COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Compliance and Ethics Risk Assessments

By Jose A. Tabuena, MA, JD, CFE, CHC[1]

Background on Risk Assessments and Risk Management

Regularly conducting a comprehensive *risk assessment* is recognized as one of the key "elements" of an effective compliance and ethics program. More broadly, as regulators have emphasized the importance of effective risk management,[2] boards and management teams have increased their focus on the concept of "risk" and have observed a measurable shift on this focus at their organizations.[3] By understanding the nature and the impact of the risks being faced, it is expected that an organization can better design programs and develop controls to mitigate those risks.

Performance of risk assessments falls under the discipline of *risk management*, where enhanced frameworks and techniques have emerged. Risk management comprises the identification, assessment, and prioritization of risks followed by the coordinated and efficient use of resources to monitor, minimize, and otherwise control the probability and/or impact of the risks occurring. Risks arise in many forms and can range from uncertainty in financial markets, operational failures, third party risks, and natural disasters, to legal liabilities and reputational harms, and even missed opportunities (the upside of potential events).

More than ever, there are areas of overlap between risk management and compliance. Risk management has become even more hardwired into more rules and regulations since the beginning of the 2008 financial crisis. Clearly, non-compliance of risk management requirements itself and other applicable regulations are themselves substantial risks requiring the attention of chief risk officers and management. Some companies in the financial services industry have gone so far as to merge the two areas so that their related activities are better coordinated, though many are of the view that the disciplines have quite different skill sets and just need to work more closely together.[4]

As legal, compliance, and ethical risks are a major subset of the overall risk universe faced by an organization, it is worthwhile for the compliance professional to be aware of risk management techniques, particularly those used in your industry sector. Risk management components and the role of risk managers vary by industry, the size and structure of the organization, as well as the risk financing strategies employed. Similar to the field of compliance and ethics, the risk management profession has evolved along functional needs and growing regulatory mandates.[5]

Organizations have increasingly focused on developing effective risk assessment processes. The question has shifted, from whether or not a foundational risk assessment for compliance has been undertaken, to whether that assessment is up-to-date and is addressing the right risks. Benchmarking surveys suggest that organizations conduct regular ethics and compliance risk assessments with most performing them annually either as a stand-alone process, as part of internal audit's risk assessment, or as part of a general enterprise-wide risk assessment.[6] The use of technology and data analytics to identify risk on a closer to real-time basis is emerging.[7]

The Compliance and Ethics Risk Assessment

For the compliance and ethics professional, the risk assessment is the foundation upon which the program is built. At a basic level, an organization cannot design an effective compliance and ethics program without first thoroughly identifying the laws and related standards with which it must comply. Moreover, periodic risk assessments enable the organization to establish priorities that permit the most efficient use of program resources. Benefits of a risk assessment include:

- providing an early warning process for detecting compliance and ethics threats
- allowing companies to correct identified problem areas before they are discovered by regulators, investors, potential acquirers, buyers, the media, or potential plaintiffs
- allowing for prioritizing of compliance and ethical risks with concomitant strengthening of existing controls or the development of new controls for those risks
- enabling a company to revise the ethics and compliance policies, training, auditing, and initiatives that require attention
- improving decision-making by providing managers with critical information on compliance risks and mitigation strategies
- demonstrating to regulators a proactive approach to compliance and thereby meet a due diligence element of an effective compliance and ethics program.

The Role of Risk Assessment in Compliance and Ethics Programs

The Organizational Sentencing Guidelines, when amended in 2004, explicitly included risk assessment within the definition of an effective compliance program.[8] Although commentators believed that the importance of performing a risk assessment was already implicit in the original definition of an effective program, the Advisory Group appointed by the U.S. Sentencing Commission intended to make clear that:

> ... risk assessments need to be made at all stages of the development, testing, and implementation of a compliance program to ensure that compliance efforts are properly focused and effective.[9]

Thus, to obtain the benefit or credit for an effective compliance program (and the reduction in the organization's culpability score) the revised Sentencing Guidelines mandate the performance of periodic risk assessments in order for the program to be considered effective. Specifically, the amended Guidelines provide that:

> The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each (of the components of an effective compliance and ethics program) to reduce the risk of criminal conduct identified through this process.[10]

Additionally the Sentencing Guidelines comment that organizations must:

> Prioritize periodically the elements of the program in order to focus on preventing and detecting the criminal conduct identified in the risk assessment

> process as most likely to occur.[11]

These provisions in the Guidelines provide the foundational perspective for the performance of the risk assessment. It becomes apparent that the risk assessment should precede all other steps in the establishment of the compliance and ethics program in order for program efforts to be properly focused. How would you know what policies, training, auditing, etc. are needed without an assessment of the compliance risks? Further, while a risk assessment is a good starting point, it clearly is not a one-time event and must be conducted regularly in order for the program to adapt to changing business and regulatory conditions. And in order for the program to remain effective, the risk assessment must then be integrated into the organization's overall compliance program and company processes on an ongoing basis.

