by Amy E. Hutchens, JD, CCEP and M. Shivkumar

Compliance Risk Assessment: Getting It Right

» Assess the risk of organizational misconduct to enable compliance with regulations.
» Scope the risk assessment based on the organization's culture and goals.
» Collaborate with appropriate internal stakeholders for information while identifying risks.
» Align risk assessment to the other components of the compliance program.
» Implement controls based on the risk score and prioritization.

Business operations are becoming increasingly complex, and the economic environment is more uncertain than ever. Due to this, companies need to make risk management a top priority to remain competitive. A key part of this process is managing the risk of civil and criminal law violations.

Regulatory frameworks like the Organization for Economic Co-operation and Development (OECD) guidelines, the United States Federal Sentencing Guidelines, and acquisition regulations make it mandatory for companies to periodically assess the risk of misconduct in their organizations. Failure to comply with these laws and regulations can lead to litigation, fines, loss of reputation, withholding of payment, and cancellation of contracts. Companies are, in turn, striving to effectively control compliance and legal risks with good policies, effective training, aggressive risk monitoring, and frequent auditing. The first step in that direction is to conduct a thorough legal compliance risk assessment.

Why do companies need a risk assessment process?

A legal compliance risk assessment essentially evaluates the risk of violating regulations or laws in the course of normal business operations. It constitutes just one aspect of the enterprise risk management process, but it is critically important for the following reasons.


Hutchens


Shivkumar

To mitigate risks

Periodic assessment of compliance risks helps identify where to apply corporate resources to effectively prevent the highest risks from occurring, or at least mitigate the impact of non-compliance. The enforcement of an effective compliance program can help prevent and reduce the costs of civil litigation and regulatory penalties.

To ensure regulatory compliance

The US Federal Sentencing Guidelines require companies to assess risks periodically, and consider their impact based on factors such as the history of the company and industry specific risk trends. The Federal Acquisition Regulation, which applies to federal contractors, contains similar requirements. These regulations, too, call for periodic assessments of the risk of criminal conduct.

To identify and understand exposure to new risks

New risks may be related to new business operations, a new product or service launch,

or business expansion to a new country with different laws and regulations. Mergers and acquisitions can also introduce new risks by radically affecting the structure of an organization. Changes to regulations and laws or enforcement trends can likewise expose a company to new risks. Compliance risk assessments help capture, quantify, and determine the impact of these risks.

To prevent compliance failures
When a significant compliance failure like a data breach occurs, it usually indicates that the company had underestimated the risk in that particular area, function, or process. Many times incidents can be avoided or controlled if the company assesses the risk accurately and implements appropriate controls.

Risk assessment best practices

As with any other organized corporate effort, a solid risk assessment process requires advance planning and coordination. A well-planned assessment will take into account the necessary expertise, resources, company culture, and the scope and complexity needed to accomplish the goals of the assessment.

Decide on an external or internal assessment
The board of directors is ultimately responsible for ensuring that there is a compliance risk management system in place. First, they need to decide who will carry out the risk assessment. It could either be a senior executive, one of the operational staff or a contractor.

External help is commonly needed when a company is small and is doing a risk assessment for the first time. In larger companies there can be a number of players in the process who sometimes prefer not to clearly see how their risk areas fit into the whole. An external consultant can help introduce a fresh, unbiased, and less complex approach in carrying out periodic risk assessments.

Thus, the first thing management needs to do is to decide whether the company has a capable and experienced staff to carry out an unbiased risk assessment process, or whether an external consultant should be hired to carry out the risk assessment.

Determine the scope of the risk assessment
Organizations vary widely, based on cultures and business goals. Instead of a "one-size-fits-all" approach, the risk assessment process should be customized to fit the culture of the company.

The scope of the risk assessment depends on the size of a company. A small company may face risks in diverse areas and may not have an enterprise risk management plan in place. If this is the case, the company needs to start slowly and simply, by identifying and prioritizing the top risks that require appropriate controls to be put in place.

A larger company may have a more mature risk mitigation strategy and pieces of a risk assessment could possibly already be completed. This can help complete the process in an efficient and effective way.

When defining the scope, it is critical to ensure an open dialogue among management situated across business areas. This will help in properly quantifying risks to clarify and enable implementation of the right kinds of control in the right areas.

Identify stakeholders
Stakeholders are the people who can provide information regarding compliance and legal risks, the probabilities of the risks occurring, and their impact if and when they do occur. For instance, the Legal department can provide information about current litigation facing the company, and any particular areas where the company is likely to face litigation in the future, due to non-compliance with regulations. The Human Resources (HR)

department is subject to a vast array of continually morphing employment and labor laws and regulations. It is the best place to get information on employee misconduct and the types of complaints that employees bring forward most often. Knowing which stakeholders to involve in the process at the right time is vital to an accurate risk picture.

