COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2021
Dismantling the silos: Integrating risk assessment activities across stakeholders

By Terrence S. Brody and Rachel Woloszynski

Terrence S. Brody (terrence.brody@ankura.com) is Senior Managing Director and **Rachel Woloszynski** (rachel.woloszynski@ankura.com) is Director of Compliance, Investigations, and Oversight for Ankura in New York City.

Strong risk and compliance programs are predicated on effective risk assessment processes that identify, prioritize, and develop actionable strategies to effectively oversee and manage key risk areas. In more mature organizations, various risk assessment activities often are independently undertaken by different stakeholders, including enterprise risk management (ERM), compliance and ethics, and internal audit. While each of these stakeholders may have slightly different objectives, oftentimes, the methodologies and goals substantially overlap.

This writing explores the risk assessment processes of various corporate stakeholders and advocates for their integration where feasible in order to:

- Minimize disruption to business operations;
- Create process efficiencies;
- Leverage diverse perspectives of leadership, management, and subject matter experts; and
- Realize a more holistic view of risk across the organization.

Defining risk assessment typologies

Today, corporate entities regularly conduct risk assessments covering a range of key areas, including legal and regulatory compliance, ERM, internal audit, anti-bribery and anti-corruption, and anti-money laundering, to name a few. The goals and methodologies of three frequently conducted risk assessment exercises are defined below.

Legal and regulatory compliance risk assessment

In addressing the components of an effective compliance and ethics program, Chapter 8 of the United States Sentencing Commission's *Guidelines Manual*[1] provides that corporate entities "shall periodically assess the risk of criminal conduct" and incorporate findings from the assessment into the design of the compliance and ethics program. Chapter 8 was drafted in response to Section 805(a)(5) of the Sarbanes–Oxley Act of 2002 (SOX Act),[2] which directed the commission to review the guidelines to ensure they sufficiently "deter and punish organizational criminal misconduct." The U.S. Department of Justice Criminal Division's *Evaluation of Corporate Compliance Programs*[3] further instructs that the risk assessment should be tailored to the organization's unique risk profile, considering factors that include the jurisdictions in which business is conducted, the industry sector, and the regulatory landscape, among others. The organization must then tailor its compliance program to

address the most prominent risks identified in the assessment.

In conducting a legal and regulatory compliance risk assessment, best practices provide that for each risk area, the organization should evaluate the likelihood of a violation and the degree of potential impact. Additionally, it is important to assess the controls in place to determine the residual risk rating and rank the risks to prioritize mitigation action planning. Notably, unlike an ERM risk assessment (discussed below), it is not appropriate to apply a risk appetite to legal and regulatory risks, as no organization should tolerate criminal violations.

Enterprise risk management risk assessment

ERM derives from the SOX Act's internal control framework requirement that mandates a regular enterprise risk assessment. The goal of ERM is to align risk management with the organization's strategic planning activities and operational performance. To accomplish this, ERM holistically assesses risk across a broad range of categories (e.g., operational, financial, strategic, operational, technology, legal) to identify and plan for risks that may affect the organization's ability to achieve its strategic goals. The scope of the ERM risk assessment, therefore, is far broader than the legal and regulatory compliance risk assessment.

As part of the ERM process, organizations define a risk appetite and risk tolerance to set boundaries of how much risk the entity is prepared to accept. Like the legal and regulatory risk assessment, the ERM risk assessment typically evaluates the likelihood of the risk occurring and the degree of impact. Those metrics will then be compared to the established risk tolerance to ensure the organization is sufficiently controlling risk within the bounds of the defined risk appetite.

Internal audit risk assessment

In developing a risk-based audit plan, the chief audit executive of an organization should undertake a documented risk assessment process, which incorporates feedback from senior management and the governing board. The process should be designed to assess the organization's strategies and objectives, associated risks, and risk management practices. As with the other risk assessments discussed above, the internal audit risk assessment should analyze the risks inherent to the nature of the business and its operations, the mitigating controls in place, and the resulting residual risk. An audit plan is then designed to address priority risks.

Integrating these assessments and their stakeholders

While there is substantial overlap in the objectives and methodologies of each of these risk assessment types, many organizations undertake these initiatives in a disconnected, siloed manner. There are, however, compelling reasons why these efforts should be integrated to the extent possible. Among other benefits, a unified approach minimizes disruption to the business, lends broader subject matter expertise and a more diverse perspective, yields a more holistic view of risk, and engenders broader stakeholder support.

