The sanctions risk assessment

A challenging exercise that results in a powerful tool

December 2021

kpmg.com

Recently, there has been a lot of discussion about the importance of conducting sanctions risk assessments. As the foundation upon which the compliance program is built, it is critical that such assessments are undertaken in a methodical and comprehensive manner. From our work with multinationals of various sizes, we've found several leading practices to be particularly effective. This article is intended to help organizations that may be ready to execute their first risk assessment, as well as those seeking to validate or improve their existing methodologies.

Why are risk assessments crucial?

While the financial services industry has long understood the importance of risk assessments,[1] those outside of banking haven't necessarily had the same expectation spelled out by a regulator until very recently, when the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) published its Framework for OFAC Compliance Commitments (Framework).[2] Other elements of an organization's Sanctions Compliance Program (SCP) depend on an effective risk assessment, or as OFAC states, "the results of a risk assessment are integral in informing the SCP's policies, procedures, internal controls, and training in order to mitigate such risks."[3] The Framework recommends that organizations undertake routine risk assessments to identify and mitigate organizational vulnerabilities, and that the exercise should generally consist of a holistic review of the organization from top to bottom and assess its touchpoints to the outside world.

The Framework provides two key considerations in evaluating the risk assessment program:

1. **Risk assessment program:** The organization conducts, or will conduct, an OFAC risk assessment in a manner, and with a frequency, that adequately accounts for the potential risks. The risk assessment will generally inform the extent of the due diligence efforts at various points in a relationship or in a transaction (e.g., through a Know Your Customer or Customer Due Diligence process and sanctions compliance integration into the merger, acquisition, and integration process). Examples of ongoing risk assessments include at the time of onboarding a supplier or other third party, or during mergers and acquisitions.
2. **Risk recognition methodology:** The organization has developed a methodology to identify, analyze, and address the particular risks it identifies. As appropriate, the risk assessment will be updated to account for the conduct and root causes of any apparent violations or systemic deficiencies identified by the organization during the routine course of business, for example, through a testing or audit function.

While the first consideration seems fairly straightforward, the actual nuts and bolts of such an exercise may not be as easy to plan. However, we often find that the second consideration (methodology) requires extra consideration to ensure it is properly aligned with a company's unique risk profile.

Where do we begin?

The foundational element of a successful risk assessment is the collection and documentation of an organization's touchpoints with the world. We call this document the "touchpoint inventory." During the touchpoint inventory step, you should identify areas of potential sanctions risk, including reviewing existing products and services, geographic footprint, customer base, and transaction types. While some of this can be accomplished through review of existing documentation, interviews with key stakeholders throughout the organization are crucial to confirm that the documentation accurately reflects the current state, and to identify additional gaps. We have found in our work that documentation of risks and controls often lags identification of the same. While management may believe that relevant documentation accurately reflects what is happening, interviews with stakeholders closer to day-to-day operations can provide additional valuable insights. In addition to mapping counterparties, the touchpoint inventory exercise may also include data mapping to understand the information associated with each counterparty, process flows, and how it is maintained in the organization's systems. Each supporting system and data intake mechanism should be fully documented, and screening activities should be identified and assessed. The resulting touchpoint inventory, while useful in its own right, will also serve as the starting point for a risk and control matrix, which is further discussed below.

Looking at inherent risks

Once the touchpoint inventory has been completed, you are ready to identify inherent risks within the organization's specific businesses to inform risk-based decision-making and controls. During the inherent risk assessment step, the organization should use a defined risk scoring methodology to determine and quantify inherent sanctions risks. While we might wish that OFAC would provide a risk scoring methodology, there's actually a good reason that they don't. Each organization has a unique risk profile and its risk scoring methodology should be calibrated to the organization's unique circumstances. The most important step is to fully document how and why you choose the scoring methods you intend to use. In the event that a potential sanctions violation is reported to OFAC, and OFAC determines that the potential violation occurred in part due to an issue with the risk assessment, showing OFAC that you thoughtfully chose reasonable methodologies can mean the difference between a substantial fine and a small penalty, or even a cautionary letter with no financial penalty.

---

[1] For example, see the BSA/AML Risk Assessment section of the FFIEC's BSA/AML Manual.
[2] Source: "A Framework for OFAC Compliance Commitments" published by the U.S. Treasury Department's Office of Foreign Assets Control.
[3] Ibid.

