

## Enterprise Risk Management and the audit committee

### About this document

The Audit Committee Leadership Network is a select group of audit committee chairs from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit environment.

*ViewPoints* is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *ViewPoints* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *ViewPoints* may share it with those in their own network. The more board directors, management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

The Audit Committee Leadership Network held its third meeting on December 12, 2003. The discussion focused on the role of the audit committee in managing enterprise-wide risk:

- **Identifying risk:** How does the audit committee get a comprehensive view of risk?
- **Prioritizing risk:** How are risks classified and put before the audit committee?
- **Managing risk:** How to coordinate across silos, and who in the corporation “owns” risk?

The members of the network present at the meeting, representing in all more than 25 large and small public company boards, were:

- Mr. Jim Adams, Audit Committee Chair, Texas Instruments
- Mr. Dan Akerson, Audit Committee Chair, American Express
- Mr. Bob Burt, Audit Committee Chair, Pfizer
- Mr. John Clendenin, Audit Committee Chair, The Home Depot
- Mr. John Ferraro, Vice Chairman, Ernst & Young
- Mr. Gene Fife, Audit Committee Chair, Caterpillar
- Mr. Tom Flannery, Americas Director, Quality, Ernst & Young
- Mr. Tom Kierans, Audit Committee Chair, Manulife Financial

*ViewPoints* reflects the network’s use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments made during the meetings are not attributed to individuals or corporations.

## Executive Summary

The discussion at the third meeting of the Audit Committee Leadership Network on December 12, 2003, focused on enterprise risk management. The issues found to be most important to members are highlighted below, with more detailed discussion on the following pages. We hope these viewpoints will spark further discussions of value to audit committees, their auditors and, ultimately, to investors.

- **Overview: Enterprise risk management and the audit committee** *(Page 3)*

While network members do not use the words enterprise risk management or the acronym ERM, they are committed to a holistic, organized, and comprehensive approach to risk management. Members described risk management as a journey, with different corporations at different stages, ranging from complex risk management frameworks and methodologies to less complex processes complemented by experience-driven intuition.

- **Identifying risk: How does the audit committee get a comprehensive view of risk?** *(Page 4)*

Reflecting common practice, members provide oversight of most risks by allocating time in regular meetings. However, this approach does not address their fear of being blindsided by unidentified reputation risks or non-calendar-based risk events, such as acquisitions. Several members have overseen the integration of risk management with the corporation's crisis management planning.

- **Prioritizing risk: How are risks classified and put before the audit committee?** *(Page 5)*

Most network members are being provided with rating systems by management (most often by the internal auditor); for instance, they may use traffic-light colors to indicate the degree of risk. The criteria being used to prioritize risk are often unclear to audit chairs. Despite their support for the internal audit function, many network members are concerned about whether that function has the necessary competencies to develop a comprehensive view of risk or the expertise to classify certain types of risk. Members agree that the audit committee should not rely on management's perspective alone, and should seek views from the independent auditor, subject experts, or risk management consultants.

- **Managing risk: How to coordinate across silos, and who in the corporation owns risk** *(Pages 5-6)*

Corporations are using internal audit, the general counsel, or the financial organization to provide risk management coordination across the enterprise, but network members feel strongly that the CEO has to embrace and drive the risk management process if it is to be successful. Members also expressed concern with the audit committee's agenda being over-managed by the corporate function that is coordinating risk management, and they would like to see less formal presentations and more robust discussions of risk in audit committee meetings.

## Overview: Enterprise risk management and the audit committee

A number of factors have combined to bring the topic of enterprise-wide risk management to the fore, including complex global operations, high-profile risk management failures, and regulatory attention. In order to fulfill their duties to shareholders responsibly, directors must have a comprehensive understanding of the risk associated with their companies.

What is the role of the audit committee with regard to enterprise-wide risk management? Although the New York Stock Exchange (NYSE) listing rules do not require that the audit committee be the sole body responsible for risk assessment and management, they do indicate that audit committees must discuss guidelines and policies for governing the process by which the company handles its exposure to risk.

Members of the network do not use the words enterprise risk management or the acronym ERM, but they are nonetheless committed to a holistic, organized, and comprehensive approach to risk management. The methods they use differ in their details, but tend to take a portfolio approach to managing enterprise-wide risks, allocating priority status to critical risks within each portfolio. Each audit committee is giving a high level of attention to risk identification, prioritization, and management.

