SULLIVAN & CROMWELL LLP

May 10, 2019

OFAC Issues Compliance Commitments Framework

OFAC's Framework Provides "Best Practices" Guidance; Identifies Five Essential Components of a Sanctions Compliance Program and Outlines Ten Root Causes of Apparent Violations of OFAC Sanctions Programs

SUMMARY

On May 2, 2019, the U.S. Department of Treasury's Office of Foreign Assets Control ("OFAC") published a framework for compliance commitments (the "Framework"), which provides guidance to organizations subject to U.S. jurisdiction (including foreign entities that conduct business in or with the United States, with U.S. persons, or that use U.S.-origin goods or services) on what OFAC considers to be the five essential components of a risk-based sanctions compliance program ("SCP"): (i) management commitment, (ii) risk assessment, (iii) internal controls, (iv) testing and auditing, and (v) training.[1] These five components closely mirror the required elements of a financial institution's Bank Secrecy and Anti-Money Laundering ("BSA/AML") Program set out in the Federal Financial Institutions Examination Council's ("FFIEC") Examination Manual.[2] The Framework also explains how OFAC will consider these five components in the enforcement context and highlights the importance OFAC places on the adequacy of an SCP in resolving enforcement actions.[3] Indeed, two recent enforcement actions have incorporated the commitments as conditions to negotiated settlements.[4] Finally, the Framework includes an appendix that identifies ten root causes of apparent violations of U.S. economic and trade sanctions programs that OFAC has identified in its public enforcement actions.[5]

BACKGROUND

Although OFAC's regulations do not expressly require parties to implement and maintain SCPs (and the Framework does not change this), OFAC's Enforcement Guidelines[6] have included the existence and

adequacy of a risk-based OFAC compliance program as a general factor to be considered in determining appropriate administrative action in response to an apparent violation.[7] In public remarks made at the time of the release of the Framework, an OFAC official stressed the consistency of the Framework with both OFAC's longstanding recommendation for a risk-based approach and the current practices of large, sophisticated financial institutions.[8] The OFAC official also confirmed that the Framework relies heavily on the FFIEC's BSA/AML Examination Manual, and indicated that OFAC also solicited feedback from Federal banking regulators when developing the Framework.

Recently announced settlements with two foreign financial institutions of apparent violations of OFAC regulations foreshadowed the Framework by requiring each institution to undertake six compliance commitments, the first five of which align precisely with the elements set forth in the Framework.[9] The sixth element present in each of the two recent settlements, but absent from the Framework, is a requirement that a senior-level executive or manager provide an annual certification to OFAC for the next five years confirming that the institution has implemented and continued to maintain the compliance commitments enumerated in the five other categories.[10] In recent public remarks, an OFAC official confirmed that the certification requirement present in these settlements does not represent a broader requirement applicable to institutions generally,[11] but will instead be applied on a case-by-case basis.

In a statement accompanying the release of the Framework, Under Secretary of the Treasury for Terrorism and Financial Intelligence Sigal P. Mandelker explained the significance of the Framework by observing that, "[a]s the United States continues to enhance our sanctions programs, ensuring that the private sector implements strong and effective compliance programs that protect the U.S. financial system from abuse is a key part of our strategy."

DISCUSSION

The Framework states that OFAC "strongly encourages" subject persons to "employ a risk-based approach to sanctions compliance, by developing, implementing and routinely updating [an SCP]."[12] Although the Framework acknowledges that each SCP will vary based on several factors such as an organization's size and sophistication, products and services, customers and counterparties, and locations in which it operates, the Framework notes that each program should incorporate at least the following five components:

1. Management commitment,
2. Risk assessment,
3. Internal controls,
4. Testing and auditing, and
5. Training.

The Framework then uses these five components, each of which is discussed in greater detail below, to provide guidance on the development and implementation of a risk-based SCP.

