

# The Complete Compliance and Ethics Manual 2024

## Corporate Compliance in a Geopolitical World: OFAC's Framework for Compliance Commitments

---

By Jeremy Page and Shannon Fura<sup>[1]</sup>

As the world continues to shrink and geopolitical risks continue to grow, incorporating a robust sanctions compliance program (SCP) into a company's broader compliance and ethics program is a must.

To support companies in the implementation of an effective SCP, on May 2, 2019, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) published *A Framework for OFAC Compliance Commitments*<sup>[2]</sup> "in order to provide 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, with OFAC's perspective on the essential components of a sanctions compliance program."<sup>[3]</sup> In addition to providing guidance on the implementation of an effective SCP, the framework "outlines how OFAC may incorporate these components into its evaluation of apparent violations and resolution of investigations resulting in settlements" and "offers a brief analysis of some of the root causes of apparent violations of U.S. economic and trade sanctions programs OFAC has identified during its investigative process."

### Who Is OFAC?

The Office of Foreign Assets Control is an agency of the US government that "administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States."<sup>[4]</sup> OFAC accomplishes these objectives through two principal means:

1. Through the administration of a wide range of sanctions programs that can be either comprehensive or targeted in scope while focusing on financial/asset-based restrictions and/or constraints or prohibitions in two-way or unilateral trade; and
2. Through the development, implementation, and maintenance of lists of individuals, companies, and entities that either: (1) are owned or controlled by, or are acting on behalf of, a sanctioned country; or (2) are identified with a noncountry-specific sanction program.

From a "list" perspective, the principal resource maintained by OFAC is the Specially Designated Nationals and Blocked Persons (SDN) List. As of July 2021, approximately 6,300 parties were identified on the SDN List,<sup>[5]</sup> with additions (not so much deletions) occurring on a frequent, if not constant, basis. That list is derived from the 37 distinct sanctions programs OFAC has in place,<sup>[6]</sup> with whole or in part programs imposed against such countries as Iran, Cuba, Syria, North Korea, Venezuela, Hong Kong, Ukraine, and Russia, and issue-specific programs in place against such interests as Chinese military companies, narcotics trafficking, money laundering, counterterrorism, cybersecurity, and human rights. While many of these programs exist under the sole authority of OFAC, in some instances, oversight is shared with the U.S. Department of Commerce's Bureau of Industry and Security.

---

## The Framework

The framework offered by OFAC revolves around “five essential components of compliance”:

1. A commitment from management,
2. Weighted risk assessment,
3. The development of a system of internal controls,
4. Ongoing testing and auditing, and
5. Training.

As concepts, nothing in these five elements is new, as any program worth its salt will consider these attributes in establishing a compliance foundation. Where the difference lies, therefore, is in the unique considerations pertinent to US sanctions programs and the laws and regulations that OFAC administers.

### 1. A Commitment from Management

The first building block to development of a qualified SCP is an unwavering commitment from management to adhere to all sanctions requirements. This is not as straightforward as it might appear, as US sanction policy is oftentimes extraterritorial in nature, extending beyond US borders to entities and individuals not necessarily under the jurisdiction of the United States. It can also, in select instances, result in “secondary sanctions,” by which US policy is imposed on entities/individuals with absolutely no nexus to the United States through imposition of a chokehold or other restriction on access to US financial or commercial markets for those non-US individuals/entities that choose to conduct business with or provide services to a country or SDN contrary to US interests.

Because of this reach, management can, on occasion, find itself battling competing corporate interests in an effort to comply with US legal and regulatory requirements. And yet, it is precisely that firm hand that OFAC is seeking in gauging the strength of management’s commitment to OFAC compliance.

