COSMOS
Navigate the Compliance Universe

SCCE Compliance 101 Third Edition
Chapter 5. Risk Assessment

Risk assessments must be dynamic and ongoing: *dynamic*, to address the changing risks of the organization, and *ongoing*, to continually review and prioritize the risks of the organization. Conducting a risk assessment when you first start your program assists you in understanding the cultural variables related to risk, such as how tolerant the organization is to take on more risk and whether there is management accountability to resolve or mitigate risk. Risk assessments help identify priority risk areas to target when building the compliance program's education, auditing, monitoring, and communication plans. This is an essential process for launching an effective compliance program.

A baseline compliance risk assessment forms the foundation of a new compliance program. The dynamic nature of an organization and its risk portfolio requires an ongoing look at priority risks to keep the program aware of real, potential, and emerging risk areas that need to be monitored and addressed.

Baseline Compliance Risk Assessment

After completing the initial infrastructure design, the next step in launching an effective compliance program is conducting a baseline compliance risk assessment of the organization's operations. A baseline compliance risk assessment is the starting point for understanding the compliance risk profile of an organization. The baseline can then be used to compare the risk environment of the organization at one point in time with another point in time, usually year to year.

Establishing this information for the compliance officer and the management team assists in determining the progress made in minimizing or resolving identified risks or in potential areas of vulnerability. Also, as you review risks dynamically and on an ongoing basis, you will be able to compare findings to the baseline risk assessment to determine if new risks have been identified and/or whether the baseline risk assessment has changed.

Consider current risk assessment activities already occurring in the organization when developing processes for conducting the baseline compliance risk assessment. The compliance officer should not duplicate efforts around this process. Consider leveraging other activities that might be related to gathering risk information, such as internal audit risk assessments and security risk assessments.

Ongoing Risk Assessment

Established programs also need to conduct ongoing risk assessments to provide spot checks for identifying new risks or to evaluate if risks may have escalated since the baseline compliance risk assessment was conducted.

The methodology for ongoing risk assessments can vary. Depending on the organization's capacity and available resources, ongoing risk assessments can be performed throughout the year as a mini version of the annual or initial baseline compliance risk assessment. Ongoing risk assessment activities could include using baseline results and interviewing management to identify any areas that have escalated, been resolved, or have emerged since the last assessment activity occurred. Frequency of conducting the ongoing risk assessment also varies according to capacity and resources available. However, it is recommended to review the previous results against the current state at least once or twice during the year to ensure that the compliance program elements are

continually addressing the organization's key risk priorities and to minimize any surprises.

Conducting Risk Assessments

Your approach and methodology to a compliance risk assessment can vary depending on the available resources, size of the organization, and risk tolerance and appetite of the organization, but there are some basic elements to all risk assessments regardless of the approach and methodology. Considerations and the basic elements follow.

Risk Assessment Pre-Work

There are three main areas of prework to do before beginning your risk assessment. They include understanding the following:

- The organization's culture
- The organization's risk appetite and tolerance
- The compliance officer cannot conduct extensive organization-wide compliance risk assessments alone

Understanding the Organization's Culture

To learn more about your culture, certain questions to consider may include: Is there board oversight in ensuring management systems and controls are working? Is management held accountable for mitigating risks? What is the board's understanding of the real and potential compliance risks of the organization? Questions regarding your management team and its support of the compliance efforts are important to ask as well. These activities are important for helping to understand the tone of accountability, appetite for risk, and risk management structure in the culture. If the organization's culture is unsupportive of resolving and mitigating risks, the compliance professional should work with senior leaders and the board to improve those aspects before moving forward with a risk assessment. If the compliance officer is being instructed by the board or senior management to put a compliance program in place, it must be understood that the culture and tone of the leaders and board are essential for the success of the organization's compliance program. A risk assessment will identify risk priorities that need to be addressed. If the culture lacking accountability or support of compliance efforts remains the same, the risk assessment's identified priorities will only result in more risks not being mitigated or resolved. The risk assessment process and documentation could then ultimately increase legal risks to the organization. For these reasons, the timing may not be appropriate to conduct a risk assessment. However, the compliance officer should at least review any activities that might already be occurring around compliance and consider how to build on them when developing the compliance structure.

There are compliance programs that have proceeded with the risk assessment process, even when the cultural environment does not support the program. Programs such as these usually struggle to establish a strong compliance infrastructure because the cultural tone doesn't support building a firm foundation. The compliance professional who leads such a program in these circumstances often winds up being the "owner" of a program that will disappear if they should leave. That is why organizational buy-in and ownership of the compliance efforts are essential for an effective compliance program.

Understanding the Organization's Risk Appetite and Tolerance

Before conducting the risk assessment, be aware of the risk appetite and tolerance of the culture. *Risk appetite* refers to the level of risk an organization is willing to accept in pursuit of its business objectives before action is deemed necessary to reduce the risk. *Risk tolerance* is the acceptable levels of variation in performance related to

achieving an organization's business objectives. If the organization's culture has an increased risk appetite, then its risk tolerance will be high, and this might influence how risks are mitigated (or if they even *will* be mitigated). Organizations going through growth tend to have increased risk appetite and risk tolerance. As such, risk is inherent to their strategic goals. If the company is not considering growth and the organization is stable in its business, there may be a decreased risk appetite; however, its risk tolerance can vary depending on the culture in these situations. Additionally, in these types of organizations, risk can be higher due to complacency around controls in place. For instance, approval policies and processes may be in place, but the individual accountable for them may be lax or is no longer attentive to details. Such complacency creates risk, even when a control was meant to decrease or mitigate the real and potential risks.