Higher efficiency

For each of the risk assessment typologies referenced above, best practices provide that the assessment should leverage qualitative and quantitative methodologies. On the qualitative side, risk assessments typically incorporate compliance artifacts and records reviews, leadership and management interviews, and employee focus groups. Quantitative data often is generated from employee risk rating surveys. Each time a risk assessment is conducted, many of the same stakeholders will be engaged to solicit input, including responding to document requests, participating in interviews, or completing surveys. This amplifies disruption to the business, often generates frustration by employees who perceive the processes to be redundant, and leads to duplicative efforts. An integrated process can alleviate many of these inefficiencies.

Additionally, across the risk assessment typologies described above, there is significant overlap in terms of the types of risks that should be assessed. For example, compliance, ERM, and internal audit all typically assess third-party risk management. Having all three business functions review that risk in isolation is inefficient and can likely generate different or even contradictory findings.

Increasingly, compliance and ERM report up to a chief risk officer. This is a logical reporting structure, as both functions make up the second layer of defense, and further militates in favor of an integrated risk assessment process.

Finally, an integrated process enables risk and compliance professionals to collectively leverage data. Increasingly, regulators have emphasized the importance of data analytics in risk and compliance. Employing advanced data analytics enables an organization to effectively monitor and evaluate key risk indicators, perform continuous monitoring and continuous risk assessment, and allow for a dynamic audit planning process. Having collaborative stakeholders in the risk assessment process allows for the pooling of resources to invest in data analytics and business intelligence tools that provide real-time intelligence on a wide variety of risk and compliance topics.

A more holistic view of the risk landscape

Compliance, ERM, and internal audit all have unique subject matter expertise and perspectives. For example, internal audit regularly interacts with the business and often has the greatest insights into how the business operates, which is a critical perspective. Compliance generally has stronger expertise on applicable regulatory standards. And ERM likely will have the broadest visibility across the risk landscape. When properly harnessed and integrated, together, they provide a much more holistic view of risk for the organization.

Stronger stakeholder support

A collaborative approach to the risk assessment will provide employees with unified objectives and a clear road map for addressing risks across the organization. Having stakeholders who truly embrace the process is key to a successful assessment and to the effective implementation of compliance enhancements and risk mitigation action plans following the assessment.

Integration requires coordination and project management

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." - Sun Tzu

While the advantages of integrating the various risk assessment processes are many, in practice, they can be very difficult to achieve successfully. Strong governance, advanced strategy-setting, and effective project management are critical to a successful integration.

Governance and strategy considerations

The integrated assessment team must clearly define scopes of responsibility, decision-making processes, and reporting chains. Ideally, the principal heads of compliance, ERM, and internal audit should form a steering committee to guide the strategic direction of the risk assessment process and oversee tactical implementation. The steering committee should ensure that workstreams are well defined and led by experienced professionals, and also regularly meet with workstream owners to track progress and address issues as they arise. The steering committee should also report on the methodology, findings, and enhancement plans to executive leadership and the board.

In the absence of a strong governance foundation, integrated approaches to risk assessments often get derailed. Without committed leadership and a defined strategy, project teams tend to be disjointed and undisciplined, which often results in delayed project timelines, lost stakeholder engagement, and less impactful work product.

Project management is critical

Once the steering committee establishes a clear vision and strategy for the project, a strong project manager (or project management team) should be assigned to assist with the day-to-day administration of the project. The project manager is responsible for translating the steering committee's strategy into a tactical work plan, which defines workstreams, tasks, owners, and timelines.

The project manager should regularly meet with the workstream owners to drive progress, ensure accountability, and keep the project on schedule. Doing so affords the project manager a holistic view of the project and enables executive-level briefing to the steering committee. The project manager also may facilitate the production of records and assist with the scheduling of interviews.

The clear advantage

An integrated risk assessment process offers many benefits to business organizations, including increased efficiencies and diversity of perspective. Most importantly, it provides a comprehensive understanding of the risk landscape and often yields more informed tactics to manage priority risks. While the advantages are clear, executing multiple risk assessment types in a collaborative manner can be challenging. To overcome these challenges, leadership should establish a strong governance framework supported by effective project management capabilities to ensure that the strategic goals of the risk assessment initiatives are timely and properly executed.

Takeaways

- Many organizations undertake related risk assessment initiatives in a disconnected and siloed manner.
- An integrated risk assessment process enhances efficiency and minimizes business interruption.
- An integrated approach produces a more holistic and comprehensive understanding of the risk landscape.
- Collaboration in the risk assessment process provides employees with unified objectives and a clear road map for addressing risks across the organization.
- Strong governance, advanced strategy-setting, and effective project management are critical to coordinating an integrated risk assessment process.

1 USSG § 8 (U.S. Sentencing Comm'n 2018), http://bit.ly/38BgFRS.
2 Sarbanes–Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (July 30, 2002).
3 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.