



## **Enterprise Risk Management and the audit committee**

### **Introduction**

The Audit Committee Leadership Network in North America (ACLN) shared its views on Enterprise Risk Management (ERM) in the December 22, 2003, edition of *ViewPoints*. *VantagePoint* has been developed as a companion to *ViewPoints*; it compares and contrasts the perspectives of the Mid-Atlantic Audit Committee Network (MAACN) with those of the ACLN. Both reflect a synthesis of key issues arising from facilitated discussions among members of the respective networks.

The third meeting of the MAACN was held in Philadelphia on March 2, 2005, and focused on three questions related to enterprise-wide risk management:

- **Managing risk**
- **Identifying and prioritizing risk**
- **Disclosing risk**

The members of the network present at the meeting, who sit on the boards of more than 14 large-, mid-, and small-cap public companies between them, were:

- Mark Bartlett, Partner, Ernst & Young
- Jim Brady, Audit Committee Chair, Constellation Energy Group
- Bill Jews, Audit Committee Chair, MBNA
- John Schwieters, Audit Committee Chair, Smithfield Foods
- Larry Small, Audit Committee Chair, Marriott International
- John Tierney, Partner, Ernst & Young
- Ken Wolfe, Audit Committee Chair, Bausch & Lomb

*VantagePoint* 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

A number of factors have combined to bring the topic of risk management to the fore: complex global operations, high-profile risk management failures, and regulatory attention. In order to fulfill their duties to shareholders, directors must have a comprehensive understanding of their companies' business risks.

Although the New York Stock Exchange 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.<sup>1</sup>

Many companies are pursuing a holistic approach in the form of Enterprise Risk Management (ERM), a methodology that views risk in the context of business strategy rather than looking at individual hazards. ERM frameworks differ in their details, but all take a portfolio approach to managing enterprise-wide risks, allocating priority status to critical risks within that portfolio.

At its December 2003 meeting, the ACLN described risk management as a journey, with some corporations far down the road (already implementing complex risk management frameworks and methodologies) and others still at an earlier point (relying on less complex processes, complemented by experience-driven intuition). ACLN members said that management typically reports risks to the audit committee, but noted that the criteria used to prioritize risk are often unclear to audit chairs.

- **Managing risk: allocating responsibility across board committees** *(Page 3)*

MAACN members agree that the full board is responsible for overseeing the management of enterprise-wide risks. However, they feel it is appropriate for the board to delegate oversight of the risk management process to the audit committee and specific risks to relevant board committees. Some members think a company's Section 404 infrastructure could be extended to manage a more complex enterprise risk management effort, though they worry that frustration with the cost and disruption of Section 404 might decrease support for an integrated Section 404/ERM implementation.

- **Identifying risk: adding structure to intuition** *(Pages 3-4)*

MAACN members described processes for identifying and prioritizing risk in their companies that rely largely on management's experience-based intuition. Members recognize that risk factors are dynamic; they believe a more structured approach to risk identification and prioritization is likely to be required in the future.

- **Disclosing risk: informing investors and assessing management** *(Page 4)*

While MAACN members agreed that companies often over-disclose, revealing every possible risk to investors, some said that board directors could learn a lot about senior management's ability to identify, prioritize, and manage risk by probing their disclosure decisions.

---

<sup>1</sup> *Final NYSE Corporate Governance Rules 303A.07(c)(iii)(D)*, <http://www.nyse.com/pdfs/finalcorpgovrules.pdf>



## Managing risk: allocating responsibility across board committees

Members agreed that while the audit committee should have responsibility for overseeing some risk areas, the full board was ultimately responsible for the enterprise-wide risk management effort. Members thought the audit committee should review risks that are primarily financial in nature, but noted that there are *“other very significant risks that have nothing to do with finance.”* For this reason, members asserted it was *“hard to see how all the principal risk factors could be placed in the audit committee.”*

Members also distinguished between oversight of the process by which risk is identified, prioritized, and managed and oversight of the actual risks themselves. Some members felt the audit committee had a natural role overseeing the management processes associated with risk. One member, describing the audit committee chair’s leadership role during the risk-oriented parts of the board’s executive sessions, observed that while all board directors play a part in enterprise-wide risk management, *“right now, the audit committee is somewhat in the lead.”*

Once the full board has agreed on the priority risk areas, several members felt it was appropriate for some of the risks to be allocated to standing committees of the board. The allocation of responsibility for particular risk areas depends on a variety of factors (including relative committee workloads, committee members’ expertise, industry risk profile, and corporate tradition). Members suggested that a standardized approach to enterprise-wide risk management was impractical.

