COSMOS
Navigate the Compliance Universe

Compliance Risk Assessments - An Introduction
Chapter 8. Step Six: Implementing a Compliance Risk Mitigation Plan —Monitoring, Reassessing, and Modifying

Chapter Goals:

- Understand why continual compliance risk monitoring is needed.
- Determine how to develop a customized system to continuously monitor the compliance risk assessment initiative.
- Determine your compliance risk reassessment time schedule.
- Decide how to document monitoring the compliance risk assessment program.

At this point in your compliance risk assessment program, you have completed the following:

- Identified the compliance risk universe;
- Determined the compliance risk factors, such as likelihood of occurrence and impact of occurrence;
- Conducted the compliance risk assessment survey;
- Scored the survey results and generated a risk universe matrix; and
- Developed and had approved by the CEO or other upper management your initial compliance risk mitigation plan.

What is next? With all that work completed, one might be tempted to sit back and congratulate oneself on a job well done. Well, the job might have been performed "well," but it certainly is not "done."

For your compliance risk assessment program to be of ongoing use to the overall compliance program, best practice requires ongoing monitoring of all compliance risks. And clearly, compliance work is never really finished. Laws change, employees change, and the focus of upper management changes. It is certain that there will always be change; you just cannot predict how the change will affect a compliance initiative. Just know that it will.

The key is having a continuous improvement system in place that provides enough flexibility to adapt to a changing environment. But the key also requires having enough rigidity in the system to ensure that the compliance initiative will not falter when the new hotshot manager arrives in your division and wants to shake things up.

If you are the compliance officer, your job is to develop and maintain this continuous improvement system. How do you begin accomplishing this task?

Monitor

The first step is to develop a continuous daily compliance risk monitoring process. Customization for your business is critical. What should you include in your plan to keep the risk assessment process going for your employees and management? And how should you monitor continued effectiveness of the program? Here are some tactics you can try:

- **Develop and publicize a compliance calendar**. Identify when reports are due to federal or state agencies and even when reports are due to internal departments.
- **Perform random audits**. If training on a law or policy was supposed to occur, ask the employee responsible for documenting such training to show you the documentation.
- **Attend the training sessions**. Are they well prepared, well presented, informative, and engaging? What changes could be made to make them more effective training programs? Is the information up-to-date? Is it accurate? Are you training everyone or are you spending time to determine who should be trained on what policies and just training those employees?
- **Ensure that employees responsible for compliance with certain laws can attend training specific to their needs**. Stress the importance of training the trainer. Professional development budgets will always be tight, but this does not mean that the business should ignore this important element.
- **Do not fear external or internal auditors**. Use their audit findings to determine the existing holes in your compliance risk assessment program and then work to plug the holes.
- **Review trends in employee discipline**. What do the trends mean? Is it possible that the trends mean that ineffective policies are in place or that training on those policies is ineffective?
- **Ensure you have a reporting policy (whistleblower policy) in place**. Best practices require an organization to have and publicize a system for reporting noncompliance. A method for anonymous reporting must be included. Make sure that this reporting policy is written so that every employee understands what needs to be reported and to whom.
- **Review your nonretaliation policy**. Does the reporting policy include a prohibition against retaliation for reporting or does your sole standard policy focus only on "no retaliation if involved in a discrimination case"? Make sure it is the former and not just the latter.

Bottom line: Nothing is as effective as getting out of your office and walking around to talk with employees dealing with day-to-day implementation of a policy, procedure, training, etc. These are the employees who know what works and what doesn't. Is the training effective? Are employees consistently disciplined for noncompliance with a policy? Find out the facts from employees who should know the most about the effectiveness of the compliance program in their particular area.