A. MANAGEMENT COMMITMENT

The Framework notes that the first component, commitment by senior management, is "one of the most important factors" in determining an SCP's success because it helps to ensure that the SCP is adequately resourced and fully integrated into the organization's daily operations. It also can help to legitimize the SCP, empower personnel and, more broadly, foster a culture of compliance throughout the organization.[13] The Framework notes that, although the term "senior management" may differ across organizations, it should generally include senior leadership, executives and/or the organization's board of directors.[14] The Framework then further identifies five aspects of the managment commitment component: reviewing and approving the SCP; ensuring appropriate authority and reporting structure of SCP compliance unit(s), including sufficient automony; taking steps to ensure adequate resourcing in the compliance unit(s); promoting a culture of compliance; and demonstrating a recognition of the seriousness of apparent violations or compliance deficiencies.

B. RISK ASSESSMENT

The second component of the Framework is OFAC's recommendation that each organization take a risk-based approach to designing or updating its SCP. A central aspect of this approach is to conduct a risk assessment on a routine, and, where appropriate, ongoing basis, the results of which will be integral in informing an organization's risk-based decisions and controls. Although the Framework acknowledges that risk assessments will vary across organizations, it indicates that a risk assessment should generally consist of a holistic, top-to-bottom review of the organization and its external touchpoints, and may include assessments of: (i) customers, supply chain, intermediaries and counterparties; (ii) products and services offered by the organization; and (iii) the geographic location of the organization and its customers, supply chain, intermediaries and counterparties. The Framework then further identifies two aspects of the risk assessment component: manner and frequency (including updates to the risk assessment); and methodology to identify, analyze, and address the particular risks. The Framework specifically notes that the risk assessment should be updated to account for the root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business.

Two aspects of the guidance provided in this section of the Framework are noteworthy. First, the Framework highlights the importance of risk assessment and sanctions-related due diligence in the context of mergers and acquisitions, particularly in scenarios involving non-U.S. companies or corporations. Second, in describing the types of information that may be included in a risk assessment, the Framework refers to an organization's sanctions risk ratings for its customers. During recent public remarks, an OFAC official confirmed that incorporating a customer's sanctions risk into an overall risk rating would be consistent with OFAC practice.[15]

C. INTERNAL CONTROLS

The third component of the Framework provides that effective SCPs should include internal controls, including policies and procedures, to identify, interdict, escalate, keep records of, and, where appropriate, report, activity that may be prohibited by OFAC's regulations. The Framework also identifies three purposes of internal controls: (i) to outline clear expectations, (ii) to define OFAC compliance-related procedures and processes, and (iii) to minimize risks identified by the organization during the risk assessment process. The Framework emphasizes the importance of the ability of an organization's internal controls to adjust rapidly to changes including updates to OFAC's sanctions-related lists, new, amended or updated sanctions programs and prohibitions, and the issuance of general licenses. The Framework then further identifies seven aspects of the internal controls component: policies and procedures; risk assessment results and risk profile; audits; recordkeeping; addressing weaknesses; communication (including with business units operating in high-risk areas and external parties performing SCP responsibilities on the organization's behalf); and personnel. The Framework emphasizes that for internal controls to be effective, "policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis."[16]

D. TESTING AND AUDITING

The fourth component of the Framework stresses the need for a comprehensive and objective testing or audit function within the SCP to assess the effectiveness of current processes and check for inconsistencies between these processes and actual day-to-day operations. The Framework then identifies three aspects of the testing and audit component: accountability, independence and skill; tailoring; and immediate action to address negative results.[17]

E. TRAINING

OFAC describes the fifth component of the Framework, training, as "an integral component of a successful SCP" and states that it should be provided to "all appropriate employees and personnel on a periodic basis (and at a minimum annually)."[18] The Framework further identifies three main objectives of a training program: (i) providing job-specific knowledge based on need; (ii) communicating sanctions responsibilities for each employee; and (iii) holding employees accountable for training through assessments. The Framework then further identifies five aspects of the training component: adequate and tailored information to employees and, as appropriate, outside stakeholders; appropriate scope; appropriate frequency; immediate corrective training or action following a negative result or deficiency; and accessibility.