So, what must management commit to in a sanctions compliance world? First, it must be senior management that buys in and not merely the manager/senior manager/director who oversees the nitty-gritty of compliance. For OFAC, C-suite engagement as well as the imprimatur of the board of directors/overseers is critical to the success of any SCP. That support must be deep, including ensuring that adequate resources with delegated authority and a supporting safety/operational net to dictate policies and/or practices are put in place to preserve a continuous commitment (i.e., the authority to say no) to sanctions compliance. Maintaining open lines of communication, including a direct reporting structure, ensures that senior management remains apprised of any potential or identified risk while also avoiding the possibility that updates or general information sharing will be squelched before it can be fully discussed. A regular schedule of meetings is also preferred, even where there is (hopefully) nothing to report, to ensure that sanctions compliance remains on senior management’s radar. In addition, compliance must have a seat at the table, being brought in early in the new business or acquisition environment to ensure that any potential compliance risk is weighed before the trigger is pulled.

Beyond these considerations, senior management must invest in the appropriate tools to support ongoing compliance. That includes designating a dedicated OFAC sanctions compliance officer and/or compliance team who understands the rules and requirements that must be satisfied while providing that individual/team with sufficient visibility and knowledge of the company’s financial and operational structure to gauge any potential risk to the organization as a whole. That individual/team must also be identified and known across the enterprise

as the go-to resource for questions and/or concerns, as any delays in securing guidance can be crucial to avoiding even inadvertent violations of US sanctions policy.

Finally, and perhaps most importantly, senior management must imbue the organization with a culture of compliance. This extends beyond simply building the SCP to taking palpable action that’s visible to all employees. Establishing a mechanism for reporting any identified or perceived sanctions-related misconduct without risk of retaliation, forcefully addressing any violations through remedial/corrective action, and ensuring that senior management itself is held to the same standards are all critically important to OFAC in demonstrating management engagement. While mistakes may (and likely will) still occur, they are less likely to be the result of bad actors (or simply overly enthusiastic businesses) where senior management has made its position clear.

2. A Risk-Based Approach

Multinational corporations are constantly on the move, which can challenge even the best of SCPs. Because of that reality, it is essential that any SCP incorporate an assessment model that prioritizes those activities/businesses most likely to engender risk.

To be truly effective, the risk assessment model must start at 10,000 feet, looking down on the enterprise as a whole before tiering the organization for purposes of identifying those areas/operations most likely to run up against US sanctions policy. All aspects of the business must be considered, whether that be an assessment of customers, suppliers, transportation service providers, and other parties to the transaction; the goods and services offered or provided as part of the business; the systems of record and personnel (including locations) that support the company’s operations; or the geographic footprint of the business, its customers, and its supply/business partner chain.

With that segregation in place, a plan can be developed to determine the type, frequency, and depth of assessments required to be performed. Logically, those areas/operations found to have greater potential risk must be evaluated with greater frequency, although even lower-risk activities need to periodically be considered. In addition, and as already noted under the management commitment discussion above, it is essential that any new proposed business opportunity—whether that be a new line of business, an acquisition (particularly one based outside of the United States), a new geographic market, or even a new customer—be risk assessed in advance of any engagement both to level-set where compliance stands today and to integrate that activity for ongoing assessment purposes.

For companies not certain where to start in evaluating their customers, businesses, or potential acquisitions, OFAC has provided a helpful tool that can be customized to an individual company’s needs. Although principally developed to help financial institutions evaluate their own compliance programs, the elements identified from the OFAC Risk Matrix (Table 1)<sup>[7]</sup> can form the foundation for any risk assessment modeling.

