Compliance Risk Assessments - An Introduction
Chapter 6. Step Four: Conducting the Compliance Risk Assessment Survey

Chapter Goals:

- Develop a compliance risk assessment survey that is unique to your business.
- Decide who will conduct the survey.

Remember the cake baking exercise? Well, at this point, you have identified what cake you want to bake (Step 1: Defining Your Compliance Risk Universe) and you have identified what ingredients are going to be part of the batter (Step 2: Determining Likelihood of Occurrence and Step 3: Determining Impact of Occurrence), so, you must be ready to actually bake the cake, right? Sorry—you are close, but are not ready yet to even turn on the oven. In order to develop your risk universe matrix, you need to assess your company's status with each of the laws and regulations in your risk universe. That process will require you to gather information from those most involved in complying with the laws and regulations.

Who Does the Work?

The next decision point you'll need to make—who is going to bake the cake? In other words, who at your business is actually conducting the compliance risk assessment survey? What follows are some action items to consider when thinking about your assessment method and how the method will actually work at your business.

Ideally, your first action will be to head to your in-house legal department or external legal counsel. Before any assessment work begins, you will want to clarify whether your compliance risk assessment needs the protection of attorney-client privilege or attorney-work product. Basically, having such protection may be necessary if the attorneys have reason to worry the business could be facing a criminal investigation or private litigation. The last thing you want is for your assessment of compliance risks to be requested during a government enforcement action or in the discovery phase of a civil lawsuit. Depending on what your assessment uncovers, the report could be used as evidence that your company had prior knowledge of improper conduct. If this is your situation, some careful planning will be needed to preserve the confidentiality of the assessment report. However, those details are beyond the scope of this book.

Let's assume you've been cleared to move forward with the compliance risk assessment. If your business has a one-person compliance office with responsibility for this entire compliance initiative, then it is possible that the assessment format may look different than the assessment format for a larger business that has a structured compliance committee and/or a large compliance department. In either scenario, the assessment will involve gathering information from the organization's compliance partners and compiling it to prepare for creating the compliance universe matrix. Note—compliance partners are individuals who have the most day-to-day knowledge of one or more compliance risks and who are empowered by your organization to take responsibility for ensuring compliance.

For example, a large compliance staff may use a method that would include making personal visits throughout the organization, chatting with the persons who are responsible for implementing certain laws, and then recording the data. This method has pros and cons. It would enable the compliance staff to establish positive long-term relationships with key employees who serve as compliance partners. But this process could be very time-consuming, depending on the number of laws you have identified in your compliance risk universe and the number of employees who serve as compliance partners. Also, this method has the potential for creating response bias. Perhaps the interviewer is a close friend with a particular employee and determines the employee has not created a needed policy nor done the required training nor has any clue about what the law requires for compliance. It is possible that the interviewer might record responses that are not as clear and direct as they should be.

An alternate method involves providing printed surveys to the compliance partners who have the most knowledge about relevant laws and what is being done to ensure the organization is in compliance with them. This method would be less time-intensive for a single compliance officer. But recognize that this method cannot be done without requiring all the compliance partners to receive significant training on use of the survey instrument. Also, this method could be time-consuming if the compliance partners need a lot of nudging to complete the survey.

In conducting a risk assessment survey, concerns about the reliability of the responses are another issue. Will the compliance partners be truthful in their responses or will they be concerned about consequences if they divulge negative information? Those concerns must be dealt with up front in the training. The compliance partners must be told that honesty is important and that there will not be ramifications for negative information such as not having the policy, training, documentation, etc. in place. They need to be told that this is their opportunity to tell the business and upper management what needs to be done and what resources they need in order to accomplish the goal of compliance. The more buy-in you receive from the compliance partners, the more detailed and truthful will be their responses, and the better your compliance initiative will be. Of course, you will have to audit the responses to ensure that the responses correlate with what you know about the business and its processes.

The choice of having one person conduct in-person compliance risk assessment surveys or having each compliance partner complete a printed assessment survey should be based on your organization’s culture and simple logistics of which method will be more effective at your business. Both methods will work; both methods are effective ways to collect the data. And, obviously, there may be other methods for this data collection to occur. Customization for your business cannot be stressed enough.