Decide on the degree of formality and complexity

Depending on how it is structured, the risk assessment process can be very informal for smaller organizations or more formal for larger organizations. What really matters is whether a clear risk picture emerges.

The risk assessment process has to maintain a fine balance between simplicity and complexity. It has to be complex and robust enough to obtain all the details needed to assess risk, and yet should not be so complex as to impede the flow of information in a timely manner. Key executives should be able to view and understand the risk picture quickly.

Implement efficient methods to collect information

Any tool that makes the risk assessment process more efficient and effective is your friend. Information about risk profiles can be collected through a variety of tools and methods, including:

- Surveys and questionnaires
- Interviews with the in-house counsel or the company's external law firm
- Litigation charts
- Analyzing hotline and discipline records of incidents, such as HR-related complaints and frauds
- Interpreting employee turnover trends
- Tracking political and economic changes
- Tracking enforcement trends of applicable agencies

Technology can automate the collection of data from multiple sources across the enterprise, and aggregate it in a common database for easy reference and analysis. It can also separate valuable data from "noise," so that stakeholders can leverage the data in an appropriate manner to make the right decisions.

Align the compliance program with the environment

An organization's compliance program will be impacted by a number of internal and external factors and the compliance risk assessment process should be robust enough to align with these changing factors.

Organizations are required to keep track of changes in the external environment, for instance, by closely monitoring enforcement trends and external regulatory activity, and subsequently interpreting regulatory changes appropriately. This aim of this practice is to help organizations preempt non-compliance risks and implement appropriate controls.

The compliance risk assessment process must also tie in closely with other functions and processes. For example, the gaps identified by the auditors in the compliance program may provide inputs to realign controls for effective risk mitigation.

Ensure confidentiality

During the course of risk assessment, it is important to protect data sources while making sure that risks are assessed realistically. Companies need to maintain a fine balance between enabling transparency in compliance while protecting confidentiality. The Legal department may try to withhold information that reflects negatively on the company or subject it to adverse action by regulators or litigants. The legal team may also ask for information to be protected, and may stipulate that only the final risk assessment

should be shared. Therefore, the risk assessment team needs to check beforehand with the Legal department on which documents can be shared.

Analyze the risks

Risk analysis involves analyzing data on company and industry trends, inputs from stakeholders, and the financial and legal impact of non-compliance. In order to get an accurate risk picture, we need to quantify both the probability of a risk and its impact.

Probability can be assessed based on the company history, industry history and enforcement trends. Key executives need to discuss the probability and impact of each risk. These discussions can become an educational tool by documenting and filling in knowledge gaps, especially when executives disagree about the probability or impact of a given risk.

When it comes to impact, the full spectrum needs to be considered in order to effectively quantify it. This includes financial, reputational, and workforce impact, as well as the degree of board or senior level involvement. For example, when Martha Stewart was indicted in insider trading, the share value of her company plummeted, because it was closely aligned to her wholesome image. Had this indiscretion been linked to an entry-level employee, it most likely would not have made the news.

Using software that incorporates techniques like quantitative modeling and risk heat maps can also be invaluable for effective risk analysis.

Prioritize risks

Companies face many risks, but often do not have the time or resources to manage all of them. They need to choose and prioritize the risks that need to be covered by the compliance risk management strategy. When in doubt about quantifying the probability or impact of a risk, it is always safe to assign a higher rating. As the risk picture is completed, it will become clear whether that particular risk is properly ranked or if it seems out of place.

A typical XY graph (figure 1) can be used to rank potential risks and thereby enhance strategic decision-making. Corporate resources should be directed to the risks that have the greatest impact on the organization and the ones that are most likely to occur.

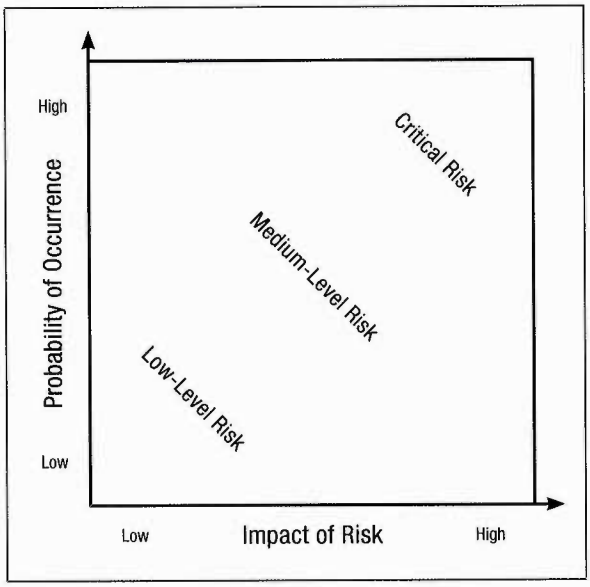

Figure 1: Ranking potential risks

Technology can simplify the complex data obtained from different departments by enabling the creation of a risk impact matrix with multiple levels, rows, and departments. This risk matrix makes it easy to assess risks from a departmental/functional perspective as well as an enterprise perspective. Stakeholders can essentially gain a 360-degree view of the company's risk profile, which can be drilled down to view finer details.

