

Service

Export Controls &  
Economic Sanctions

Professionals

CORTNEY O'TOOLE  
MORGAN  
WASHINGTON:  
202.378.2389  
CORTNEY.MORGAN@  
HUSCHBLACKWELL.COM

GRANT D. LEACH  
OMAHA:  
402.964.5143  
GRANT.LEACH@  
HUSCHBLACKWELL.COM

# New OFAC Framework Increases Penalties for Deficient Compliance Programs

## Key Points

Members of the international business community who are subject to U.S. trade sanctions and who have non-existent or inadequate sanction compliance programs (SCPs) are now potentially subject to significantly higher penalties for any sanctions violations they commit.

If companies already have SCPs, they should re-evaluate those programs and revise them as necessary to conform to this new guidance.

It continues to be critically important that senior management within an organization adequately support the sanctions compliance function.

## The new framework for OFAC compliance commitments

On Thursday, May 2, 2019, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) published guidance titled "A Framework for OFAC Compliance Commitments" (the Framework), which should prompt members of the international business community (both inside and outside the U.S.) to adopt or re-evaluate their SCPs. The Framework provides practical guidance on OFAC's enforcement philosophy going forward. Specifically, the Framework: (i) establishes that the non-existence or adequacy of an organization's SCP will now be a factor that OFAC considers when determining whether to apply significantly enhanced penalties for "egregious" violations; (ii) notifies global businesses that OFAC will continue its recent practice of requiring sanctions violators to implement or modify SCPs in enforcement actions when OFAC imposes a civil monetary penalty; (iii) identifies what

OFAC considers to be the five essential components of an effective SCP; and (iv) identifies common recurring “root causes” that are often associated with OFAC violations.

### **Overview of OFAC sanctions enforcement concepts**

U.S. statutes and regulations impose a variety of sanctions against foreign individuals, entities and, in some instances, entire foreign countries. These sanctions apply to U.S. persons at all times and extend to non-U.S. persons who conduct business with the U.S., route transactions through the U.S. financial system or trade in U.S. origin goods, technology or services. OFAC is tasked with administering these sanctions and enforcing sanctions violations. The base civil monetary penalty for an “egregious” violation of these sanctions is typically equal to the *greater* of: (i) \$295,141 per violation or (ii) twice the amount of the underlying transaction. If OFAC determines that a violation is non-“egregious,” then the violation’s maximum base civil monetary penalty is calculated based on the dollar value of the transaction according to a significantly reduced penalty schedule, which ultimately caps any violation penalty at the maximum amount of \$295,141 per violation.

OFAC’s Economic Sanctions Enforcement Guidelines (the Enforcement Guidelines) are published in the Code of Federal Regulations and provide a list of 11 General Factors that OFAC considers when assessing penalties for sanctions violations. As a preliminary matter, the Enforcement Guidelines require OFAC to first consider four General Factors when determining whether a violation is “egregious”: (A) whether the violation was a “willful or reckless violation of law”; (B) whether the offender had “awareness of [the] conduct at issue”; (C) the “harm to sanctions program objectives” caused by the violation; and (D) additional “individual characteristics.” In this preliminary “egregiousness” analysis, the Enforcement Guidelines require OFAC to place particular emphasis on the aforementioned factors (A) and (B). This “egregiousness” determination sets the applicable base civil monetary penalty (as described above) and the Enforcement Guidelines then allow OFAC the discretion to either increase or decrease that base penalty amount after considering the full list of all 11 General Factors.

The “existence, nature and adequacy” of a suspected violator’s SCP has always been one of the Enforcement Guidelines’ seven General Factors that OFAC considers when adjusting a base penalty upward or downward but not when making its initial determination of whether the underlying conduct was “egregious.” However, the Framework now provides that “OFAC may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed ‘egregious.’” This means that organizations that violate OFAC sanctions while operating with a non-existent or ineffective SCP are now at risk that OFAC will use their SCP deficiencies as a basis to classify their violations as “egregious” and impose the significantly higher penalties described above.