Some commentators have suggested that “[Sarbanes-Oxley] compliance could provide a much-needed infrastructure to support ongoing risk management,”<sup>2</sup> because the framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for the assessment of internal controls for Section 404 is a component of the recently released COSO ERM framework. While members said this integration *“sounds good if you say it fast,”* they worried that it might be difficult to achieve because of *“psychological barriers”* that result from what they see as the frustrating and expensive process of complying with Section 404.

## Identifying risk: adding structure to intuition

During their meeting in December 2003, ACLN members felt 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.”<sup>3</sup> MAACN members agreed that management is responsible for compiling a comprehensive list of material risk areas, yet few members described a formal process for soliciting outside input when identifying and prioritizing risks.

Audit committees have historically relied on board directors’ experience and intuition in overseeing enterprise-wide risks. However, one member recognized that intuition alone may not be sufficient. Observing *“We don’t do [this] as formally as we need to going forward,”* this member wondered if management needed to develop more systematic processes for evaluating and managing enterprise-wide risks.

<sup>2</sup> Joanne Sammer, “Companies Migrating from SOX ‘Myopia’ to ERM,” *Compliance Week*, November 2004, 26.

<sup>3</sup> Audit Committee Leadership Network, “Enterprise Risk Management and the audit committee,” *ViewPoints*, December 22, 2003, 2.



Members see an opportunity for the external auditor to help in the identification of enterprise-wide risk, acknowledging that the external auditor's insight into the company often goes beyond what is required for the audit. However, members recognize that they have not always sought out the external auditors' perspective, prompting one member to muse, *"I wonder what the auditor thinks about [the company's business risks] outside the numbers."*

Some audit committees have asked senior managers to use their experience-based intuition to develop a "Top 10" list of the most important areas of risk. Other committees follow a more systematic approach, with one member describing a detailed questionnaire that is sent annually to management and board directors. Respondents assess dozens of risk areas in terms of severity and incidence rate (frequency). Responses are then aggregated to reflect a prioritized, consensus view of enterprise-wide risks.

Although some members felt the Top Ten list would be fairly static, others members said it was surprising how perceptions of risk evolve over time. One member said that at any point in time, two-thirds of the risks were predictable, but the other third had changed to the point that they were *"worth talking about."* In spite of management's best effort to develop a comprehensive list of risk factors, one member observed, *"There's always a surprise."* This member noted that those surprises are incorporated into the list, and this feedback loop is used to refine the list over time.

### **Disclosing risk: informing investors and assessing management**

Regardless of how much responsibility the audit committee takes in overseeing enterprise-wide risks, it still has primary responsibility for approving filings to the Securities and Exchange Commission, many of which include a discussion of key risk factors facing the company.

Members are not worried that material risks might be omitted from public filings. Rather, many feel that companies tend to *"over-disclose"* risks, to the point that the list of risks factors included in many 10-Ks is *"beyond comprehension."* One member said, *"If anything, [companies are] going overboard on risk disclosure, [with] everyone trying to be holier than the church."*

Another member said that management regularly develops a matrix that compares the company's risk disclosures against those of its competitors. This member said that the objective is to develop a reputation with investors for disclosing more than anyone else in the sector.

One member observed that the disclosure process does offer board directors a valuable opportunity to assess management's ability to identify, prioritize, and manage risk. He said there is a lot to learn by asking management to describe *"the things they considered putting in [the disclosures], but didn't."*



## Conclusion

Risk management is not about eliminating business risks, but rather about developing and sustaining a company-wide process to identify, prioritize, and manage risk. Enterprise-wide risk areas are reviewed not only by the full board, but also by a number of board committees, including the audit committee. Given the many sources of risk, audit committees must develop effective mechanisms to communicate risk factors with the full board, and vice versa.

Board directors may want to consider the example of some MAACN members, whose boards rely not only on management for insight into the company's risk exposure but also seek the input of outside experts to help create a broader, more systematic view of enterprise-wide risks. Given the complexity inherent in the global business environment, it is impossible for a company to avoid surprises entirely. However, experts from outside the company may be able to highlight new, significant risk factors that lie outside management's base of experience. In this way, management and board directors can develop effective processes for identifying and managing risks, thereby ensuring that the company's enterprise-wide risk management program is aligned with its strategic objectives.

## About this document

The Audit Committee Leadership Network is a 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 Mid-Atlantic Audit Committee Network is a group of audit committee chairs from leading companies based in the Mid-Atlantic area. The networks are 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.

The ultimate value of *ViewPoints* and *VantagePoint* lies in their power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives these publications may share them with those in their own network. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

*The views expressed in this document represent those of the Mid-Atlantic Audit Committee 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.*