



AUDIT COMMITTEE INSTITUTE

Oversight of Risk Management: What is the Audit Committee's Role?

KPMG IN CANADA

Reprinted from *Canadian Audit Committee Update*, Fall 2006

As many audit committees are discovering, oversight of risk management is no simple matter

The essential issue

In their efforts to strengthen the integrity of the financial reporting process, leading audit committees today are recognizing the important—if not imperative—link between effective oversight of financial reporting risk and effective oversight of risk management. A robust risk management process—for systematically identifying and analyzing, avoiding, transferring, mitigating or accepting the spectrum of risks facing a company—can help the audit committee more effectively oversee the management and reporting of significant risks. As many audit committees are discovering, however, oversight of risk management is no simple matter.

Most audit committees are comfortable in their oversight of traditional financial reporting and related compliance risks, however, oversight of other risks that could become financial reporting risks is a different challenge. Frequently it is not clear whether the board, the audit committee, or another board committee is responsible for overseeing such risks.

Inadequate reporting of risk information can hamper oversight efforts, internal and external audit plans that do not clearly focus on key areas of risk can make oversight more difficult, and lack of a common “risk” vocabulary complicates matters.

These challenges notwithstanding, audit committees have a central role to play in the oversight of risk management.

To help audit committee members and directors gain a better understanding of risk and the role of the audit committee in the oversight of the risk management process, KPMG's Audit Committee Institute facilitated interactive roundtable discussions in Montreal, Toronto, Calgary and Vancouver in the Spring of 2006 (“Spring 2006 Roundtables”). These discussions generated insights into key concerns, perspectives, and emerging practices driving the oversight of risk management today. During the roundtables there were questions concerning the oversight of risk management. This article reports some of those results.

Often it is not clear who is responsible for overseeing non-financial risks.

Considering risk

Risk—broadly defined as anything that could preclude a company from achieving its objectives—is inherent in doing business. An organization’s critical risks can be wide-ranging including, for example, risks affecting reputation, ethics, technology, health, safety and the environment, not just financial or insurable hazards.

From the audit committee’s perspective, risk falls into two general categories: financial reporting risks, such as critical accounting judgments and estimates, and non-financial reporting risks with possible financial reporting implications, such as a supply chain problem, product recall, or a marketing practice affecting revenue recognition.

Risk management involves identifying risks that may prevent an organization from achieving its objectives, analyzing those risks, avoiding certain risks, and transferring, mitigating or accepting the risks that remain.

The role of management is to implement business strategies—and manage their associated risks—based on the amount of risk the company deems acceptable and the return it aims to achieve.

The role of the board, audit committee, and other board committees—as guardians of shareholder interests—is to provide risk oversight: to help ensure the company’s process for risk management is effective and in line with the company’s strategies and the expectations of shareholders and regulators.

The management and the oversight of risk are made more difficult in the absence of a formal risk management process. Heavily regulated industries, such as financial services, utilities, and health care, tend to have more mature risk management processes in place for certain categories of risk. Generally, however, risk management in most other industries is still an emerging practice, often lacking a common vocabulary, consistent context, and formal framework.

In polling at the Spring 2006 Roundtables, on average only one in four respondents indicated they thought the board, including the audit committee, was very effective in overseeing the potentially significant business risks—both financial and non-financial—facing the company, and another quarter of the respondents felt that there was a need for improvement. The balance were somewhere in between.

Risk management involves identifying, analyzing and managing risks.

Respondents were slightly more negative about the process that management uses to identify and prioritize the potentially significant business risks.

Unlike the New York Stock Exchange, Canadian regulators do not specifically require audit committees to be responsible for discussing guidelines or policies to govern the process for risk assessment or risk management. Notwithstanding this fact, oversight of risk management is an area of significant concern and is gaining attention.

Risk management: why it matters to the audit committee

In Canada, primary oversight responsibility for the company's financial reporting and disclosure process rests with the audit committee.

A company's risk management efforts are critical to the audit committee's oversight of the financial reporting process in several respects: A robust risk management process can be invaluable to the audit committee by identifying and prioritizing the company's significant financial reporting risks and non-financial risks that may have financial reporting implications. It also can help the audit committee ensure that, for each significant risk:

- the company has appropriate internal controls
- management makes appropriate disclosures, e.g., the presentation of critical accounting judgments and estimates in MD&A
- the financial statement impact of the risk is properly recorded
- CEO and CFO certifications are appropriate, especially with respect to disclosure controls and procedures, and internal control over financial reporting
- internal and external audit plans appropriately address the risk

Given the breadth, complexity, and dynamic nature of risk, the alignment and allocation of oversight responsibilities is vital to ensure that risks and their financial reporting implications are identified, assessed, and managed effectively.