Low	Medium	High

No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (i.e., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the institution addressed the issues and is not at risk of similar violations in the future.	Multiple recent actions by OFAC, where the institution has not addressed the issues, thus leading to an increased risk of the institution undertaking similar violations in the future.
Management has fully assessed the institution's level of risk based on its customer base and product lines. This understanding of risk and strong commitment to OFAC compliance is satisfactorily communicated throughout the organization.	Management exhibits a reasonable understanding of the key aspects of OFAC compliance and its commitment is generally clear and satisfactorily communicated throughout the organization, but it may lack a program appropriately tailored to risk.	Management does not understand, or has chosen to ignore, key aspects of OFAC compliance risk. The importance of compliance is not emphasized or communicated throughout the organization.
The board of directors, or board committee, has approved an OFAC compliance program that includes policies, procedures, controls, and information systems that are adequate, and consistent with the institution's OFAC risk profile.	The board has approved an OFAC compliance program that includes most of the appropriate policies, procedures, controls, and information systems necessary to ensure compliance, but some weaknesses are noted.	The board has not approved an OFAC compliance program, or policies, procedures, controls, and information systems are significantly deficient.
Staffing levels appear adequate to properly execute the OFAC compliance program.	Staffing levels appear generally adequate, but some deficiencies are noted.	Management has failed to provide appropriate staffing levels to handle workload.
Authority and accountability for OFAC compliance are clearly defined and enforced, including the designation of a qualified OFAC officer.	Authority and accountability are defined, but some refinements are needed. A qualified OFAC officer has been designated.	Authority and accountability for compliance have not been clearly established. No OFAC compliance officer, or an unqualified one, has been appointed. The role of the OFAC officer is unclear.
Training is appropriate and effective based on the institution's risk profile, covers applicable personnel, and provides necessary up-to-date information and resources to ensure compliance.	Training is conducted and management provides adequate resources given the risk profile of the organization; however, some areas are not covered within the training program.	Training is sporadic and does not cover important regulatory and risk areas or is nonexistent.

The institution employs strong quality control methods.	The institution employs limited quality control methods.	The institution does not employ quality control methods.
---	--	--

### 3. A System of Internal Controls

While senior management commitment and risk modeling are critical to the implementation of a successful SCP, perhaps no element is as important as the internal controls developed and implemented to ensure the organization remains on the compliance track. Documented policies, procedures, and work instructions, based in part on the company's risk assessment and in part on the general legal and regulatory requirements that must be satisfied, are essential tools to any SCP. They not only establish the path to be followed organizationally, but also create a legacy from which future compliance professionals may be guided. Those controls are not solely internal to the compliance function either, as the world of sanctions compliance requires the efforts of many disciplines, including, but not limited to, engineering/product development, purchasing, logistics, accounting/finance, information systems, human resources, customer service, and sales.

Therefore, in order to be effective, any system of internal controls needs to integrate sanctions compliance within these functions' own policies and procedures. Is the goal to make those professionals compliance experts? No, certainly not. Instead, the objective is to make those areas sensitive to sanctions-related considerations and establish an open line of communication across the enterprise so that any potential sanctions-related risk is identified early and, hopefully, before any actual harm to the company arises. Any such education should be performed by the enterprise's designated OFAC compliance officer/team to enhance their visibility within the organization for purposes of ongoing dialogue.

In addition, reliable external resources such as utilization of a dynamic screening tool are also essential. As noted previously, the players in the sanctions world change rapidly, with new restrictions imposed literally overnight. While some modifications come with a safe harbor or delayed implementation, in many instances, companies are expected to move mountains and shut off all business ties on a moment's notice. No sympathy is provided to those who fail to comply either, as OFAC's expectation is that companies are continuously monitoring developments with a contingency plan in place. OFAC's designations can also be broader in scope than they appear, as sanctions imposed can extend not only to the individual or entity named, but also to those owned 50% or more by those so identified. This is labeled the 50% Rule.<sup>[8]</sup> Identifying those additional players without a strong screening program can be extremely difficult. Care must be taken, therefore, to ensure that any screening tool/partner relied upon for purposes of gauging ongoing sanctions compliance has the capability to filter not only those directly named, but also those affiliated with those individuals/entities.

The system of internal controls also extends to an organization's record-keeping practices. Under US law, the lookback period associated with any potential/identified violation of US sanctions policy extends for five years from the date of that event.<sup>[9]</sup> Record retention *across the enterprise* is therefore essential in order to effectively scope out the extent of any risk while also being able to defend past practices should OFAC or any other export control agency draw them into question. Such records must also be organized in an easy-to-identify, cross-referenced manner so the information needed to support/defend the company's activities can be readily obtained.

Finally, and as amplified further below, existing internal controls should be periodically reviewed to ensure that they continue to mimic the organization's footprint. Where weaknesses are identified, any affected policy or

procedure should be timely updated so that the most current information and guidance required are shared organizationally.

