On May 2, 2019, the U.S. Department of the Treasury’s Office of Foreign Asset Controls ("OFAC"), the U.S. agency responsible for administering and enforcing economic and trade sanctions, released “A Framework for OFAC Compliance Commitments” (the “Framework”). The Framework outlines what OFAC views as the essential components of a Sanctions Compliance Programs ("SCP"). In order to comply effectively with economic sanctions restrictions and requirements, many companies choose to implement risk-based SCPs. This guidance, however, marks the first time that OFAC has provided explicit guidance to companies on its views of what should be included in an effective SCP, and appears to signal the latest installment in its subtle-but-steady push to communicate more with the economic sanctions user community regarding its enforcement and compliance expectations.

Many of the concepts will be familiar to compliance professionals generally, as sensible baseline compliance measures that any program addressing cross-border risks would naturally include. Some suggested measures, however, are tailored to specific risks that arise in the sanctions compliance context; other measures one might expect to see addressed are not included.

The OFAC guidance comes at a time when economic sanctions have come to occupy a position of greater prominence in the regulation of cross-border economic activity and as U.S. officials continue to ramp up both the number of enforcement actions and the range of penalties imposed. Recent prominent settlements have included a requirement that the targeted company implement compliance measures that closely mirror the elements of the SCP. OFAC is clearly seeking to leverage the impact of its enforcement activity to encourage companies globally to adopt preventative measures. OFAC may also be seeking to close the “guidance gap” between it and the other U.S. agencies concerned with cross-border legal risks, including the Department of Justice ("DOJ"), whose National Security and Criminal divisions have issued extensive compliance and enforcement guidance in recent years. Ever-present requests for guidance from the private sector may also have been a catalyst.

Whatever the motivation, we see increased engagement by OFAC with the international business community as a positive development, and one likely to serve companies’ and OFAC’s interests by providing for more explicit compliance standards up-front, and clearer guideposts in the investigation and enforcement context.

However, now that OFAC has provided this communication, OFAC will likely come to expect more from companies that previously may have pleaded ignorance as to what would be sufficient for a risk-based SCP for an organization. In issuing this Framework, OFAC expressly stated that it would now consider
“the existence of an effective SCP” in determining penalty calculations for violations.\(^3\) We also expect financial institutions, often on the “front line” of sanctions enforcement actions, to begin demanding that borrowers who operate in higher-risk environments adopt measures reflecting the OFAC principles. Accordingly, companies would be well advised to take the time to evaluate their compliance programs against the five factors set forth in the Framework, and assess any changes that may need to be made to comport with OFAC’s new recommendations.

The Framework

The Framework sets out OFAC’s position that an effective SCP contains the “five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training,” and explains in some detail what OFAC views as the elements of each component.\(^4\) OFAC also includes an appendix outlining ten “root causes” of past sanctions violations, explaining how they have led to enforcement actions in certain types of enterprises since the publication of OFAC’s Economic Sanctions Enforcement Guidelines.\(^5\)

The Five Components

OFAC has long included a Risk Matrix in its Economic Sanctions Enforcement Guidelines (“Guidelines”) as an appendix to the OFAC federal regulations as a way for financial institutions to “evaluate their compliance programs.”\(^6\) Several elements of the matrix are now included in the more detailed and precise Framework. While OFAC acknowledges that the level of complexity and sophistication required for an SCP will vary depending on company-specific factors, the five components on which an SCP should be predicated remain the same, which are identified and explained as follows.

**Management Commitment**

OFAC considers senior management’s commitment to a company’s SCP as “one of the most important factors in determining its success,” and has set out five ways that a company’s senior management—including its senior leadership and the board of directors—should be involved in an effective SCP:\(^7\):

1. Reviewing and approving the company’s SCP;
2. Ensuring the compliance function has the requisite authority and autonomy to be effective, including direct reporting lines to senior management;
3. Providing the compliance function with adequate resources, such as personnel and technology;
4. Promoting a “culture of compliance” throughout the company; and
5. Demonstrating recognition of the severity of OFAC violations and implementing appropriate measures to ensure compliance with sanctions.

OFAC emphasizes that in order for an SCP to be adequately resourced, a company should maintain a “dedicated OFAC sanctions compliance officer,” who—in a nod to the many hats most compliance officers often wear—may be someone serving in other senior compliance positions. Demonstrating that a company has a single individual who is responsible for sanctions compliance oversight is a simple, but significant, way to exhibit a management commitment to sanctions compliance.
**Risk Assessment**

As with similar documents published by the DOJ, SEC, and other enforcement agencies concerned with foreign corruption and other wrongdoing, the Framework explicitly states the need for companies to conduct tailored risk assessments. Unlike those documents, however, the Framework does so in a more focused and targeted way, emphasizing three key areas that companies may assess in order to determine areas where a company may engage with sanctioned persons or jurisdictions:

1. Third parties (i.e. customers, supply chain, intermediaries, and counter-parties);
2. Product and service offerings; and
3. Geographic locations of the company.

