Risk Insights

Managing Uncertainty

The audit committee's role in enterprise risk management

UNCERTAINTY IS INEVITABLE, but effective enterprise risk management recognizes and acknowledges the threats associated with that uncertainty. The audit committee plays a crucial role in assessing and managing enterprise-wide risk of an organization by overseeing management's focus on identifying, evaluating and responding to risks that face the entity. It requires the recognition of ever-changing uncertainty and the importance of deploying programs and tools to assess the risk and opportunities that such uncertainty creates. Completion of an enterprise risk assessment enables management to determine whether or not the entity's risk appetite and strategic objectives are aligned. More impactful are the monitoring activities, controls and indicators to mitigate and monitor unfavorable risks that management implements. The overall process begins with an effective enterprise-wide risk assessment.

The enterprise risk assessment should encompass external and internal risks, and each identified risk should be evaluated both on the likelihood of it occurring and the potential impact to the entity. Cybersecurity, rising labor costs, political instability in overseas markets and major difficulties facing large customers present external risks, as do more stringent regulatory requirements. Fraud or unethical behavior, management succession, underperformance by various business units and ineffective financial reporting controls are examples of internal entity risks.

Each organization is unique in the risks it faces and the way broad risks affect the entity. While changes in economic conditions affect thousands of companies across a broad range of industries, the impact of such risks varies from company to company.

Even for businesses operating within the same industry, the effect of a particular risk will vary. All transportation companies face risk from rising fuel costs. The individual companies differ, however, in the markets they serve, their business models and internal costs, and the other risks they face. Such factors influence how crucial that risk is to each entity and the steps required for managing that risk.

Frameworks Provide a Means for Assessing Enterprise Risk

WITH THAT UNDERSTANDING of enterprise risk assessment, management can deploy a variety of tactics or models for identifying and evaluating entity risks. Following an enterprise risk management framework, such as the *Enterprise Risk Management – Integrated Framework* developed by the Committee of Sponsoring Organizations (COSO), provides proven guidance for developing a culture that is aware of risk, establishing strategic

goals and objectives, identifying events (both internal and external) that pose risk or provide opportunities to the achievement of strategic goals, assessing the significance of identified risk events, and developing risk response, mitigation and monitoring activities.

The International Standards Organization has also issued a framework for managing enterprise risk, *International Standard 31000 – Risk Management Principles and Guidelines*. This framework provides high-level objectives for the performance of an enterprise risk assessment including risk identification, analysis, evaluation and treatment. The ISO standard suggests that risk management is a process within and across the organization to identify, understand, and manage uncertainty and risk.

Both frameworks are based upon a thorough and robust risk identification process. An enterprise risk assessment includes and begins with risk event identification and brainstorming. Starting with external and internal risk categories, an organization should brainstorm the potential events that pose risks and opportunities and could impact the achievement of strategic objectives. Identified risk events should consider current and emerging actions and vary in probability of occurrence and magnitude of impact. Ask the question, "What could occur and influence the organizations plans, processes, opportunities, requirements and ultimately, success?"

The risk assessment process will allow management of the entity to collectively determine how probable and impactful individual identified risk events may be to the achievement of the entity's strategic goals, both in the short-term and for the long-term growth.

For example, a company that derives most of its earnings from manufacturing outdoor recreational products for younger adults would view a steady rise in the average age of the nation's adult population as a sign that its market for those products is shrinking. Aging population constitutes an external, demographic risk event. Though it may take years for the entity to feel the full impact of this risk, the likelihood that it will occur seems quite evident. Since the company has a recognized dependence on younger adults for most of its earnings, that long-term impact may be substantial. The company faces a crucial entity risk, a risk it cannot accept.

In response, the company might invest in researching and developing new products that would appeal to older individuals, it may look toward expanding into international markets that present more favorable demographic trends, or it might take other steps to mitigate that risk.

Once risks are identified and linked to the company's strategic objectives, management evaluates and determines whether or not they align with the company's mission, vision and risk appetite. The COSO framework classifies entity objectives as: strategic, operations, reporting and compliance.