## **4. Ongoing Testing and Auditing**

An effective SCP is dynamic in nature, requiring constant recalibration to ensure that it mimics and tracks an organization's current operational and financial footprint. Whether as the result of acquisitions, divestitures, mergers, changes in supply chain or customer base, personnel changes, or the adoption/elimination of corporate infrastructure, an SCP is consistently bombarded with challenges to its operating model.

Because of those challenges, any SCP must incorporate a routinized program of testing and auditing to ensure that it continues to provide the protection the organization requires. That testing must occur not only at the program level but also with respect to individual transactions so both the big picture and myopic details are brought into focus. Weaknesses in the tools used (software, systems, programming), as well as in the personnel resources relied upon can create immediate, consequential risk to an organization if not quickly identified and remediated. As a result, it is essential that testing and auditing not only evaluate the current state but also incorporate budgeting and the necessary operational approvals to ensure that any transition required can be implemented quickly to stem and/or forestall any bleeding.

Testing and auditing must be objectively performed. While any previously identified area(s) of risk should be included to ensure that the remedial steps taken have proven effective, the assessment performed needs to consider all flows/activity, as even an otherwise innocuous transaction can come with its own peril. Indeed, there are any number of violations published not only by OFAC but also by its sister agency, Bureau of Industry and Security, that arose out of seemingly innocuous activity on the part of the violating entity. Where a weakness or gap is identified, further investigation is required as OFAC, similar to the other US export control/enforcement agencies, does not condone "self-blinding" and expects that any red flag will be fully and completely vetted. Once complete, the results of these evaluations must be shared with senior management, with any resulting required corrective action documented for purposes of ongoing compliance as well as for potential use in ongoing training.

## **5. Training**

Training: The final frontier. No SCP can thrive without a continuous program of sensitivity and operational training. Any such program must be comprehensive in nature, addressing both the overall operational and financial footprint of the organization while also educating all personnel to sanctions compliance. And by all personnel, we truly mean all personnel, as the risk of a sanctions violation can occur at any level of an organization.

An example can bring this point home. XYZ Corporation has a contract for the sale and delivery of US goods to a European customer canceled after the goods have been offloaded at the initial European port of arrival. Rather than ship the goods back to the United States, XYZ Corporation reaches out to its global sales network to see whether there might be another customer in need. As it turns out, there is, but that customer, who could be serviced by XYZ Corporation's overseas operations with no nexus to the United States, is located in Syria. Under normal circumstances (i.e., notification and reporting through the OFAC compliance chain), XYZ Corporation would say no to this opportunity. However, in this instance, because these goods are being redeployed from overseas, there was no mechanism in place to share that information for purposes of compliance screening. As a result, the transaction was completed, and the goods reexported to Syria. To further complicate things, XYZ Corporation had to arrange for a one-off transportation routing, as the movement of goods from Europe to Syria was not within the scope of its normal transportation flows. Finally, payment to the freight forwarder that



arranged and advanced payment for that transportation also had to be provided. Although the initial effort to tender payment was rejected by XYZ Corporation's financial institution based on a reference to Syria on the payment authorization, the accounts payable clerk who had processed that initial request subsequently removed the reference to Syria (considering it an anomaly), so that payment could in fact be made.

The end result? Multiple violations of US law. The negotiation of the sale to Syria, the actual sale itself, arranging transportation for those goods, and the payment for the transportation services each reflect a violation of US sanctions policy. Could this have been avoided? Certainly, with the appropriate level of training. That training is not only with respect to those personnel engaged in the transaction but also for the compliance team itself, as this is a product/transaction flow that was not previously identified for sanctions compliance oversight. Therefore, to be effective, training must consider not only the broader implications to an organization as a whole, but also the implications arising out of individual employee's job functions and transactional responsibilities. Where possible, that training should also be reflected in operating policies and procedures so that when a situation such as the above example is encountered, sanctions compliance guidance is available regardless of who is currently in that position.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)