A robust risk management process identifies and prioritizes significant non-financial risks that may have financial reporting implications.

Ultimate responsibility for risk management rests with the board.

Ownership of risk oversight

The board is ultimately responsible for assessing the principal risks, approving risk tolerance levels and overseeing risk management. The entire board should participate in this process on a company-wide basis. However, because some risks are highly technical or complex, the detailed work of overseeing certain risks is often delegated to specific board committees.

While most audit committees may be comfortable in their oversight of traditional financial reporting and related compliance risks, the oversight of non-traditional risks—such as operational, strategic, regulatory, cultural, and others that could become financial reporting risks—present formidable challenges. Often it is unclear whether the board, audit committee, or another board committee is responsible for overseeing these risks.

Audit Committee versus Board (Committee): Who oversees what risks?

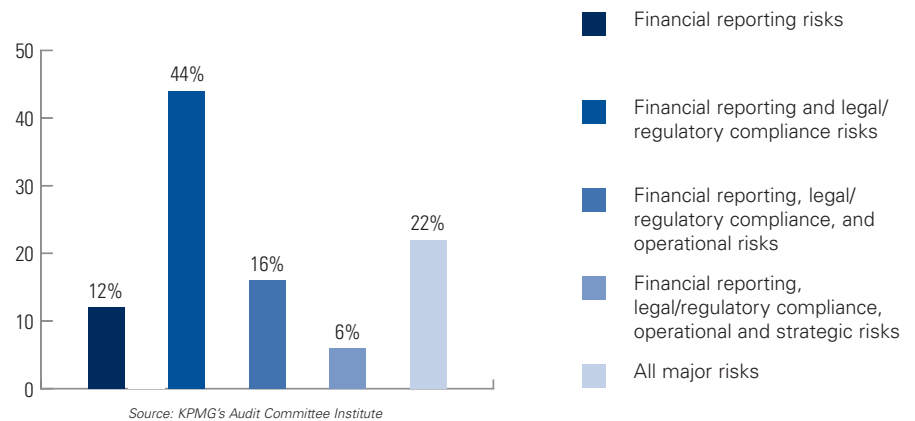


The audit committee should be informed of non-financial risks that may have financial reporting implications.

This figure illustrates, from a governance perspective, who is responsible for overseeing which risks. The audit committee’s responsibility for overseeing financial reporting risks is represented in the top left triangle. The board must clarify the responsibilities for non-financial risk, represented in the lighter blue, deciding who will oversee these risks. As depicted by the black boxes, boards must have a process by which the audit committee is informed of non-financial reporting risks that may have financial reporting implications. The audit committee requires notice as early as possible, and certainly long before a crisis occurs, when conditions can change quickly.

At the Spring 2006 Roundtables, participants were asked for what categories of risk should the audit committee have primary oversight responsibility. There was a diversity of opinions as can be seen in the following chart.

For what categories of risk should your audit committee have primary oversight responsibility?



This broad range of views points to the need for audit committees to review their charters to ensure they understand the scope of their risk oversight responsibilities—and that their oversight activities correspond to those responsibilities.

The charter should clearly define the scope of the audit committee's risk oversight responsibilities.

Over time, the diversity of opinion about the audit committee's role in risk oversight may narrow with the evolution of oversight practices, regulatory guidance, and perhaps court decisions on the matter.

Absent a "bright line" that delineates such responsibilities, leading audit committees are taking a common sense—and prudent—approach to determining which risks are (or should be) within the committee's purview, and for those that are not, where the oversight responsibility lies and the process by which the audit committee stays informed of potential financial reporting risks that are "owned" by other committees.

Coordination of risk oversight

Information flow between the audit committee, the full board, and other board committees is increasingly seen as vital to ensuring that risk oversight responsibilities are appropriately assigned and coordinated, and that key risks don't fall through the cracks. While the committee structure can improve efficiency and provide specialized oversight through delegation of responsibilities, it also poses the potential for "balkanization" of risk oversight activities—and possible gaps in oversight. Recent scrutiny of stock option backdating, executive incentive compensation, and pension

Oversight activities need careful coordination where there are multiple board committees.

Possess a clear understanding of the company's process for identifying, managing, and reporting risk.

accounting demonstrates the importance of coordinating the oversight activities of multiple board committees—such as the compensation, finance, technology, governance, and risk committees—with the audit committee on issues that have financial reporting implications.