## **Expect mandatory compliance commitments under OFAC settlement agreements going forward**

The Framework also states that, when OFAC becomes aware of sanctions violations, OFAC will consider refusing entering into any settlement agreements for sanctions enforcement actions unless the offending companies agree to integrate specified SCP practices required by OFAC. OFAC previously employed this approach in three settlement agreements that preceded the Framework: (i) a December 2018 settlement agreement with Zoltek Companies, Inc. (imposing a \$7,772,102 penalty for a mix of “egregious” and non-“egregious” violations of the Belarus Sanctions Regulations); (ii) a March 2019 settlement agreement with Stanley Black & Decker, Inc. (imposing a \$1,869,144 penalty for “egregious” violations of its Iranian Transactions and Sanctions Regulations); and (iii) an April 2019 settlement agreement with Standard Chartered Bank (imposing a \$639,023,750 penalty for “egregious” violations of multiple sanctions programs). In each of those settlement Agreements, OFAC required the respondent to incorporate a list of at least 20 specifically identified compliance commitments into their respective SCPs. These mandated commitments included (but were not limited to) providing adequate resources to the SCP, implementing adequate internal controls to prevent sanctions violations and performing ongoing testing or auditing of the SCP. For the five years following each settlement agreement, OFAC will also require senior-level executives from each respondent company to submit an annual certification confirming their continued compliance with their respective settlement agreement’s compliance commitments. Any breach of those compliance commitments will entitle OFAC to re-open its sanctions investigations.

The *Zoltek*, *Stanley Black & Decker* and *Standard Chartered Bank* settlement agreements all featured “egregious” violations. However, the Framework has now stated that OFAC will impose compliance commitments “as appropriate” in any sanctions settlement that results in a civil monetary penalty and does **not** limit this remedy to only settlements involving “egregious” violations. Companies that choose not to implement a SCP and then violate U.S. sanctions will likely find that the cost of implementing and administering a SCP under OFAC mandate will far exceed the costs they would have spent to do so voluntarily.

## **The five essential components of a sanctions compliance program**

While noting that “[E]ach 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 Framework provides that each SCP “should be predicated on and incorporate at least five essential components of compliance: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.” To the extent that

companies either do not have a SCP or have a SCP that is deficient in any of these five components, OFAC will consider those deficiencies when determining whether to classify violations as “egregious” when imposing penalties for sanctions violations and/or when deciding whether to mandate compliance commitments in connection with a settlement agreement. Conversely, the Framework provides that companies with effective and adequate SCPs incorporating these five components will receive favorable consideration should they become subject to an OFAC investigation.

## **1. Management commitment**

OFAC expects senior management within an organization to support the SCP and generally “foster a culture of compliance throughout the organization.” The Framework establishes expectations for senior management that include (but are not limited to): (1) providing the compliance unit with sufficient resources and authority; (2) maintaining direct reporting lines between the compliance unit and senior management, to include “routine and periodic meetings between these two elements of the organization”; (3) designating an OFAC sanctions compliance officer within the organization and ensuring that the organization’s persons with sanctions compliance responsibility have sufficient technical knowledge and expertise in OFAC matters; and (4) promoting a “culture of compliance” within the organization where personnel can report sanctions misconduct to senior management without fear of reprisal. Senior management’s role in sanctions compliance is particularly critical because the Enforcement Guidelines’ General Factors (A) and (B) (discussed above) also place significant emphasis on whether senior management was involved in or had knowledge of any OFAC sanctions violations when determining whether to classify any violations as “egregious.”