Strategic objectives relate to high-level goals that align with and support the company's mission and vision. Operational effectiveness and efficiency factors, including performance and profitability goals, comprise operations objectives. Those objectives vary, depending upon management decisions regarding structure and performance. Reporting objectives relate to the entity's reporting effectiveness and consist of internal and external reporting practices, including financial and non-financial information. All companies must meet various laws and regulations, and compliance objectives relate to the entity's performance in meeting those mandates.

The four categories of objectives provide a basis for management to categorize risks and recognize their relationship to the entity. Examples:

- Management may decide that a celebrity spokesperson's legal troubles detract from the company's image and brand equity. Therefore, keeping that celebrity as a spokesperson presents a **strategic objective risk.**
- Inability to process and ship customer orders in a timely manner during peak demand periods threatens quarterly earnings goals, representing an **operational objective risk.**
- Delays in consolidating financial reporting data for period-closing threaten an entity's ability to present timely financial results and create a **reporting objective risk.**
- Difficulties meeting the regulatory requirements associated with disposing of hazardous material poses a **compliance objective risk.**

Once such risks are identified and linked to entity objectives, management evaluates and determines whether or not those risks align with the organization's risk appetite. Upon completion of the enterprise risk assessment, the entity should have a documented risk profile that indicates what risk events are relevant for the entity, the significance of those risks, the nature of those risks (current or emerging), and the linkage of identified risk events to the entity's goals and objectives. Once documented, the risk profile provides a basis for prioritizing risk management activities and making informed, risk-based decisions.

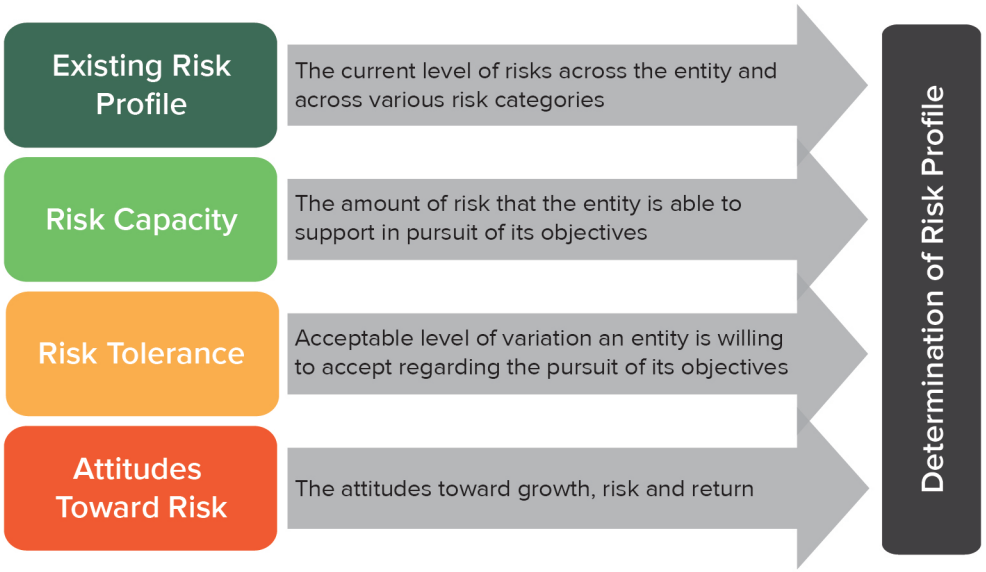
A risk profile depicts the sum of risk awareness and tolerance. Risk awareness is the general level of overall risk consciousness within the organization. It is usually described at a high level and includes consideration of the entity's overall cultural capacity and attitude to accept risk. Typically, the risk appetite is written in attributes or phrases that link directly to strategic goals and clarify what the entity is "willing to do" and "not willing to do" in the pursuit of strategic objectives. It is necessary to consider the people, technology and capital resources available as risk capacity to appropriately align the risk profile with operations.

Risk tolerance is defined as the acceptable variation relative to the achievement of a specific objective and is often measured in the same units as those used to measure the related objective. In setting tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Each component of a complete risk profile should be considered thoroughly with an appropriate alignment of resources to effectively establish the foundation for enterprise risk management.