There should be a clear understanding of what information the audit committee needs from other committees as well as what information other committees need from the audit committee to ensure effective coordination and communication regarding significant risks.

Boards approach risk management in a variety of ways. The board may assume that responsibility itself or it may assign selected oversight responsibilities to other board committees. Nonetheless, the board retains overall responsibility for risk management. As such, risk management should always be on the board agenda, demonstrating the board's clear ownership of risk management oversight.

As risk underlies nearly all business activities, the responsibility for managing and reporting on various risks may reside with different members of management, the CEO, the CFO, internal audit, line managers, and others.

In its oversight role, the audit committee should have a good understanding of, and level of comfort with, the company's process for identifying, managing, and reporting risk.

To help the audit committee obtain a clear picture of the company's risks and its risk management approach, the information generated by this process should include:

- identifying and prioritizing significant risks
- quantifying the financial implications of each risk
- determining who has primary responsibility for management of specific risks
- evaluating the status of management's risk mitigation efforts

Certain risks that are more "qualitative" in nature—for example, management inexperience or misalignment of employee incentives and strategy—can be difficult to quantify or translate into financial terms. Nevertheless, management should have a method for reporting these types of risks to the audit committee.

In polling at the Spring 2006 Roundtables, about 58 percent of directors and audit committee members indicated they were either very or somewhat satisfied with the reports that management provides regarding the potentially significant risks facing the company. However, 42 percent felt that such reports needed improvement. This is not surprising due to a lack of a common and consistent understanding of what is risk.

Periodically assess the adequacy of risk management information, both financial and non-financial.

The board or the audit committee must demand relevant, timely and accurate information from senior management, the internal auditor, and the external auditor, to ensure it is meeting its oversight responsibilities. In addition, the board or the audit committee needs to assess periodically whether they are receiving appropriate risk management information, regularly enough, and in a format that meets their needs. They need to evaluate, at least annually, the adequacy and timeliness of management reporting to the board or the committee on financial, non-financial, current and emerging risk trends. By asking probing questions about risk management, the board and its committees can help bring clarity to the processes for managing risk.

Risk and the audit process

Review internal and external audit plans dealing with significant business risks.

An important role for the audit committee is to help ensure that the internal and external audit plans properly focus on internal controls associated with potentially significant business risks—both financial reporting risks and non-financial reporting risks that may have financial reporting implications—facing the company.

In its review of internal and external audit plans, the audit committee should consider whether the internal and external auditors have:

- communicated their process for identifying and ranking the financial and non-financial reporting risks they believe may have financial reporting implications
- focused their audits on key areas of risk and that audit procedures are appropriate given the potential impact and potential occurrence of significant risks
- identified the same risks that management identified
- explained variations from management’s identified risks or risk rankings
- communicated the design and performance of planned audit procedures (including their nature, timing, and extent) and demonstrated that the procedures are responsive to the identified risks
- communicated the potential “consequences” if a control is found to be ineffective, including any additional audit procedures required to be performed

Putting it all together

In *Risk—From the CEO and Board Perspective*¹, risk management professional James Lam observes that “the only alternative to risk management is crisis management.” Similarly, from an audit committee perspective, the likely alternative to oversight of risk management is oversight of financial reporting crisis.

As the potential financial reporting implications of non-financial reporting risks become more widely appreciated and better understood, leading audit committees—working with their boards—are devoting more time and resources to ensuring that:

- management has a process in place to identify, evaluate, and mitigate significant risks that may have financial reporting implications
- management’s process for reporting risk information and the status of risk management efforts to the audit committee is robust
- responsibility for oversight of specific risks is clearly allocated among the audit committee, board, and other committees, and that the audit committee understands—and is carrying out—its risk oversight responsibilities as articulated in its charter
- risk oversight activities are coordinated and communicated among the various board committees that have ownership of the oversight of risks
- management and auditors understand the audit committee’s expectations of them in conjunction with the audit committee’s role of overseeing risk management objectives and processes, including risk reporting and tone from the top
- internal and external audit plans and activities complement and support the audit committee’s consideration of the company’s risks, including risk prioritization and allocation of audit resources to address those risks
- the audit committee’s oversight activities are appropriately documented (in consultation with counsel) in its meeting minutes

By focusing on these oversight activities and practices—within the context of the company’s own needs and objectives—audit committees should be well positioned to answer the question underlying their role in the oversight of risk management: Are the audit committee’s oversight processes, including the risk reports provided by management, sufficient to demonstrate that the committee is fulfilling its fiduciary duties of care and good faith?

Management and the auditors must understand the audit committee’s risk expectations.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.
© 2006 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. 3563