The following examples are some of the factors an organization might consider when determining inherent sanctions risk ratings:

Customer base	Board of directors
Customer risk	Staffing
Products	Sourcing
International transactions	Accountability
History of violations	Training
Management	Quality control
Culture of compliance	Policies
Systems	Self-testing
Independent testing	Corrective actions

Once completed, the results can be documented in a table summarizing the results of the sanctions inherent risk assessment, remembering to also fully detail the risk calculation analysis.

Identifying mitigating controls

Once the inherent risks are documented, it's time to identify any mitigating controls. The primary purpose of mitigating control identification is to outline clear expectations, define procedures and processes pertaining to sanctions compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessment. For each inherent risk identified, the organization should assess whether there is a mitigating control, which can be learned through interviews and documentation review. When collecting information, keep in mind the topics described in the table below that are viewed as primary components of an effective SCP by regulatory bodies and industry guidance.

Control environment		
Compliance pillar	**Strength indicators**	
Management Commitment, Governance & Culture	— Clarity and execution of board responsibilities — Key stakeholders have reviewed the results of risk assessment	— Management expertise, involvement, and responsiveness
Policies & Procedures, and Other Internal Controls	— Applicability, depth, and coverage of regulatory requirements	— Formal evaluation and approval process — Sufficiency of procedures
Staffing & Training	— Training coverage, frequency, and completion — Effectiveness of training — Employee skill set in compliance	— Employee turnover — Accountability: Discipline and penalties for noncompliance
Testing & Auditing Program	— Scope, depth, and frequency — Analysis of results	— Issues management and escalation processes — Report adequacy and timeliness
Monitoring & Reporting Program	— Scope, depth, and frequency — Report adequacy and timeliness	— Key performance indicators/key risk indicators adequacy and frequency
Hotlines & Escalations	— Timeliness and completeness of issue intake and disposition	— Analysis of complaint trends and root cause — Report adequacy and timeliness

Once completed, the results should be mapped to the inherent risks identified in the previous step to enable residual risk analysis.

Putting it all together: Evaluation of residual risk, final risk rating, and the risk and controls matrix

In the fourth and final risk assessment phase, the organization will document the residual sanctions risk that remains against the inherent risk identified leveraging control-related information learned through interviews and review of relevant documentation. Based on the results of the residual risk calculation, a final sanctions risk rating for the organization can be assigned.

While the OFAC Framework sets forth the expectation that an organization has implemented internal controls that adequately address the results of its risk assessment and profile, it does not prescribe how to track and monitor internal controls. Instead, it simply states that "[they] should enable the organization to clearly and effectively identify, interdict, escalate, and report to appropriate personnel within the organization transactions and activity that may be prohibited by OFAC."

One such way to address this standard is via a risk and control matrix, a tool that can help an organization identify, rank, and implement control measures to mitigate risks. It serves as a repository of risks that pose a threat to an organization's operations, as well as the controls in place to mitigate those risks. To address comprehensive risk, the organization can add to the touchpoint inventory additional factors for each risk such as the frequency, the type of control (preventative/detective; automated/manual), system used, residual risk if any, and an analysis of how effective the controls are in addressing the perceived risk. Furthermore, to align with the expectations set out in the OFAC Framework, the risk and control matrix should clearly address all areas of the Framework such as management commitment, risk assessments, training, and auditing. The risk and control matrix should be a living document—meaning as risks and controls change, the matrix should be updated to reflect the current state.

Are we done now?

An organization's risk assessment is only as effective as it is current. While some companies may choose to only conduct risk assessments every few years, leading practice is to revisit the risk assessment annually, as well as when the risk profile is likely to change, such as introducing new products, entering new markets, or acquiring other businesses. When these events occur, it makes sense to ensure that any associated risk changes are promptly identified and assessed so that applicable controls can be added or tuned appropriately.

Additionally, a risk assessment can help uncover business changes that the sanctions team was unaware of—but may impact compliance. Sanctions compliance teams may not have full visibility into the daily business operations that would enable them to easily identify when risks creep into the organization. The risk assessment facilitates this deep dive that leads to robust compliance procedures.

How KPMG can help

The KPMG Export Controls and Sanctions practice is composed of sanctions professionals who have deep experience developing compliance solutions that are effective, scalable, and sustainable. Our technical experience is supported by sophisticated automation that accelerates information collection and analysis. We understand the many challenges multinational companies face in conducting cross-border transactions. We bring this knowledge with us when we design and execute risk assessments—leading to insightful results that not only provide visibility into business operations but also support development of compliance procedures.

Sanctions management is complex. But we bring methodologies that streamline compliance.

Contact us

Steven Brotherton
Principal, U.S. & Global Export Controls & Sanctions Leader
T: 415-963-7861
E: sbrotherton@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia