Updates
May 07, 2019
OFAC Issues Sanctions Compliance Program Guidance

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

OFAC had not previously published guidance addressing essential elements for an effective sanctions compliance program (SCP). It has now done so. Specifically, on May 2, 2019, OFAC published such guidance, entitled "A Framework for OFAC Compliance Commitments" (OFAC Framework).

OFAC Framework and Its Enforcement Guidelines

The OFAC Framework clearly establishes the agency's expectations regarding an effective SCP. Given the importance that OFAC places on an effective SCP in its enforcement decisions, including the determination of the amount of any civil penalty, a company with international activities should consider whether to update its SCP to meet OFAC's standards.

OFAC recognizes that a risk-based SCP will vary depending on a variety of factors, including the company's size and sophistication, products and services, customers and counterparties, and geographic locations. The agency, however, states that each SCP program should incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training. The OFAC Framework addresses each of these five components in detail.

Further, the agency reiterated that its Economic Sanctions Enforcement Guidelines (Guidelines) consider the existence of an effective SCP at the time of the violation as a critical mitigating factor and that, in appropriate cases, OFAC may consider the existence of an effective SCP at the time of an apparent violation in determining whether a case is deemed "egregious." Under the Guidelines, an OFAC determination that an apparent violation is non-egregious generally results in a substantial reduction in the civil monetary penalty. The agency indicates that an SCP that fully incorporates the OFAC Framework will be the most likely to result in mitigation under the Guidelines.

The OFAC Framework contains an appendix that identifies ten root causes of sanctions violations. The agency recommends that all entities subject to U.S. jurisdiction review the settlements published by OFAC and reassess and enhance their SCPs as appropriate.

Five Components of Compliance

The OFAC Framework addresses each of the five components of compliance. We outline below the agency's key points about each component.

1. Management Commitment

OFAC identifies senior management commitment as a critical factor in determining the success of the SCP. This factor includes the following elements:

- Senior management has reviewed and approved the organization's SCP.

- Senior management ensures that its compliance unit has the requisite authority and autonomy and provides a direct reporting line between the SCP function and senior management.
- Senior management ensures that the compliance unit receives adequate resources commensurate with the company's overall risk profile, including:
    - Appointing of a dedicated OFAC sanctions compliance officer.
    - Ensuring that the company's SCP personnel have knowledge of and expertise with OFAC's regulatory scheme and the ability to apply OFAC's requirements to complex financial and commercial activities.
- Senior management promotes a "culture of compliance" throughout the company, including:
    - Allowing personnel to report sanctions misconduct to senior management without fear of reprisal.
    - Discouraging prohibited activities and highlighting the potential repercussions of noncompliance with OFAC sanctions.
    - Providing SCP oversight over the entire organization for the purposes of compliance with OFAC sanctions.
- Senior management demonstrates recognition of the seriousness of apparent violations of OFAC requirements or failures to comply with the SCP's requirements.
- Senior management implements necessary measures to reduce future violations, including addressing the root causes of past apparent violations and systemic measures.

2. Risk Assessment

Risks in sanctions compliance are potential threats that, if ignored, can lead to sanctions violations. OFAC recognizes that there is no "one size fits all" risk assessment but indicates that it should include a review of the entire organization and an identification of potential areas in which it engages with sanctioned persons, countries, or regions. This potentially could include an assessment of the following: (1) customers, supply chain, intermediaries and counterparties; (2) the products and services that the company offers; and (3) the geographic locations of the company and its customers, supply chain, intermediaries and counterparties.

- The company should conduct its risk assessment in a manner, and with a frequency, that adequately accounts for potential risks and the root causes of any deficiencies identified by the company. The assessment should leverage existing information, and the risk assessment generally should inform the extent of due diligence efforts at various points in a relationship or in a transaction, including on-boarding of customers and mergers and acquisitions.
- The company should develop a methodology to identify, analyze and address the identified risks. The risk assessment should be updated to account for any apparent violations or systemic deficiencies identified by the company.

The annex to the Guidelines provides a risk matrix that companies can use to evaluate their compliance programs.