OFAC encourages companies to conduct a risk assessment both “in a manner, and with a frequency, that accounts for the potential risks.” Accordingly, OFAC provides that a “central tenet” of an effective risk assessment is ensuring that it is routine and, if appropriate, ongoing. Risk assessments can most effectively assist in creating internal controls and training when companies update and adapt the assessment periodically, in order to account for any underlying root causes that have led to deficiencies within the organization that could lead to sanctions violations.

**Internal Controls**

The Framework explicitly sets out seven key internal controls that should be included in an SCP. Implementing these controls provide an organization with the policies and procedures necessary to minimize risk and identify, escalate, remedy, and keep reports of potential sanctions violations. The seven internal controls that OFAC explains are:

1. Written policies and procedures that are easy to follow and designed to prevent employees from engaging in misconduct;
2. Internal controls such as technology solutions that are calibrated to appropriately address the company’s risk profile;
3. Internal or external audits designed to enforce the policies and procedures;
4. Recordkeeping policies to adequately account for any requirements imposed by sanctions programs;
5. Mechanisms to take immediate and effective action to remedy internal controls when a weakness is identified;
6. Clear communication of the SCP policies and procedures to relevant personnel and third parties; and
7. Appointment of personnel to integrate the SCP into the daily operations of the company.

Interestingly, OFAC emphasizes that in order to be effective, SCP “should be capable of adjusting rapidly to changes published by OFAC”—including changes to lists of blocked persons, new or updated sanctions, and the issuance of general licenses.
Testing and Auditing

While many of the Framework components were previously considered in the Guidelines and are common across all compliance disciplines, testing and auditing was not previously included in such guidance and represents a new piece of the compliance puzzle. Companies are encouraged to conduct audits to discover discrepancies between the ideal practices as set forth in the SCP, and day-to-day operations of a company. OFAC now expects to see at least three attributes in connection with the sanctions audit function, including a company’s commitment to ensuring:

1. The audit function is accountable to senior management and equipped with the necessary tools and resources;
2. The audit procedures are appropriately scaled to the company’s level of commercial sophistication; and
3. The company will take immediate action to remedy any issues identified by the audit.

Auditing is an important mechanism by which companies can analyze the effectiveness of the policies and procedures implemented by an SCP, and OFAC now expressly considers a company’s commitment to such practices.

Training

As one would expect, OFAC identifies effective training as an “integral component of a successful SCP.” OFAC further explains that, for a training program to be considered adequate by the agency, a company must:

1. Ensure the program is tailored effectively to provide appropriate levels of information to all relevant employees;
2. Confirm the scope of the program is proportional to the company’s specific circumstances, such as third parties with which the company deals, its products and services, and its geographic presence;
3. Provide the training with suitable frequency based on the company’s risk profile;
4. Institute training upon learning of a deficiency related to sanctions compliance; and
5. Include easily accessible resources as a part of the training program.

The Framework is very prescriptive in this section; OFAC provides that the training should not only be periodic, but at a minimum annually. In addition to providing these general aspects, OFAC also explains that the training should provide job-specific knowledge, communicate responsibilities to each employee, and hold employees accountable for knowledge of sanctions compliance through assessments. Training programs are now necessary under this Framework.

What is Not Found in the Five Components

For all the valuable granularity in the Framework, there are some common compliance program items which appear in guidance documents in other areas and which one might have expected OFAC to include—but evidently, deliberately did not. Those items include, among others, a confidential reporting process, an investigations process (as opposed to auditing of the SCP as in the Framework),
disciplinary measures for employees which fail to follow the program, an emphasis on “message in the middle” (as opposed to “tone from the top”), and a number of other nuances.

It is not clear why OFAC chose to omit these nuances where many of the companies to which the Framework applies will also be subject to more general DOJ Criminal Division compliance guidance, but no doubt practitioners will seek further clarification from OFAC in the weeks and months to come.

The “Root Causes”

In what appears to be somewhat of an innovation in the cross-border compliance community, the Framework also includes an Appendix setting out ten different root causes OFAC states it often sees as the reasons for sanctions violations. We find this portion of the Framework helpful and believe it will be for companies as well, as they assess their own programs in the context of those basic issues that have led to enforcement actions over the last ten years.