## **2. Risk assessment**

The Framework indicates that an organization’s SCP should assess sanctions risks in the organization’s clients, products, services, geographic locations and other transactional counterparties on a sufficiently frequent basis. The organization should then consider the results of that initial risk assessment when structuring its SCP’s internal controls (discussed below) and due diligence procedures for counterparties and transactions. The Framework specifically notes that “Risk assessments and sanctions-related due diligence is also important during mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations.” Although the Framework does not specify how frequently organizations should repeat these risk assessments, the Framework does provide some guidance by advising that organizations should update their risk assessments to account for violations or deficiencies that an organization discovers during its routine course of business or through the testing or audit functions described below.

## **3. Internal controls**

According to the Framework, any SCP should include policies and other procedures in order to “[I]dentify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered by OFAC.” The SCP’s internal controls should address the risks identified in the organization’s risk assessment. In particular, OFAC has advised that a company’s SCP should be adaptive enough to rapidly respond to changes in sanctions policy and additions to OFAC’s various denied persons lists. OFAC continues to recommend that organizations should include technology solutions in their internal controls when appropriate, but also recommends organizations ensure those technology solutions are properly calibrated and routinely tested for effectiveness. Organizations should clearly communicate their SCP’s policies and procedures to personnel with sanctions compliance responsibilities and then confirm that those personnel understand their responsibilities.

## **4. Testing and auditing**

The Framework expects organizations to conduct appropriate testing or audit procedures in order to ensure that the SCP is functioning properly and to identify any weaknesses or deficiencies within the SCP. Personnel performing the testing or auditing may be from within or outside the organization, but they should be accountable to the organization’s senior management, independent of the activities they are auditing and sufficiently skilled and empowered to perform the testing and auditing function. If organizations do detect weaknesses or deficiencies, OFAC expects them to implement compensating controls as a temporary measure until they can identify the root cause of the weakness or deficiency and remediate that root cause through appropriate SCP enhancements.

## **5. Training**

In the Framework, OFAC advises organizations that they should conduct appropriate sanctions compliance training on at least an annual basis. Per OFAC, this training should: (i) provide personnel with job-specific knowledge based on their role within the organization; (ii) communicate each employee’s sanctions compliance responsibilities to them; and (ii) conduct assessments in order to hold employees accountable for the training. This training is particularly important for employees in positions with significant sanctions risks. When appropriate, organizations should also provide training to outside stakeholders such as clients, suppliers, business partners and other counterparties.

## **Root causes commonly associated with OFAC sanctions violations**

In order to help organizations to properly structure and/or update their SCPs, the final section of the

Framework provides a non-exhaustive list of 10 root causes that OFAC has historically associated with sanctions violations in its previous public enforcement actions: (1) lack of a formal OFAC SCP; (2) misinterpreting or failing to understand the applicability of OFAC's regulations; (3) facilitating transactions by non-U.S. persons; (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, or processing payments to or through U.S. financial institutions, for commercial transactions involving OFAC-sanctioned persons or countries; (6) sanctions screening software or filter faults; (7) improper due diligence on customers/clients; (8) decentralized compliance functions and inconsistent application of a SCP; (9) utilizing non-standard payment or commercial practices; and (10) individual liability. Organizations should consider these common root causes when they design, update and administer their SCPs.

### **What this means to you**

U.S. economic sanctions apply to U.S. persons, as well as non-U.S. persons who conduct transactions involving U.S. persons; U.S.-origin goods, services or technology; or funds transfers through the U.S. financial system. With OFAC's recent publication of the Framework, companies inside and outside the U.S. that are subject to U.S. economic sanctions should consider taking the following actions:

Companies without a SCP in place should evaluate, adopt and implement a SCP consistent with OFAC's Framework guidance.

Companies with SCPs in place should examine those SCPs and revise them as necessary to conform to the Framework.

After adopting or revising their SCP, companies should continue to perform the risk assessment, testing and auditing, and training functions on an ongoing basis. They should also be prepared to quickly update their SCP in response to any future changes in OFAC sanctions policy.

### **Contact us**

For assistance designing, implementing or updating your SCP, contact Cortney Morgan, Grant Leach, Linda Tiller or another attorney on Husch Blackwell's Export Controls & Economic Sanctions Team.