COSMOS
Navigate the Compliance Universe

Compliance Risk Assessments - An Introduction
Chapter 9. Beyond the Compliance Risk Assessment Process

Chapter Goal:

- Understand the basics of an effective compliance and ethics program.

You've made it through the basic steps for developing and implementing a compliance risk assessment and mitigation plan, ranging from identifying the universe of risk to putting a monitoring system in place for the compliance risk mitigation plan. Time to sit back and finally get to eat that cake, right?

While tempting, you're not done yet. If your business intends to adopt a complete ethics and compliance initiative, you need to consider some other elements and how they fit with compliance risk assessments to form an effective ethics and compliance initiative.

Compliance Structure

The model used in this chapter describes an effective compliance and ethics program as defined by the USSG. These guidelines represent best practices for organizations based everywhere in the world.

Just as you cannot design, implement, and monitor a compliance risk assessment program on your own, you need the support of the CEO, board, and upper management to establish the structure for a compliance and ethics program. At a minimum, the compliance structure needs to have high-level personnel who've been assigned responsibility for the program.[1] How the team effort is structured within your organization is a decision that should be made based on conversations with the CEO, other upper management, the board (if your organization has one), and industry leaders. The structure must work for your organization, not for someone else's organization.

Hiring a full-time compliance officer sounds like an easy fix. However, that may not be the right fix for a decentralized business with no previous history in compliance initiatives. Perhaps that organization might benefit from a committee structure with direct reporting lines to the board and/or CEO.

Regardless of the structure you pick, the key is to remember that the individual(s) leading this effort must have unfettered and direct access to the decision-makers (CEO, other upper management, or board). And the employees held accountable for developing policies, procedures, and training regarding compliance with a law need training on the law and resources to help your organization comply with the law.

Hiring Practices

Best practices require that the organization use reasonable efforts not to hire "substantial authority personnel" whom the organization knew, or should have known, engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.[2] Simply put, you should hire employees who are willing to work to ensure that your company will comply with the law, attend trainings to gather knowledge about the

laws, and understand their responsibilities to report noncompliance with the law. In other words, are your hiring practices netting employees that can embrace your corporate culture of compliance?

If those types of employees aren't being hired or, alternatively, if your organization's employees do not embrace a philosophy of compliance and you continue to employ them, are you really surprised that you have issues of noncompliance? Your business needs to do a good job vetting candidates to find those applicants, and ultimately employees, who will be able to contribute to your effective compliance and ethics program.

Written Standards and Procedures

According to best practices, for an organization to have an effective compliance initiative, the organization must have written standards and procedures and communicate those standards and procedures to its employees.[3]

This requirement sounds easy, right? Just write standards down and hide them in the employee manual that everyone signs on the first day of employment. And, of course, expect the employees to know these policies and follow these instructions. Sorry—*that is not likely to work.* An employer needs to develop standards of behavior and communicate those standards to employees. Typically these standards, policies, and procedures are called a Code of Conduct or Code of Ethics.

Think of these policies and procedures as the backbone of the compliance initiative. Clearly articulated policies written in easy-to-understand language will bring this initiative one step closer to being successful. Find a centralized spot (on an internal website, in a policy manual, in an app, or whatever method of communicating is best) and make sure all the policies are there. What can be worse than disciplining an employee for failure to comply with a policy when the employee is sobbing in front of you and saying, "I didn't know we had a policy; no one told me. Where is it?"

One other hint for developing policies—make the process of developing the policy as transparent as your business, industry, or country allows. You will get more buy-in and compliance with a policy if employees perceive that the policy was written to help them, its authors actually had the expertise to write the policy, and noncompliance with policy will not automatically result in a "gotcha" mentality.

Training and Education

Best practices require you to conduct effective compliance training programs.[4] This requirement is critical; if your company does not value training and education, then a compliance initiative is doomed from the beginning. You cannot have a compliance initiative without a well-trained workforce that is aware of compliance issues.

One hint—however you decide to implement training about a particular policy, consider these following ideas:

- Make sure that whomever is being trained really needs to be trained about compliance with a particular law.
- Make the training as interactive and interesting as you can, based on the subject matter.
- Remember who your audience is and adapt the training method and training time accordingly.
- Document the training and who attended the training.