Audit committees must ask what level of analysis is needed to provide an effective oversight role, given the time constraints of individual members and the need for clear distinctions in the roles of the committee and corporate management. As one chair commented, *“No system is perfect. [As audit chair], you have to be available and be a guide, but there has to be an institutional response. There has to be a bright line between management and governance.”*

Members of the network see risk management as a journey, with different corporations at different stages. Some are using complex ERM-style frameworks and methodologies, while others are relying on less complex processes complemented by more experience-driven intuition. See box below for examples of red flags used by network members to determine when a deeper dive into operational areas may be required.

### Examples of red flags that can indicate the need for deeper audit committee involvement

- “Unexpected” issues arising frequently in a particular geographic area or around a specific process – for example, inventory management, or revenue recognition
- Remote locations or those with significant distance from senior management in the organization
- Questions being answered in ways that are too slick, too quick, or defensive
- Questions being met with a quizzical look, an incomplete or “off the cuff” response, or some indication that the query is not relevant
- Output reports or numbers being frequently updated because of oversights or timing issues
- Audit deficiencies not being speedily and appropriately corrected and the audit committee so informed

## Identifying risk: How does the audit committee get a comprehensive view of risk?

Failure to identify a material risk in a timely fashion could lead to the direct, rapid destruction of shareholder value. Identifying risk is the main priority for most members of the network. The typical process undertaken by members of the network includes the following three steps:

- **Risk assessment:** The audit committee chair meets with the risk management committee, internal auditor, or whoever is driving risk management internally to discuss the overall list of risks facing the corporation. Concern about the process used to derive the list is an issue for audit chairs. *“The process we use is more important than the checklist we use because the checklist cannot be complete.”*
- **Risk categorization:** Members report using risk frameworks where risks are bucketed together in common categories typically focused on operational, financial, compliance, and strategic risks. One member’s alternative taxonomy included:
  - The emergence of disruptive technology
  - Risks associated with new business models
  - Reputation risks
  - Financial risks
- **Risk “calendarization:”** The highest risks are allocated to particular meetings of the audit committee throughout the year. One chair also *“re-look[s] at any ‘surprises’ a year later.”*

Members noted that the “calendarization” of risk brings concerns of its own. One chair summed up the prevailing opinion, *“What I don’t know about is what worries me.”* No matter how comprehensive their corporation’s risk management process is, members are concerned about the possibility of an unidentified – and perhaps unidentifiable – risk blindsiding them.

Often these unseen risks are associated with corporate reputation. Many members cited the recent mutual fund scandals as illustrating the difficulty in identifying risks. As one chair pointed out, *“Even when you catch things in a normal audit and you deal with them, you can still be trumped by someone externally [i.e., a regulator] with their own ideas about what needs to be done.”*

Several members are starting to integrate reputation risk into the corporation’s crisis management planning. *“If you have a reputation risk from left field, you need to have a crisis management plan to respond promptly and completely. We have a crisis management plan to cope with an accident even before we know all the facts.”* Indeed, one audit committee had participated in the corporation’s crisis management training.

For some members, reputation risk is as important as financial risk; they noted that reputation risk often has a financial impact on the corporation. However, other members cautioned that the audit committee should not lose sight of its primary financial role: *“It is important to ensure that we don’t lose sight of [the] numbers and the quality of the process for producing those numbers.”*

Key risk events, like acquisitions, also do not follow the audit committee’s calendar. Members observed that risk often comes to the fore post-acquisition and see an opportunity to apply risk management to the due diligence process: *“The risks involved should be part of the business case that goes to the board.”*

## **Prioritizing risk: How are risks classified and put before the audit committee?**

Once the corporation has a comprehensive view of risk, it is important to classify those risks and determine their relative priority. Most ERM frameworks prioritize risks according to three attributes:

- The probability that the risk will occur
- The potential frequency with which it may occur
- The likely severity of its impact on the corporation

Most network members are being provided with straightforward rating systems – for instance, traffic-light colors to indicate the degree of risk facing the corporation. Red and yellow risks are scheduled for audit committee oversight. Often an action plan is set out for each item and progress is tracked. On one audit committee, the appearance of a red risk at two consecutive meetings triggers an investigation.

In these rating systems, the determination of risk is usually made by management, most often by the internal audit function or occasionally the general counsel. However, the criteria being used to prioritize risks are often unclear to audit chairs: *“It is an informed judgment call from the people who have a role in identifying risk on a continuous basis.”*

Despite their support for the internal audit function<sup>1</sup>, many network members are concerned about whether internal audit has the necessary competencies to develop a comprehensive view of risk, or the expertise to classify certain types of risk. One member commented, *“The things we worry about – such as pricing in the field or quality control in the plants – are outside the view of the internal auditor and the legal department.”*

One audit chair, who has been closely involved in the process of supplementing the internal audit function, said, *“We have hired experts in a particular area and put them into internal audit. The audit committee has to support the expansion of internal audit to do this.”*

Regardless of the skill level internally, there is agreement that the audit committee should not rely on the perspective of the corporation’s management alone, and most audit committee chairs require an external view from the independent auditor, experts on the subject, or risk management consultants.