These root causes include:

(i) Failure to maintain an SCP at all;
(ii) Misinterpreting the applicability of sanctions;
(iii) Non-U.S. persons facilitating transactions with sanctioned parties;
(iv) Exporting or reexporting U.S.-origin goods, technology, or services to sanctioned persons or countries;
(v) Utilizing the U.S. financial system for transactions with sanctioned persons, including by conducting the transaction in U.S. dollars;
(vi) Relying on faulty or outdated sanctions screening software;
(vii) Conducting improper due diligence on third parties;
(viii) Inconsistent application of a compliance program;
(ix) Using non-standard commercial practices; and
(x) The actions of individuals who cause companies to be liable for sanctions violations.

Companies may use these root causes as a tool to identify what kinds of issues may be particularly applicable to them given their specific set of facts and circumstances such as commercial sophistication and international presence. While each of these root causes could be discussed at length in their own right, two root causes warrant particular emphasis: (i) the failure to maintain any formal SCP; and (ii) individual actions that lead to liability.

The Importance of Having an Effective SCP

Though sanctions violations are often caused by a confluence of events, the first root cause of sanctions violations OFAC lists is the lack of a formal OFAC SCP. Without an effective SCP, companies can engage in the regular course of business with the best of intentions but ultimately be unable to identify threats of sanctions violations because of a lack of policies or procedures designed to catch such risks. Companies without such a program therefore run the risk of unknowingly engaging in
sanctioned business and forfeiting the opportunity to voluntarily disclose it to OFAC in a manner that would demonstrate a commitment of compliance with sanctions regulations.

OFAC indicates that in past enforcement actions, it has considered the lack of an SCP to be an aggravating factor that increases the civil monetary penalty. Now that OFAC has issued the Framework wherein it says it would consider “favorably” the existence of an SCP when a violation occurred, ineffective compliance policies that do not comport to OFAC’s stated guidance also run the risk of becoming an aggravating factor.

Having an effective SCP is the gateway to sanctions compliance, and many of the additional root causes identified by OFAC as causing sanctions violations may be eliminated by having such a compliance program in place.

*The Risk of Individual Liability*

OFAC’s inclusion of the “actions of individuals” as a root cause, and its explicit acknowledgement that it may seek to hold individuals and companies liable for sanctions violations, is a new development in OFAC’s public messaging.

It may be intended to reemphasize the DOJ’s 2016 guidance on voluntary self-disclosures, cooperation, and remediation in instances of sanctions and export control violations (“NSD Guidance”). The NSD Guidance, which paralleled similar guidance relating to the then-FCPA Pilot Program and incorporated the so-called Yates Memorandum, explained that in voluntarily disclosing violations to the DOJ, companies must disclose known relevant facts, including those pertaining to the specific individuals involved in the violations.

An effective SCP is not only important in protecting companies against aggressive OFAC enforcement, but also any such individual employees who may have played “integral roles in causing or facilitating” sanctions violations.

**Bottom Line**

While many of the five enumerated elements of the SCP are common elements of sophisticated compliance programs, they are now all but mandatory in OFAC’s opinion. In publishing not only specific elements of an SCP that OFAC deems “essential,” but also detailing the ten root causes of violations, OFAC may be signaling an era of increased enforcement actions. In 2019, OFAC has already issued 14 penalties or settlements. In 2018, OFAC only issued seven in the entire year; in 2017, OFAC issued 16 in total.

This Framework and outline of root causes of sanctions violations provide a clear roadmap for OFAC to evaluate how ineffective compliance programs give rise to sanctions violations. In an environment with increasingly turbulent sanctions regime, assurance that a company’s SCP is in line with OFAC expects it must become the norm. If a company’s SCP does not meet these standards, the company may be at risk for penalties that are otherwise preventable.

---

*If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:*


3. OFAC will now consider the existence of an effective SCP in its determination of whether or not a violation of sanctions regulations is considered to be “egregious.” The Director or Deputy Director makes determinations of whether a violation is egregious for purposes of calculating monetary penalties. A determination that a violation was egregious leads to larger penalties, up to the statutory maximum if the case is egregious and the violation was not self-disclosed. The current statutory maximum penalty for violations of the International Emergency Economic Powers Act, under which many sanctions programs are promulgated, is the greater of $295,141 or twice the amount of the underlying transaction for each violation.


5. Id. at 9.

6. 31 C.F.R. Part 501, Appendix A.

7. Framework, supra note 1 at 2.

8. Id. at 3.

9. Id. at 5.

10. Id. at 6.

11. See generally The Evaluation of Corporate Compliance Programs, supra note 2.


Paul Hastings LLP
Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2019 Paul Hastings LLP.