The Scope of the Compliance and Ethics Risk Assessment

A strict reading of the Sentencing Guidelines would appear to limit the focus of the risk assessment to possible criminal conduct. The commentary to the amended Guidelines states that the organization should identify the *criminal* conduct that might occur considering "the nature of the organization's business."[12] The organization is to further consider the prior history of the organization"[13] and the legal violations highlighted by government regulations.[14]

Although the Guidelines focus on criminal conduct, most organizations take the prudent view that a broader range of compliance and ethics risks must be examined, including those that affect civil liability, regulatory exposure, business ethics or conduct, and the organization's reputation.[15] Essentially, a key step in conducting the risk assessment will be establishing a definition and shared understanding in the organization of what constitutes a "compliance and ethics" risk.

Extending the risk assessment beyond exposure to criminal conduct is essential, as legal mandates can be ambiguous and cumbersome, especially in highly regulated industries. When employees understand how the company's ethical values apply in gray areas, they are more likely to align their behavior in an appropriate manner.

Examining ethical factors and reputational impacts can demonstrate the organization's commitment to ethical business conduct by providing support and guidance when employees are unsure what to do. By emphasizing the commitment to ethics as well as technical compliance, the organization is affirming that *how* business is conducted is just as important as the business itself. Such an approach is further supported by the Sentencing Guidelines' emphasis, when the guidelines were amended in 2004, on the importance of promoting "an organizational culture that encourages ethical conduct and a commitment to compliance with the law."[16]

A compliance and ethics risk assessment should therefore at minimum involve information concerning risks of:

- Criminal misconduct
- Direct legal liability (civil and criminal)
- Ethical and reputational harm

What Is Not a Risk Assessment

It is worth noting what is *not* a risk assessment. A risk assessment is not intended to serve as an audit or investigation, although issues and circumstances that require a deeper examination may be brought to light from

the process. A compliance and ethics risk assessment is not a financial or operational audit, though it can be incorporated with these other processes.

A compliance and ethics risk assessment should also not be confused with a compliance *program assessment* (or program audit), although the objectives and activities of both exercises can overlap:

- An evaluation or audit of the program entails a comprehensive review of the compliance processes and activities to assess the overall impact and effectiveness of the compliance and ethics program. A program evaluation can include a risk assessment, especially if one has not been performed before. Such an instance often involves a baseline effort to identify the range of compliance obligations and ethical risks the organization faces in order to determine if those obligations and risks are being addressed.
- By comparison, a risk assessment more specifically involves the identification and evaluation of compliance and ethics type risks, assessing their significance based on likelihood and consequence, determining the current and desired level of controls, and the acceptable level of risk.

A program assessment necessarily will overlap with a risk assessment because the organization cannot assess risks without understanding how well its compliance and ethics program is mitigating them; and conversely one cannot measure program effectiveness without reference to the identified risks.[17] Clearly a program assessment should include a review of compliance and ethics risk assessments that have been completed as well as the process by which they are performed. And findings from the risk assessment should be evaluated to determine if the results have been used to impact program elements and the overall state of compliance in the organization.

Integration with Enterprise Risk Management (ERM) Initiatives and Other Organizational Risk Assessments?

Risk assessments, when performed from a compliance and ethics perspective, do not delve into the full range of business operational risks that a company experiences. But as noted, risk management has taken on more importance in the corporate environment, spurring more risk assessment type activities across organizations. The compliance and ethics professional should be cognizant of other risk assessment initiatives that may be taking place.

Following focus on Sarbanes-Oxley compliance and internal controls, regular risk assessments, along with the ranking and mapping of results, began taking place with business functions encouraged to evaluate their specific risks and contribute to a comprehensive understanding of the organization's overall risk profile.

Examples of other types of risk assessments taking place include:

- Disclosure controls under Sarbanes-Oxley Sec. 302 to material, non-financial, and financial information required to be disclosed
- Financial risks pursuant to Sarbanes-Oxley Sec. 404 internal controls over financial reporting
- Fraud risks, including those performed as part of the external auditor's duties under Sarbanes-Oxley and Auditing Standard 5 by the Public Company Accounting Oversight Board
- Other functional-specific risk assessments in high-impact areas depending on industry (e.g., cyber-security controls, environmental hazards, etc.)