Understanding That the Compliance Officer Cannot Conduct Extensive Organization-Wide Compliance Risk Assessments Alone

Management should understand the value of conducting a risk assessment, the methodology that will be used, how outcomes will be reported, and expectations once the assessment is completed. To obtain board and management buy-in to conduct a risk assessment, education needs to be provided that emphasizes these points and the benefits of conducting risk assessments, such as decreasing surprises, identifying potential risks that are escalating, awareness of current culture, and gathering real-time risk intelligence. Members of management should be a part of the risk assessment process to ensure they understand what the assessment entails and are willing to participate in prioritizing identified risks, which helps increase buy-in and awareness of organization's culture. Having resources for conducting the risk assessment process and ensuring identified risks are prioritized is important to an effective outcome, even if you are leveraging another effort within the organization.

Consideration may be given to having an outside expert conduct the organization's compliance risk assessment, but such a decision still requires the compliance professional be actively involved in the assessment. Even with outside specialists, having an internal champion for this process is important for providing background and an understanding of the organization's operations and for deciphering the results (which will need to be acted upon by management). Internal buy-in is critical for the risk assessment process and outcomes, and this buy-in may be diminished if an outside party conducts the risk assessment process.

Once the decision is made whether or not to use a consultant, it is important that the compliance officer gets the internal assistance and support of an executive-appointed risk assessment team. This team could later be a core group that becomes the compliance committee, especially because the team will have firsthand knowledge of the risk assessment outcomes and understand the intelligence gathered from the process. Among the risk assessment team members, there should be people with experience and expertise in the organization's operations, legal, finance, compliance, and other functions you think should be represented.

When starting the risk assessment discussions and process, be sure to include multidisciplinary teams from management to assist with buy-in and follow-up on the key risks identified.

Risk Assessment Approach

How the assessment is conducted depends on culture and resources, yet conducting a risk assessment is an essential step for any organization's compliance program efforts. You'll need to work with your management committee to identify available resources and the approach you think would be effective.

Here are a few of the resources available to help you decide which risk assessment approach to take:

- **Committee of Sponsoring Organizations of the Treadway Commission (COSO): *Enterprise Risk Management***

—Integrating with Strategy and Performance. [1]

- **SCCE & HCCA and COSO, *Compliance Risk Management:Applying the COSO ERM Framework.*** [2]
- **International Organization for Standardization (ISO) resources, such as ISO 37001:2016.** [3] While the focus of such resources is anti-bribery, the content could be applied generally to a compliance program reviewing any previous problem areas identified through internal audits, hotline complaints, investigative reports, and regulatory queries.
- **Industry and regulatory settlements.** Penalties and fines might identify key issues that would relate to your industry segment.
- **Trade and professional associations for the organization's industry.** These can provide information on current issues and emerging trends as well as identify potential areas for consideration in developing the risk assessment.
- **Hotline trends.** These are useful to consider as they will give some indication of the cultural issues as well.
- **Trends from investigations.** These should be considered during your risk assessment process.

The two primary sources of information for the assessment team are documents and staff. Documentation review should begin with an in-depth look at any previous audit reports to identify apparent policy gaps and potential vulnerabilities. Are the policies and procedures appropriate? Do the policies reflect practice or are they known to exist *only* in writing? Review actual practices related to those policies and procedures as well as regulatory concerns. Do the policies and procedures apply accurately to rules, laws, and guidance? Check, too, for availability of policies and procedures. Does staff have ready access? Do staff members know they have access?

It is important to include in your assessment where gaps may be in current educational and training practices. You may need to solicit training information from individual departments if there is no centralized system. Education plans, syllabi, handouts, and all attendance records should be reviewed and evaluated. Include information on outside education as well. A new program will use this information to identify gaps that will need to be addressed in the education plan. A more mature program might pursue a more detailed understanding of the root cause of inefficient education, or why current efforts do not seem to be working.

Whatever the findings of the risk assessment, whether baseline or ongoing, staff need to be educated on the risks and any changes resulting from existing training efforts, as well as implementation of or changes to the compliance program. If there are weaknesses in the educational program, they must be addressed as early as possible. The identified risk assessment priorities will help you better design compliance educational and training programs. Often the baseline assessment will inform your plan in your new program. Ongoing risk assessments will identify where there may be gaps in addressing key priority risks in the educational plan and compliance efforts, which should evolve to address current compliance risk priorities.

Depending on your approach, after collecting any available information, interviews are usually part of the assessment. Who you interview depends on resource availability. At a minimum, you should include representatives from the board, senior management, and other levels of talent to get a sense of their perception of the organization's risks. Questions commonly asked are related to the individuals being interviewed, their roles, and their views on risk priorities related to the organization's operations and strategies.

You could start by interviewing managers best acquainted with the organization's operations. Become familiar with the interviewee's frame of reference and overall strategic objectives of the organization and then tailor your

questions accordingly. For instance, you might ask a chief financial officer, "From your perspective, are there any obstacles in achieving the company's strategic goal of growth?" This might be a better question for getting an in-depth answer from the frame of reference of the chief financial officer vs. a question similar to, "What are the top three risks that keep you awake at night?"

Interviews are also an excellent opportunity to represent the compliance program. Begin your discussion with information about your role, plans for the compliance program, and the process that you are following to get a sense of the risks in the organization. Be sure to explain the purpose of the interview and the assessment, and, if possible, mention what follow-up processes will be completed. This is your opportunity to explore what is currently occurring and to identify managers' areas of concern. Some sample topics for discussion are:

- Functions and controls that are subject to frequent breakdowns
- The current compliance environment in the department
- The process for monitoring issues and how that information is reported
- How the department's policies and procedures are developed and updated
- How the department verifies that policies and procedures are being implemented accurately
- What communication occurs related to risk areas and mitigation of risks