Compliance Risk Assessments - An Introduction
Chapter 2. A Risk Assessment and Risk Management Primer

Chapter Goals:

- Define risk assessment.
- Define risk management.
- Understand the differences between the two concepts.

Before you begin your risk initiative, let's define some terms. Some people want to use "risk assessment" and "risk management" interchangeably; but they are in fact different. In short, you *assess* your risks so you can more effectively *address* those risks. A risk assessment includes the processes of identifying, analyzing, and evaluating the severity of risks. Performing these steps helps determine the best way to *address* those risks: to monitor, minimize, or mitigate their impact. Assessing and addressing risks together form the foundations of risk management.

To further connect these two terms, it is helpful to understand that risk management comprises a general set of processes that can be used for a variety of purposes. For example, large corporations may have a whole department dedicated to risk management, which might focus on anything from operational to liability to financial risks and more. Alternately, some organizations may only do more highly focused forms of risk management—for health and safety, natural disasters, IT infrastructure, or legal and regulatory compliance, to name a few. At the far end of the continuum is enterprise risk management (ERM), which involves a framework that aims to assess and address all forms of risk.

But, this book is about compliance risk management, which means we want to identify, analyze, and evaluate the risks of an organization being noncompliant with applicable laws and regulations, and we want to use the results to minimize or mitigate the risks. Certainly, this sort of risk management can overlap with and be integrated into other forms of risk management. For instance, if your organization is just beginning to assess and address compliance risks, then integration with an ERM framework might be a long-term goal. But for the most part, we will stay focused on compliance.

Before we can explain how to go about assessing compliance risks, we need to understand the basic premises of risk and understand how an organization's tolerance of risk impacts the process. This base knowledge will help drive the question of what will be the universe of risk to be assessed.

A Primer on Risk

Risk is everywhere. Hiring a CEO without fully vetting his or her background, hackers breaking into your supposedly secure data system, your employees walking out because of perceived non-responsiveness to claims of sexual harassment by your CFO—all of these are examples of challenges and risks that your business might encounter every day. How you deal with any one risk depends on a few factors: the likelihood of the risk occurring, the severity of impact to your organization if the risk occurs, and the level of risk tolerance your organization has for accepting the risk.

There are four basic ways to deal with risk—avoid, mitigate, transfer, and assume.

Avoid risk. Cancel all overseas business trips, never hire anyone without an FBI criminal background check and an interview with the applicant's high school or college yearbook editor, wrap your employees in bubble wrap so they won't be hurt and have a workers' compensation claim, and implement such tight controls on intellectual property rights that no one at your organization could ever argue for rights to anything an employee ever developed. Clearly these methods will work, right? Yes, they will, but if the organization wants to expand its footprint into another country, if you really do want to hire the hotshot marketing manager who 25 years ago may have said a "naughty" word, and if using intellectual property could expand your offerings, well, then risk avoidance doesn't sound like the right approach. Avoidance of risk means exactly that—you totally avoid the risk by not permitting or doing the risky activity.

Mitigate risk. Unlike the avoidance approach, mitigation of risk would require that the owner of the risk (corporation, partnership, etc.) put controls in place so that the potential negative effect of the risky activity is reduced. If you really want to hire the hotshot marketing manager who may have said an inappropriate word years ago, perhaps you can have a conversation with HR, the applicant, and the supervisor to discuss how to get ahead of this story and possibly turn the situation into a positive PR moment. If you want your employees to use intellectual property that your entity developed to expand your product line, you could have the employees sign nondisclosure and noncompete agreements and develop methodologies to monitor their use of this valuable company asset. To mitigate means to reduce the effect of the risk; it does not mean you put your head in the sand or avoid the risk at all costs.

Transfer risk. Transferring the risk is all about figuring out how the business would not be the only one, or the last one, left holding the bag if/when a lawsuit is filed. Perhaps you would consider buying insurance to protect against the risk. Or, if you want to protect against a data security breach, perhaps you can have your third-party provider sign a contract to be the one responsible for notifying the affected individuals of the breach and for paying for any fraud-monitoring services. Decide if you want your employees to purchase the add-on car insurance when renting a vehicle for business travel. Require evidence of sexual molestation insurance when a soccer team uses the flat grassy field located on your company's property.

The bottom line—ensure that other entities surrounding your business have as much, more, or even all the monetary and legal liability if a compliance violation occurs.

Assume the risk. Your business has tried to avoid the risk, mitigate the risk, and transfer the risk. Whatever risk remains from these efforts is what the entity must assume. Your entity is legally responsible for any fine/punishment resulting from a noncompliance issue where the "just say no" edict did not work (avoid the risk); where the risk could not be reduced by policy, practice, or working protocol (mitigate the risk); and where the risk could not be shifted to another entity agreeing to assume it (transfer the risk). Presumably, when your business assumes the noncompliance risk, it is with full knowledge of the risk and its consequences.

Now that you are aware of the types of risk, take a moment to ponder this: Which risk philosophy best represents your organization? Do you prefer to avoid risk at all costs, do you proceed with caution while being aware of risk, do you purchase insurance to protect against the most costly risks, or are you unprepared for risk—which is clearly why you need this compliance risk assessment process implemented quickly? These exemplify different levels of risk tolerance.

Having addressed the basic nature of risk and considered the level of risk tolerance your entity can assume, let's put risk assessment into more context by reviewing some different forms of risk management. To simplify, look at both ends of the continuum: the all-encompassing enterprise risk management and the more highly focused compliance risk management and fraud risk management.