Completing the enterprise risk assessment, developing the risk profile, developing risk response and mitigation activities, and updating the risk assessment over time are management functions. The board, and specifically the audit committee, should oversee the process and ask questions regarding the assessment and monitoring of risk to understand and challenge management on risk management activities.

At the completion of the enterprise risk assessment, management should have the information and tools to develop a risk response plan which documents the existing and planned risk management activities that are expected to reduce the residual risk to an acceptable level. The audit committee should require periodic updates from management on the effectiveness of risk mitigation activities to ensure that residual risk assumptions are reasonable and being actively monitored.

Overview of Considerations Affecting Risk Profile



The Audit Committee's Oversight Role in Risk Assessment

WHILE MANAGEMENT IS RESPONSIBLE for continually assessing risk, the audit committee has responsibility for oversight. That responsibility, as it relates to risk assessment, should be defined in the audit committee charter. It also needs to be reflected in the way audit committees are responsible for and evaluate risk assessment efforts. Describing the duties, focus and parameters for evaluating risk assessment efforts in the audit committee charter clarifies duties and responsibilities for audit committee members.

The audit committee should incorporate risk management oversight into its meeting calendar throughout the year and question the CEO, CFO, COO, enterprise risk manager, controller, internal audit director, general counsel, director of financial reporting, IT director and any other key management team members.

The audit committee should plan appropriate risk-related discussions based on the organization's culture and consistent with board member interactions. They should be prepared and have certain identical questions ready to pose to each individual. They should all be asked what they view as the greatest risks facing the entity and whether they feel comfortable raising issues without fear of retribution. Other questions should address issues specific to an individual's responsibilities and areas of expertise. The internal audit director, for example, should be asked whether the company's financial reporting controls mitigate identified risks. The general counsel should be asked if the entity faces any risks in meeting newly-enacted laws and regulations. Questions regarding which business lines had the greatest positive and negative impact on company earnings would be directed to the COO, while the CFO may be queried on the most difficult challenges facing the finance department.

Information obtained through these risk-related discussions should be compared to the risk profile provided by management, to ensure it is being maintained and that risk management activities and resources are being deployed in an appropriate manner.

The American Institute of CPAs (AICPA) offers an audit committee tool kit that includes questionnaires with sample questions. Additionally, the National Association of Corporate Directors (NACD) provides resources that assist member directors in enhancing their understanding and overseeing of the risk management activities of their respective organizations, while maintaining an adequate separation from the execution of the risk management function.

The audit committee should oversee the risk management process and results, and their involvement should be structured so that they can participate in risk identification activities and ensure the risk profile is relevant and valid to support the entity's mission and strategic objectives, without actually executing risk management activities.

Enterprise Risk Assessment is an Ongoing Process

RISK IS INEVITABLE, and events that unfold throughout the year require management's attention. Management and the audit committee need to communicate regularly to determine that such risks are identified and evaluated and that controls or activities are in place to mitigate those risks.

By assessing entity risk, management is less likely to encounter significant unreported risks. It becomes more responsive to changes and events and mitigates risks that do not align with the entity's risk appetite strategy and strategic objectives. That enhanced responsiveness also reveals opportunities that would have otherwise gone unnoticed. Overall, an enterprise risk assessment provides a foundation for strong enterprise risk management decisions that can improve the company's performance and build value for all stakeholders. Oversight by the audit committee is a key element of that process.

CONTACT US

Alyssa G. Martin, CPA, MBA
Partner-in-Charge
Risk Advisory Services
alyssa.martin@weaver.com

Weaver's risk advisory services are strategic, executable and measurable–and our nimble process is designed to help companies remain optimally functional as they identify and manage risk. We work closely with our clients to customize services that fit their existing staff structure and operations. Integral to this sensitive work, we believe our communication skills are as valuable as our technical knowledge and professional insight. You will experience thoughtful, purposeful communication throughout the process. Specific services we provide include:

- Business continuity planning
- Business process improvement
- Contract monitoring and compliance
- Enterprise risk management
- Internal audit
- Internal control evaluation
- Integrated financial and IT audit
- Performance audit and measurement
- Regulatory compliance
- Risk assessment
- Sarbanes-Oxley compliance

weaver
Assurance • Tax • Advisory