

# Developing a Sanctions Compliance Program (SCP)

A Spotlight on the Core Elements of an  
Office of Foreign Assets Control (OFAC)  
Sanctions Compliance Program

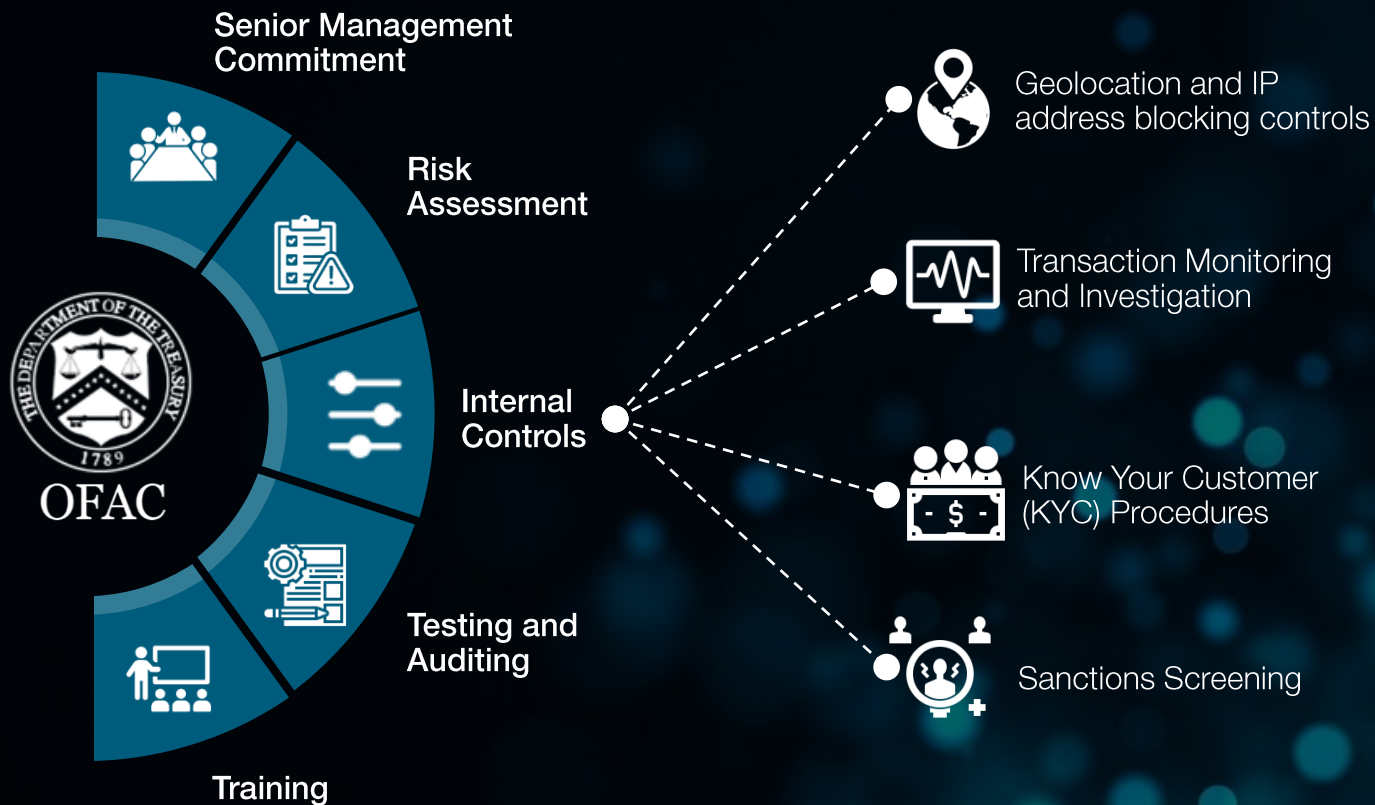


RISK | STRATEGY | CYBER | COMPLIANCE MANAGEMENT



# OFAC Sanctions Compliance Program

In 2019, the Office of Foreign Assets Control (OFAC) issued a Framework for OFAC Compliance Commitments as guidance on the integral components of a sanctions compliance program (SCP). The framework is applicable to companies and organizations within the scope of the US jurisdiction, including foreign entities utilizing services and goods from the US, or conducting business in the US and with US persons. The guidance also elaborates on how OFAC incorporates the components of an SCP when investigating, evaluating and resolving apparent violations, which may lead to settlements.