F. ROOT CAUSES IDENTIFIED BY OFAC DURING ITS INVESTIGATIONS

The Framework also contains an appendix outlining a non-exhaustive list of ten specific root causes that OFAC has identified as being associated with apparent violations. In recent public remarks, an OFAC official emphasized the importance of determining the root cause of breaches after they occur and

incorporating that information into the organization's subsequent risk assessments and internal controls, noting that it is a best practice to do so.[19] The specific root causes identified in the appendix are as follows:

1. **Lack of a Formal OFAC SCP.** The Framework notes that, although OFAC does not require the adoption of an SCP, it has issued numerous civil monetary penalties in which the subject person's lack of an SCP was one of the root causes of the sanctions violations. The absence of an SCP is also frequently identified as an aggravating factor under OFAC's enforcement guidelines.

2. **Misinterpreting, or Failing to Understand the Applicability of, OFAC's Regulations.** The Framework cites as an example of this root cause the failure to appreciate that OFAC sanctions apply to an organization based on its status as a U.S. person (or, in the case of the Cuba and Iran programs, as a U.S.-owned or -controlled subsidiary), or its dealings with U.S. persons, the U.S. financial system or U.S.-origin goods or technology.

3. **Facilitating Transactions by Non-U.S. Person Affiliates.** The Framework states that multiple organizations subject to U.S. jurisdiction have violated OFAC regulations by referring business opportunities to, approving or signing off on transactions conducted by, or otherwise facilitating dealings between their non-U.S. locations and OFAC-sanctioned countries, regions or persons. Accordingly, the Framework suggests that organizations with integrated operations, particularly those that involve or require participation by U.S. personnel, should ensure that any activities in which they engage are compliant with OFAC's regulations.

4. **Exporting or Re-exporting U.S.-origin Goods, Technology or Services to OFAC Sanctioned Persons or Countries.** The Framework indicates that non-U.S. persons have repeatedly purchased U.S.-origin goods with the specific intent of exporting, transferring, or selling them to a country, person or region subject to OFAC sanctions, in many instances despite warning signs such as the presence of contractual language expressly prohibiting such activities. The Framework also notes that OFAC's enforcement actions in this area have generally focused on organizations that: are large or sophisticated, engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, used non-routine business practices, and, in several instances, concealed their activity in a reckless or willful manner.

5. **Using the Financial System, or Processing Payments to or through a U.S. Financial Institution, for Commercial Transactions Involving OFAC-sanctioned Persons or Countries.** The Framework explains that many non-U.S. persons violated OFAC regulations by processing financial transactions pertaining to commercial activity involving an OFAC-sanctioned country, region or person, almost all of which were USD-denominated, to or through U.S. financial institutions. The Framework notes that, even when the underlying commercial trade did not involve any U.S. persons, the inclusion of a U.S. financial institution in associated payments often results in a prohibited activity, such as the exportation of services from the U.S. to a comprehensively sanctioned country or dealing in blocked property in the U.S. The Framework also notes that OFAC's investigations in this area have generally focused on persons who have engaged in willful or reckless conduct, attempted to conceal the activity (such as by stripping or manipulating payment messages, or making false representations to their U.S. or non-U.S. financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs, involved actual knowledge or involvement by the organization's management, caused significant harm to U.S. sanctions program objectives and/or were large or sophisticated organizations.

6. **Sanctions Screening Software or Filter Faults.** The Framework indicates that these faults have often been the result of failure to (i) update software to account for updates to OFAC's sanctions lists; (ii) include relevant identifiers, such as SWIFT Business Identifier Codes, of designated, blocked or sanctioned financial institutions; or (iii) account for alternative

spellings, such as Kuba, Habana or Soudan, despite the relevant organization operating in locations that use these spellings.

7. **Improper Due Diligence on Customers or Clients.** The Framework notes that an organization's due diligence on its customers is "one of the fundamental components" of an effective risk assessment and SCP, and that failures in this area can include improper or incomplete due diligence, including with respect to a customer's ownership, geographic locations, counterparties, and transactions, as well as their knowledge and awareness of OFAC sanctions.