Compliance Program Communication

Implementing a compliance risk assessment initiative could make your employees believe that the Orwellian Big

Brother has arrived. Likewise, the most basic misconception about an ethics and compliance program is that it involves all new actions and represents something management dreamt up over the weekend to add more work to an already overburdened workload. This perspective could not be further from the truth. In order to have an effective ethics and compliance program, the organization must take reasonable measures to periodically communicate the elements of the program.[5]

Focus on building awareness that this effort is nothing new and the program is simply a method of formalizing the process. Communicate how the initiative was developed and how and when it will be implemented in order to lessen possible employee resistance.

If you are a *Star Trek* fan, you will understand this reference: "resistance is futile." If you are not a *Star Trek* fan, just note that employee resistance to the initiative *will occur*, and it is your job as a compliance professional to get ahead of the resistance and smooth the path to achieve a relatively painless implementation process. Having a well-developed communication plan will result in the path of least resistance.

Publicized Reporting Mechanisms and Follow-up

An effective compliance program also needs to "have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retaliation."[6] What does this mean for your business?

Simply put, your organization must design a reporting system and have that system in place for employees to report noncompliance issues—and those reports must be made without employees fearing retaliation. In order to achieve this requirement, your business must have a reporting process—either internal or third-party reporting. Typically referred to as a hotline, this reporting mechanism allows employees to anonymously report noncompliance issues.

A few items need to be in place before a reporting process can work effectively. First, be careful when naming this policy—typically either "Reporting Policy" or "Whistleblower Policy" has been used. Your industry practices may decide this for you, but if you have the choice, consider using the label of reporting policy rather than whistleblower policy. "Whistleblower" has a connotation of "I am getting my business in trouble" while "reporting" has a less-threatening connotation that empowers an employee to feel that he or she is doing the right thing by reporting noncompliance.

Second, establish what "types" of noncompliance can be reported through your internal or external process. Ideally, the business should not only encourage the reporting of criminal acts but also other forms of misconduct. And each business needs to clearly articulate what the disciplinary actions will be if an employee fails to report noncompliance.

Third, you need to have a nonretaliation policy in place. This policy needs to state that anyone who makes a good faith report of noncompliance through the reporting system will not be subject to retaliation. There are different ways to handle this; just ensure that every employee knows that they will be protected from retaliation if they report instances of misconduct.

Monitoring and Auditing

For an ethics and compliance program to continue to be effective, simply following up on reported incidents of possible misconduct won't be enough. A system for continual monitoring and/or auditing of all risk areas must

be established.[7] The good news: If you have completed your initial compliance risk assessment then you are in an excellent position to establish a schedule for ongoing monitoring and auditing. Typically, the highest risks will be scheduled for the most aggressive reviews, while low-risk issues can perhaps be scheduled for a once-a-year audit. An advanced program will mesh the compliance risk assessment initiative with its monitoring and auditing schedules.

Enforcement and Discipline

To ensure employees know that your organization will appropriately respond to reports of misconduct, each reported case needs to be investigated. In addition, fair and consistent forms of discipline must be established.[8] Employees have ways of finding out if C-suite officials have committed misconduct and the episode was swept under the rug. So, for instance, if a higher-level manager gets caught padding expense reports, he or she must be disciplined in the same way as a lower-level employee. Likewise, if a low-level supervisor is found to have committed sexual harassment and fired as a result, then a top-level manager committing a similar form of sexual harassment will also need to be fired.

Response and Prevention

After a compliance failure has been discovered and dealt with, best practice requires that an organization review its ethics and compliance program to understand what caused the failure and then modify its program to prevent similar forms of future misconduct.[9] Continuous improvement is key for ensuring ongoing effectiveness of an ethics and compliance initiative.

These standard elements of an effective ethics and compliance program have been time-tested by organizations around the world. Putting these pieces together into a systematic process takes time and effort. But conducting a compliance risk assessment can be a great springboard into developing a full ethics and compliance program. Don't despair; keep your focus on the prize.

Action Item:

- Determine whether your organization is ready to establish an ethics and compliance program, or if it already has one, make sure all major elements are included.