3. Internal Controls

An effective SCP should include internal controls in order to identify, interdict or report apparent violations and maintain pertinent records. The internal controls should outline expectations, define OFAC compliance procedures (including reporting and escalation chains) and minimize risks identified by risk assessments. The internal controls should reflect updates to OFAC's lists of sanctioned individuals and entities; new prohibitions imposed on targeted foreign countries, governments, regions or persons by the U.S. government; and changes to general licenses issued by OFAC. Additionally, the company should:

- Have written policies and procedures that are relevant to the organization, capture the company's daily operations, are easy to follow and are designed to prevent employee misconduct.

- Implement internal controls that adequately address the results of its OFAC risk assessment and enable the company to identify and to report activity prohibited by OFAC.
- Select and calibrate information technology solutions that address the company's risk profile and compliance needs and routinely test these solutions to ensure their effectiveness.
- Review its OFAC procedures through internal and/or external audits.
- Maintain recordkeeping procedures that account for OFAC's requirements.
- Upon learning of a weakness, take immediate and effective action to implement compensating controls until the root cause of the weakness can be remediated.
- Clearly communicate the SCP's procedures to all relevant staff, including gatekeepers and business units operating in high-risk areas, and to external parties performing SCP procedures on behalf of the company.
- Appoint personnel to integrate the SCP's procedures into the company's daily operations.

4. Testing and Auditing

There should be audits to assess the effectiveness of current SCP processes and to identify SCP weaknesses and deficiencies. It is then the company's responsibility to enhance its program to remediate any compliance gaps. Enhancements might include updating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at an enterprise-wide level.

The company should employ testing or audit procedures appropriate to its risk assessment and the level and sophistication of its SCP and ensure that the audit group is accountable to senior management and has sufficient expertise, resources and authority within the organization.

5. Training

An adequate training program that is tailored to the company's risk profile and reaches appropriate personnel is critical to the success of an SCP. Training should be provided at least annually and generally should accomplish the following: (1) provide job-specific knowledge; (2) communicate the compliance responsibilities for each employee; and (3) hold employees accountable for sanctions compliance training through assessments.

Further, the company should:

- Ensure that its OFAC training program provides adequate information and instruction to employees and, as appropriate, stakeholders to support the organization's OFAC compliance efforts.
- Provide tailored training to high-risk employees.
- Provide training appropriate for its products and services; its customers, clients and partners; and the regions in which it operates.
- Provide training with a frequency that is appropriate based on its risk profile.
- Take immediate action to provide corrective training to relevant personnel when it learns of a weakness in its procedures.
- Ensure that its training program includes resources and materials that are available and accessible to all applicable personnel.

Root Causes of OFAC Sanctions Breakdowns

The OFAC Framework includes an appendix that identifies ten root causes of OFAC sanctions compliance breakdowns based on prior OFAC administrative actions:

1. Lack of a formal SCP.

2. Misinterpreting, or failing to understand the applicability of, OFAC's regulations.
3. Facilitating transactions by non-U.S. persons (including by overseas subsidiaries or affiliates).
4. Exporting or re-exporting U.S.-origin goods, technology or services to OFAC-sanctioned persons or countries.
5. Utilizing the U.S. financial system for commercial transactions involving OFAC-sanctioned persons or countries.
6. Sanctions screening software or filter problems.
7. Improper due diligence on customers/clients (e.g., ownership, business dealings, etc.).
8. Decentralized compliance functions and inconsistent application of an SCP.
9. Utilizing nonstandard payment or commercial practices.
10. Wrongdoing by key employees that may result in individual liability.

Takeaways

As noted, the OFAC Framework clearly establishes the agency's expectations regarding an effective SCP. Given the importance that OFAC places on an effective SCP in its enforcement decisions, including the determination of the amount of any civil penalty, a company with international activities should consider whether its SCP meets OFAC's standards and, if it does not, modify the SCP to satisfy OFAC's requirements.

Authors

Explore more in

Blockchain & Digital Assets Fintech & Payments

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality’s Voter ID Law