8. **De-centralized Compliance Function and Inconsistent SCP Application.** Although the Framework notes that each organization should design, develop and implement an SCP based on its own characteristics, it explains that several organizations subject to U.S. jurisdiction committed apparent violations due to a de-centralized SCP, with personnel and decision-makers scattered in various offices or business units. The Framework lists several issues that may result from a de-centralized compliance function, including (i) improper interpretation and application of OFAC regulations, (ii) lack of a formal escalation process for high-risk customers or transactions, (iii) an inefficient or incapable oversight and audit function, or (iv) miscommunications regarding sanctions-related policies and procedures.

9. **Using Non-standard Payment or Commercial Practices.** The Framework cautions that, in many instances, organizations evade OFAC sanctions by implementing non-standard business methods to complete their transactions, and notes that organizations subject to U.S. jurisdiction are in the best position to determine whether a particular dealing, transaction or activity is consistent with industry norms and practices.

10. **Individual Liability.** The Framework notes that, in several instances, OFAC has identified individual employees, particularly those in supervisory, managerial or executive-level positions, as having played dominant roles in causing or facilitating violations of OFAC regulations. In some cases, employees of an organization's foreign entities made efforts to obscure and conceal their activities from others within the organization, including compliance personnel, as well as regulators or law enforcement. The Framework explains that, in these circumstances, OFAC will consider using its enforcement authority not only against the violating entity, but also against the individual.

G. RELATION TO DEPARTMENT OF JUSTICE GUIDANCE

In addition to the previously mentioned overlaps with the FFIEC examination manual, the Framework contains several elements also present in the U.S. Department of Justice's recently updated guidance on the evaluation of corporate compliance programs, including: the need for a risk assessment, the ways in which policies and procedures are reinforced through internal controls and integrated through periodic training, the extent to which senior management has communicated appropriate standards, the resources and autonomy allocated to the compliance program, and the importance of periodic testing, review and remediation of any underlying misconduct.

IMPLICATIONS

Although the Framework is consistent with OFAC's previous statements regarding the importance of organizations adopting risk-based SCPs, it provides useful guidance to organizations by outlining what OFAC considers to be the five essential components of an SCP and identifying ways that each component should be implemented. Application of the Framework will necessarily vary based on the nature and extent

of an organization's sanctions-related risks. In recent public remarks, an OFAC official described these components as the hallmarks of a high-quality SCP for a large, sophisticated financial institution and noted that other types of institutions—such as corporations engaged in the trade of goods and services—need to do their own risk assessment and choose the elements of an SCP that make sense given their circumstances.[20]

Nevertheless, several themes emerge when reviewing the Framework, including:

- the importance of considering sanctions-related risks in the mergers and acquisitions context, and the need to involve compliance personnel in both the transaction itself as well as the integration process;
- the critical role—and associated risks—that technology can play in an SCP, and the need for an organization not only to calibrate any technology solution to its risk profile (including the geographies in which the organization operates, as reflected in the misspellings example highlighted by OFAC in the root cause appendix), but also to ensure that it is updated to reflect key external and internal events, such as updates to OFAC sanctions lists and remediating deficiencies identified by the organization;
- the need for an organization to conduct a root cause analysis whenever SCP-related deficiencies are identified, whether through the audit or testing function or other source, and to take appropriate steps in response, including the use of compensating controls until the underlying weakness has been remediated;
- the need for an appropriate degree of SCP independence, including for SCP personnel to have oversight of senior management and for the testing or audit function to operate independently from the audited activities; and
- the importance of obtaining and effectively using know-your-customer information, which may substantially inform, among other things, an organization's risk assessment and internal controls.

Companies should carefully review the Framework to determine whether updates to their existing SCP should be made in light of this guidance. In some cases, companies may have already implemented aspects of this guidance in other contexts or for other purposes, but may wish to update relevant documentation to demonstrate an awareness and understanding of OFAC-specific guidance. As an example, the Framework expressly notes that one of the criteria that could be used to measure whether senior management has promoted a culture of compliance is the ability of personnel to report sanctions-related misconduct without fear of reprisal. In many instances, companies will have already established a whistleblowing policy that may address this aspect of the Framework, but a company could benefit from reviewing its existing whistleblowing policy to ensure that it is current and encompasses its SCP.