## **Managing risk: How to coordinate across silos, and who in the corporation owns risk?**

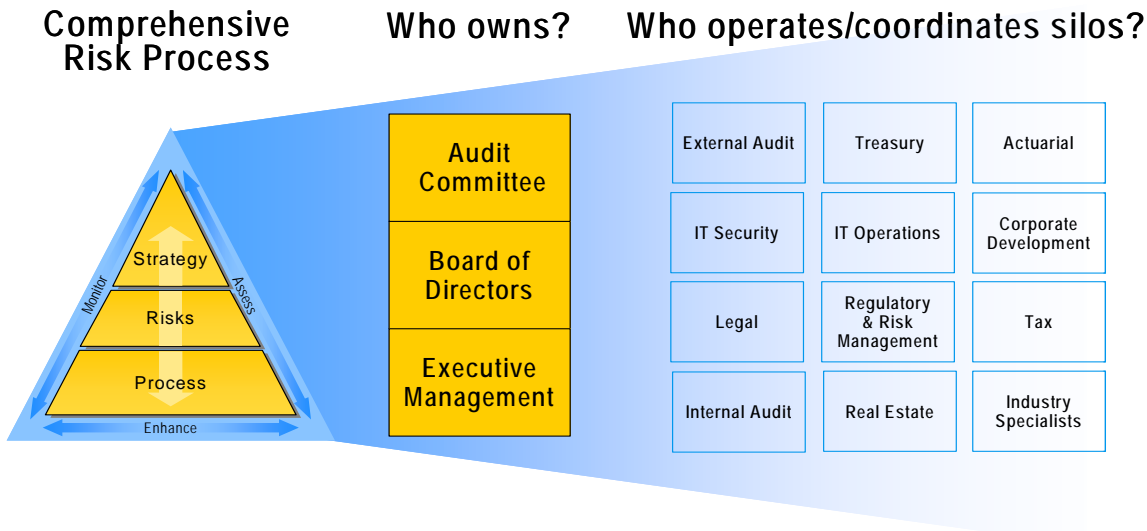
In keeping with their stated aim of taking a holistic, organized, and comprehensive approach to risk management, audit committee chairs face a critical challenge in managing risk across “siloes” functions, geographies, and lines of business.

As many as 12 different internal functions may be dealing with aspects of the risk management process (see Figure 1 on page 6). One audit chair gave a simple example regarding the insurance of operating plants where there was no coordination between the finance organization that was responsible for purchasing the insurance and the facilities team who actually managed the physical security of the plants and understood the real risks involved.

---

<sup>1</sup> Audit Committee Leadership Network, *ViewPoints*, “Audit committee emerging roles and responsibilities,” October 15, 2003: 7.

**Figure 1. Ownership and coordination of the comprehensive risk management process**



Many network members are aided in the coordination task by a cross-corporation, risk management committee. It is these committees that synthesize the information on risk drawn from individual departments. Corporations in the financial services sector have also appointed corporate risk officers (CROs) to provide a focal point for all risk management activity. In one organization the financial controllers in each business provide coordination. The audit chair commented, *“If the financial person in an operating group is not aware of risk, they should be removed.”*

There is a strong view that a comprehensive, enterprise-wide view of risk has to be both embraced and driven by the CEO. One audit chair was adamant: *“You need a CEO who really believes in the process. Without that you are in trouble. I would not serve on a board where the CEO was not committed.”*

Whichever internal group is running the enterprise-wide risk management process, there is one matter on which all members of the network agree: corporate functions should not over-manage the audit committee agenda, meetings, or the discussion of individual items. One member had the following advice for fellow audit committee chairs, *“Focus on getting good materials and ensuring that members read them ahead of the meeting. Don’t let [management] present but ask them questions, and manage the process to allow plenty of time for that.”*

*The views expressed in this document represent those of the Audit Committee Leadership Network. They do not reflect the views nor constitute the advice of network members, their companies, Ernst & Young, or Tapestry Networks. Please consult your counselors for specific advice. Ernst & Young refers to all members of the global Ernst & Young organization, including the U.S. member firm of Ernst & Young LLP.*

*This material is copyright Ernst & Young and prepared by Tapestry Networks. It may be reproduced and redistributed, but only in its entirety, including all copyright and trademark legends.*