Companies need a scale that fits the size of the company without being too complex. Smaller companies that are doing a risk assessment for the first time can start with a red-yellow-green scale (figure 2 on page 54).

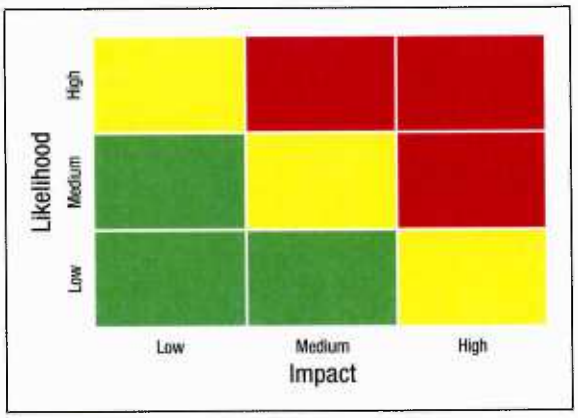

Figure 2: Simple risk profile

Companies that periodically conduct risk assessments, and have a mature process can use a scale with 5 levels (figure 3). With 25 different levels of combinations of risks, the risk model below covers many combinations of the probability and impact of risks.

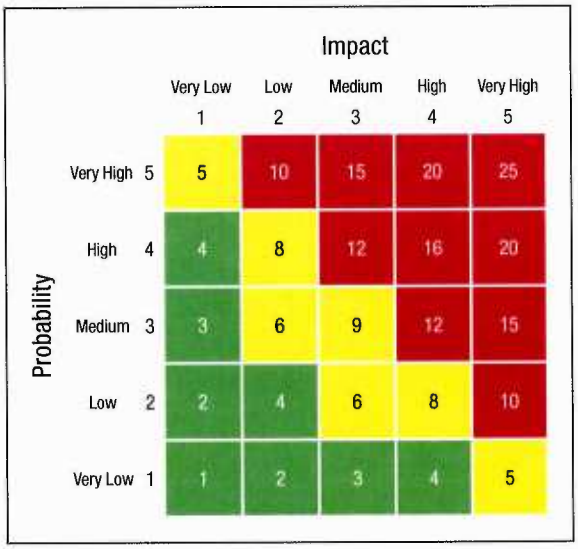

Figure 3: More complex risk profile

Develop a final risk score

When the risk assessment process has been completed, the compliance committee or senior executives need to be informed about the areas that have high risk from a legal perspective, and the resources needed to mitigate these risks. They also need to look at the enterprise risk management process holistically, and see if any of the operational risks, financial risks, or compliance risks have been overlooked.

Based on the final risk score, risks can be prioritized. The entire risk and compliance program can be viewed and comprehended at a single glance by preparing a simple chart with the risks ordered according to their priority down the rows and the measures taken to mitigate the risk across the columns. A large company operating in several locations in different countries can monitor risks at the global level, country level, and business unit level with similar charts.

Mitigation steps

Once companies become aware of risk prone areas, they will take care to put appropriate controls in place, and carry out training programs to mitigate the risks. Risk assessments help identify the best methods to mitigate risk, and from there onwards, metrics can be developed to monitor and audit the effectiveness of control measures.

A proper risk assessment will also pinpoint areas where staff needs more training to comply with regulations. With the aid of technology, companies can develop a standardized and streamlined training program to enhance employee awareness of the requirements of regulations.

Companies can gain an overall risk picture with the right technology that continually pulls in and analyzes data from internal and external sources, and monitors and updates risk data. This overview can help executives develop an appropriate and integrated enterprise risk management program.

Conclusion

Although compliance risk assessment is a very critical component of any organization's risk management strategy, it does not help the organization if it is not used correctly. It must

work in tandem with other components of the compliance program. A collaborative and transparent risk assessment supported by technology can go a long way in helping companies protect themselves against litigation and regulatory penalties. Risk is inherently a part of the future, so assessing risk is a guessing game that needs to be guided. With the right skills and tools, the information gained can help in assessing risk more intelligently, which can be extremely useful in protecting a company as it grows. *

Amy E. Hutchens *(amy.hutchens@wrmi-llc.com) is General Counsel, Vice President Compliance & Ethics Services at Watermark Risk Management International, LLC in Fairfax, VA.* ***M. Shivkumar*** *(shivkumar@metricstream.com) is Product Marketing Manager, GRC Solutions at MetricStream in Palo Alto, CA.*