* * *

ENDNOTES

1 U.S. Dep't of Treasury, Office of Foreign Assets Control, "A Framework for OFAC Compliance Commitments" (May 2, 2019), https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf ("*A Framework for OFAC Compliance Commitments*").

2 Federal Financial Institutions Examination Council, Bank Secrecy Act Anti-Money Laundering Examination Manual, Examination Procedures: BSA/AML Compliance Program https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_008.htm.

3 A Framework for OFAC Compliance Commitments, 1.

4 U.S. Dep't of Treasury, Office of Foreign Assets Control, Settlement Agreements with Standard Chartered Bank, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/scb_settlement.pdf (April 9, 2019), and UniCredit Bank AG, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190415_unicredit_bank_ag.pdf (April 15, 2019).

5 A Framework for OFAC Compliance Commitments, 9–12.

6 U.S. Dep't of Treasury, Office of Foreign Assets Control, *Economic Sanctions Enforcement Guidelines*, Appendix A to 31 C.F.R. Part 501.

7 31 C.F.R. § Pt. 501, App. A, III.E.

8 OFAC Official, Panel Discussion at the American Conference Institute's Economic Sanctions Enforcement and Compliance Conference (May 3, 2019) ("*May 3 Remarks of OFAC Official*").

9 U.S. Dep't of Treasury, Office of Foreign Assets Control, Settlement Agreements with Standard Chartered Bank, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/scb_settlement.pdf (April 9, 2019), and UniCredit Bank AG, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190415_unicredit_bank_ag.pdf (April 15, 2019).

10 U.S. Dep't of Treasury, Office of Foreign Assets Control, Settlement Agreements with Standard Chartered Bank, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/scb_settlement.pdf (April 9, 2019), and UniCredit Bank AG, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190415_unicredit_bank_ag.pdf (April 15, 2019).

11 May 3 Remarks of OFAC Official.

12 A Framework for OFAC Compliance Commitments, 1.

13 A Framework for OFAC Compliance Commitments, 2.

14 A Framework for OFAC Compliance Commitments, 2.

15 May 3 Remarks of OFAC Official.

16 A Framework for OFAC Compliance Commitments, 5.

17 The Framework indicates that one aspect of testing and auditing is that, upon learning of a confirmed negative testing result or SCP-related audit finding, an organization will take immediate and effective action to identify and implement compensating controls until the root cause of the weakness is remediated. During recent public remarks, an OFAC official explained that this recommendation is premised on the audit finding or testing result being meaningful and relevant to the organization's SCP and acknowledged that a dialogue among the appropriate stakeholders may be necessary as, for example, certain findings may be more AML-focused in nature. May 3 Remarks of OFAC Official.

18 A Framework for OFAC Compliance Commitments, 7.

19 May 3 Remarks of OFAC Official.

20 May 3 Remarks of OFAC Official.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York

Thomas C. Baxter Jr.	+1-212-558-4324	baxtert@sullcrom.com
Nicolas Bourtin	+1-212-558-3920	bourtinn@sullcrom.com
David H. Braff	+1-212-558-4705	braffd@sullcrom.com
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Elizabeth T. Davy	+1-212-558-7257	davye@sullcrom.com
Stephen Ehrenberg	+1-212-558-3269	ehrenbergs@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
Wendy M. Goldberg	+1-212-558-7915	goldbergw@sullcrom.com
Charles C. Gray	+1-212-558-4410	grayc@sullcrom.com
Shari D. Leventhal	+1-212-558-4354	leventhals@sullcrom.com
Mark J. Menting	+1-212-558-4859	mentingm@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Samuel W. Seymour	+1-212-558-3156	seymours@sullcrom.com
Adam J. Szubin	+1-212-558-7204	szubina@sullcrom.com
Stephanie G. Wheeler	+1-212-558-7384	wheelers@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com

Washington, D.C.		
James A. Earl	+1-202-956-7566	earlja@sullcrom.com
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Los Angeles		
Patrick S. Brown	+1-310-712-6603	brownp@sullcrom.com
London		
Craig Jones	+44-20-7959-8488	jonescra@sullcrom.com
Tokyo		
Keiji Hatano	+81-3-3213-6171	hatanok@sullcrom.com