Because ethics and compliance risks touch so many areas of the enterprise, organizations should consider

integrating when possible the ethics and compliance risk assessment into an existing enterprise risk management process. Studies have suggested that while formal risk assessments have become common, companies initially did not undertake them in an integrated manner, and when they did so, did not address compliance- and ethics-related risks in adequate depth.[18]

One obvious benefit of an integrated approach is consistency and uniformity with respect to terminology, criteria, process, and the risk information that is collected. When risk assessments are conducted separately by different business units, the use of different frameworks can result in the need and cost for reconciling the information collected across the organization. Integration can lead to a better quality of risk-based information upon which strategic and tactical decisions are based.

Integrating the assessment with other business processes can enhance its outcomes and observations, given that ethics and compliance concerns as a practical matter filter into every department and operation. Conducting enterprise-wide compliance and ethics risk assessments in conjunction with financial auditing, manufacturing, marketing, sales, IT, and other functions, ensures that a more complete range of risks is identified and correlated to ethics and compliance concerns.

Other advantages to a holistic risk management and assessment approach include:

- Efficiencies gained as risk issues and operational processes often overlap. More effective mitigation strategies can be developed if process interdependencies are understood.
- An integrated approach can also foster the perception that ethics and compliance is central to all the organization's activities rather than a stand-alone program outside of mainstream organizational concerns as when a siloed compliance assessment is performed (even if a wide range of functions are involved in the compliance and ethics risk assessments).

There are some disadvantages to blending the compliance and ethics risk assessment into a broader enterprise-wide effort:

- Compliance and ethical risks may not be as obvious as operational risks and therefore may receive less attention from the majority of those involved.
- Involvement by the compliance unit in an enterprise assessment will necessarily require more time, participation, and resources from program staff than when driving the assessment from purely a compliance and ethics perspective.

Risk Management Frameworks and Resources

While the U.S. Sentencing Guidelines are clear about the role and significance of risk assessments for an effective compliance and ethics program, the guidance is conspicuously meager on *how* to actually perform one. Generally, the Sentencing Guidelines expect an organization to "scrutinize its operating circumstances, legal surroundings, and industry history to gain a practical understanding of the types of unlawful practices that may arise in future organizational activities.[19] As the commentary to the amended guidelines provides only minimal instruction, it can be valuable to look to other frameworks and standards for ideas on how to go about doing a risk assessment.

Examples of alternative risk management frameworks include:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a comprehensive enterprise risk management framework (ERM) in 2004 for companies to evaluate the broader universe of

business risks.[20] Some commentators find COSO's ERM framework to be confusing and difficult to implement[21] and have turned to other standards.

- AU/NZS 4360, the Australian/New Zealand risk management standard uses a more concise definition of risk than COSO.
- ISO 31000, from the International Organization for Standardization is based on the AS/NZS 4360 risk management standard.
- The GRC Capability Model "Red Book 3.0" by the Open Compliance and Ethics Group (OCEG) seeks to integrate principles of effective governance, risk management, compliance and integrity (GRC) into tangible business practice[22] and provides an ERM approach. OCEG comprises a multi-industry and multidisciplinary coalition of business leaders striving to provide a common framework and language for compliance and ethics professionals.

Each of the above-referenced sources provides a framework with guidance for conducting risk assessments as part of an overall risk management program. Other resources exist from professional associations and industry groups that the compliance and ethics professional should consider when designing a risk assessment approach. The following organizations have useful materials on risk assessments generally, and legal and compliance related risk assessments in particular:

- The Ethics and Compliance Officer Association (http://www.theecoa.org)
- The Society of Corporate Compliance and Ethics (https://www.corporatecompliance.org)
- Compliance and Ethics Leadership Council (https://www.cebglobal.com/public/compliance-ethics/home.html)
- Association of Corporate Counsel (https://www.acc.com)
- Association of Certified Fraud Examiners (https://www.acfe.com)
- Institute of Internal Auditors (https://global.theiia.org/Pages/globaliiaHome.aspx)
- The Conference Board (https://www.conference-board.org)
- National Association of Corporate Directors (https://www.nacdonline.org)
- Open Compliance and Ethics Group (OCEG) (https://www.oceg.org)

Whichever framework or approach that is ultimately adopted, the key is to utilize a systematic approach to the identification, classification, and prioritization of compliance and ethics risks.