# OFAC Guidance on the SCP Components



## Senior Management Commitment

- Review, endorse, and approve the sanctions compliance program, policies and procedures.
- Delegate sufficient authority and autonomy for compliance units to deploy policies and procedures.
- Ensure that adequate resources are assigned to support the compliance function, whether it be associated to expertise, information technology, human capital or oversight, among others.
- Promote a culture of compliance.
- Appoint a dedicated and qualified sanctions compliance officer to oversee all compliance areas.
- Demonstrate recognition of the gravity of apparent violations of laws and regulations administered by OFAC, as well as the identification and remediation of deficiencies, failures or points for improvement in compliance.



## Internal Controls

- Implement adequate internal controls that address an organization's risk profile, compliance needs and the results of the risk assessment.
- Enforce and validate compliance to policies and procedures through internal or external audits.
- Ensure that OFAC-related recordkeeping policies and procedures are followed.
- Take immediate and effective action upon the determination of failures or deficiencies.
- Clearly communicate SCP's policies and procedures to all relevant staff, personnel and external parties.
- Designate personnel who will integrate the SCP's policies and procedures into the day-to-day operations.



## Risk Assessment

- Conduct a sanctions risk assessment in a manner and frequency appropriate to potential risks posed by clients, products, services, counterparties, intermediaries, transactions, geographic locations, partners, and nature of the organization.
- Develop a methodology that distinguishes, analyzes, and addresses identified risks, combined with the process of updating the SCP and the risk assessment itself to account for systemic deficiencies or apparent violations, if any.



## Testing and Auditing

- Ensure that the testing and audit function is accountable to senior management, and has the sufficient authority, expertise, qualifications, resources and autonomy within the organization.
- Employ testing and audit procedures that are commensurate to the size, level and complexity of its SCP.
- Take immediate action and implement compensating controls upon the discovery of negative audit results or findings.



## Training

- Provide regular OFAC and sanctions-related training that is appropriate to the organization's risk assessment, risk profile, products and services, and to the training audience (e.g., staff level, senior management, stakeholders, or third party).
- Ensure that any negative findings from audits, testing or normal course of business are addressed through update or remediation trainings.



# OFAC Reporting Requirements

Under OFAC's Reporting, Procedures and Penalties Regulations (RPPR) and guidance, the following are the key reporting requirements:

## Reports on blocked, unblocked or transfer of unblocked property and rejected transactions



The initial reporting for blocked properties, including when they are unblocked or transferred, and blocked or rejected transactions need to be reported by any US person within 10 business days of the action or occurrence date.

## Voluntary Self-Disclosure

A notification to OFAC initiated by a subject person who committed or participated in an apparent violation of a statute, which must be submitted prior to or simultaneous with the discovery by OFAC or another government agency of the apparent violation.



## Annual Report of Blocked Property (ARBP)



The ARBP needs to be filed by any US person that has possession or control over any blocked property by September 30 and needs to include the total quantity of blocked accounts as of June 30 of the same calendar year.

## Annual Certification of Compliance

Requires a senior-level executive or manager of an entity under a Settlement Agreement with OFAC to annually provide a certification for five (5) years to confirm that the settling party or entity has implemented and continues to maintain its compliance commitments with OFAC.



OFAC



Discover  
what  
Stratis  
Advisory  
can do  
for you



## **OFAC Sanctions Risk Assessment**

Whether a financial institution, logistics company, import/export company, etc. understanding your exposure to OFAC sanctions programs and the quality of implemented risk mitigants is critical to maintaining compliance with OFAC. Stratis can execute your OFAC risk assessment to identify broader risk identification and control mitigation across your business operations.



## **Screening Vendor Due Diligence, Implementation, Testing, and Gap Analysis**

Multiple vendors provide list screening services from limited to exhaustive lists. However, most of those vendors focus exclusively on name screening at onboarding and in transactions. Compliance with OFAC sanctions requires broader systems, inclusive of cybersecurity systems, to form a comprehensive screening program. Stratis can help you assess vendors, implement, tune, and test your new screening systems, and tune and gap existing systems to ensure appropriate coverage.



## **NYS DFS Part 504 Annual Transaction Monitoring and Watchlist Filtering Certification of Compliance**

Operating as a New York State Department of Financial Services (NYS DFS) regulated institution such as a bank, insurance company, money transmitter, trust company, etc. (or applying for a license) requires an organization to annually certify to maintaining a compliant transaction monitoring (AML) and watchlist filtering (OFAC) program. Stratis can assess the readiness of your organization to submit a certification of compliance prior to the annual April deadline.





