC denotes that a strong sanctions compliance program may be a mitigating factor in assessing penalties.

The OFAC guidance aligns with the Department of Justice's (DOJ) expectations for effective corporate compliance and ethics program which was separately issued.

For additional information please contact [Teresa Pesce](#) or [Stephen Marshall](#).

Amy Matsuo
Principal and National Lead
Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Contributing authors:
Amy Matsuo, Principal and National Lead,
Regulatory Insights

Karen Staines, Director, Financial Services
Regulatory Insight Center

Nicole Stryker, Director, Advisory

kpmg.com/socialmedia



All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. NDPPS 592774