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.